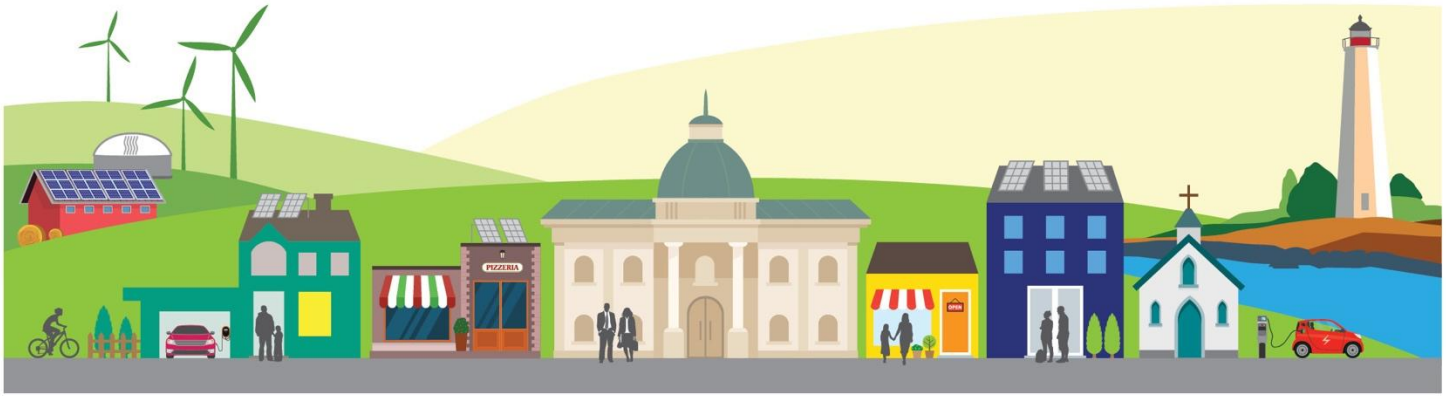
CONNECTICUT GREEN BANK®

Audit, Compliance and Governance Committee

MEETING DATE: TUESDAY, JANUARY 13, 2026 • 8:30AM



Audit, Compliance, Governance Committee

Thomas M. Flynn

Chair of ACG Committee

E: Tom.Flynn@tomflynn.org **P: 203-209-0059**

Thomas M. Flynn is the Managing Member of Coral Drive Partners LLC, a financial and operations consulting firm serving the Media and Information Services industry. He serves as Chairman of the Board of Finance for the Town of Fairfield, CT and as a member of the Board of Directors of Beardsley Zoo. Mr. Flynn is a graduate of Syracuse University with dual degrees in Accounting from the Whitman School of Business and Broadcast Journalism from the Newhouse School of Communications. Senator John McKinney appointed Mr. Flynn to the Board in July 2012.

Dr. Joanna Wozniak-Brown

Board Member

E: Joanna.Wozniak-Brown@ct.gov **P: 860-418-6252**

Dr. Joanna Wozniak-Brown has nearly two decades of experience in environmental management and planning in Connecticut. Currently, she serves as the Climate & Infrastructure Policy Development Coordinator at the Connecticut Office of Policy & Management. Prior to this role, she was the Assistant Director of Resilience Planning at UConn CIRCA. She earned her Ph.D. in Environmental Studies from Antioch University New England, an M.Sc. from Johns Hopkins University in Environmental Planning, and a B.A. from Drew University in Political Science and Environmental Studies. Dr. Wozniak-Brown has been certified by the American Institute of Certified Planners (AICP) since 2021.

Lonnie Reed

Board Chair

E: Lonnie.Reed@ctgreenbank.com **P: 203-481-4474**

Lonnie Reed serves as the Chair of the Green Bank's Board of Directors. Ms. Reed brings significant experience in environmental policy leadership, job creation, and a deep understanding of the climate challenges facing Connecticut. Reed served in the Connecticut State House of Representatives for five terms, from 2009 to 2019, before choosing not to run for reelection. She also served on the Bi-State NY & CT Long Island Sound Committee and helped lead the successful battle to stop Broadwater, a floating liquefied natural gas plant with a 22-mile pipeline proposed for Long Island Sound. Ms. Reed was appointed as Chair in October 2019 by Governor Ned Lamont.

Joins on an as needed basis for quorum

CONNECTICUT GREEN BANK

Audit, Compliance and Governance Committee Meeting Schedule

Tuesday, January 13th 2026

Tuesday, April 7th 2026

Tuesday, October 6th 2026

*all meetings from 8:30am-9:30am

The Green Bank Model

A Planet Protected by the Love of Humanity

1 Attract Private Investment by Leveraging Public Funding

Public Funding
Ratepayer dollars, taxpayer dollars

CONNECTICUT GREEN BANK

Private Investment
Individuals, credit unions, banks, bond buyers

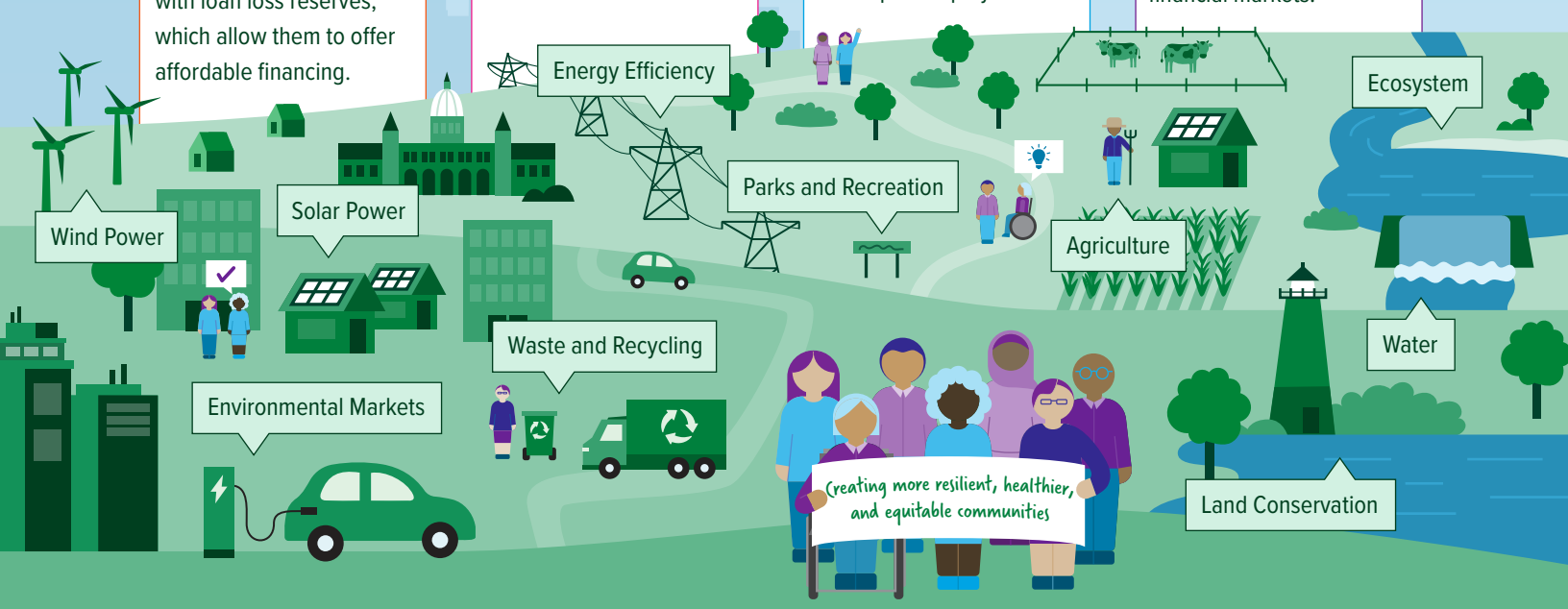
2 Apply Innovative Financial Tools to Deploy Investment Towards Our Mission

Generate **credit support** by providing local community banks with loan loss reserves, which allow them to offer affordable financing.

Initiate **co-investment** through public-private partnerships.

Support **performance-based incentives** to increase private investment and capital deployment.

Convert assets into **green bonds and notes** to be bought and sold in the financial markets.



3 Deliver Benefits to Connecticut's Families, Businesses, and Communities

Economic Development

- Creating thousands of jobs
- Generating millions in tax revenue

Ecological Resilience

- Driving environmental conservation, restoration, stewardship, and resilience

Energy

- Reducing energy burden by deploying clean energy
- Increasing energy security by deploying clean energy

Environmental Protection

- Reducing greenhouse gas emissions
- Improving the health of our residents by reducing air pollution

Equity

- No less than 40% of investment and benefits must reach vulnerable communities

CONNECTICUT GREEN BANK

Societal Impact Report

FY12 FY25

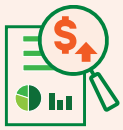
Since the Connecticut Green Bank's inception through the bipartisan legislation in July 2011, we have mobilized more than **$3.11 billion of investment** into the State's green economy. To do this, we used **$463.3 million** in Green Bank dollars to attract **$2.65 billion** in private investment, a leverage ratio of **$6.70 for every $1**. The impact of our deployment of renewable energy and energy efficiency to families, businesses, and our communities is shown in terms of economic development, environmental protection, equity, and energy (data from FY 2012 through FY 2025).*

ECONOMIC DEVELOPMENT

JOBS The Green Bank has supported the creation of more than **30,539** direct, indirect, and induced job-years.

TAX REVENUES

The Green Bank's activities have helped generate an estimated **$157.9** million in state tax revenues.



$60.6 million individual income tax

$60.6 million corporate taxes

$35.4 million sales taxes

$1.2 million property taxes

ENERGY

ENERGY BURDEN

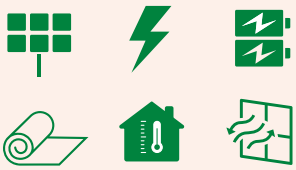
The Green Bank has reduced the energy costs on families, businesses, and our communities.

69,000+
families

8,500+
businesses

DEPLOYMENT

The Green Bank has accelerated the growth of renewable energy to more than **732.2 MW** and lifetime savings of over **93.9 million MMBTUs** through energy efficiency projects.



ENVIRONMENTAL PROTECTION

POLLUTION The Green Bank has helped reduce air emissions that cause climate change and worsen public health, including **7.4** million pounds of SOx and **9.3** million pounds of NOx lifetime.

11.8 MILLION tons of CO_2 : EQUALS

178 MILLION tree seedlings grown for 10 years

OR

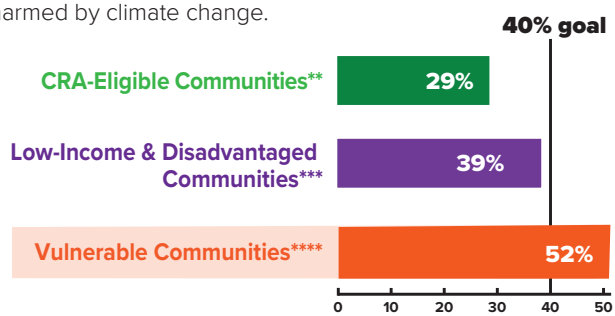
2.3 MILLION passenger vehicles driven for one year

PUBLIC HEALTH The Green Bank has improved the lives of families, helping them avoid sick days, hospital visits, and even death.

$234.7 – $530.8 million of lifetime public health value created

EQUITY

INVESTING in vulnerable communities, The Green Bank has set **goals** to reach **40% investment** in communities that may be disproportionately harmed by climate change.



** Community Reinvestment Act (CRA) Eligible Communities – households at or below 80% of Area Median Income (AMI)

*** Low-Income and Disadvantaged Communities – those within federal Climate and Economic Justice Screening Tool and Environmental Justice Screening Tool

**** Vulnerable Communities – consistent with the definition of Public Act 20-05, including low- to moderate-income communities (i.e., less than 100% AMI), CRA-eligible communities, and environmental justice communities (e.g., including DECD distressed communities)

* Includes projects, deployment, and investments approved, but not yet interconnected under Energy Storage Solutions.

Learn more by visiting ctgreenbank.com/strategy-impact/societal-impact/

Winner of the 2017 Harvard Kennedy School Ash Center Award for Innovation in American Government, the Connecticut Green Bank is the nation's first green bank.

Sources: Connecticut Green Bank Comprehensive Annual Financial Reports

75 Charter Oak Avenue, Suite 1 - 103, Hartford, CT 06106
T 860.563.0015
ctgreenbank.com

CONNECTICUT
GREEN BANK

January 6, 2026

Dear Audit, Compliance and Governance ("ACG") Committee Members,

We look forward to our meeting on Tuesday, January 13th, via Microsoft Teams (**Join the meeting now**) from 8:30 a.m. to 9:30 a.m. Our agenda will focus on three key items:

1. **Operating Procedure Revision – Chair approval required at $150,000**
2. Discuss **Information Technology Improvements**
3. Discuss **Legislative and Regulatory Policy Process and Update**
4. Discuss **Air Quality Impact Methodology**

As always, please let me know if you have any questions.

Sincerely,

Brian Farnen
General Counsel & Chief Legal Officer

AGENDA

Audit, Compliance and Governance Committee of the
Connecticut Green Bank
75 Charter Oak Avenue, Suite 1-103
Hartford, CT 06106

Tuesday, January 13, 2026
8:30 – 9:30 a.m.

Staff Invited: Jane Murphy, Brian Farnen, Dan Smith, Bryan Garcia, Bert Hunter, Joe Buonannata, Eric Shrago, and James Desantos

Others invites:

1. Call to order
2. Public Comments
3. Approve Meeting Minutes for October 7, 2025* – 5 minutes
4. Operating Procedure Revision – Chair approval required at $150,000** - 10 minutes
5. Information Technology Improvements** - 10 minutes
6. Legislative and Regulatory Policy Process and Update – 10 minutes
7. Air Quality Impact Methodology** – 5 minutes
8. Update on Statutory Report Status – 5 minutes
9. Board of Directors Membership Status Update – 5 minutes
10. Adjourn

*Denotes item requiring Committee action
** Denotes item requiring Committee action and recommendation to the Board for approval

Join the meeting now

Meeting ID: 286 817 346 357 5
Passcode: L84rn9hf

Or Call in using your telephone:
Dial +1 860-924-7736

Phone Conference ID: 758 308 752#

RESOLUTIONS

Audit, Compliance and Governance Committee of the
Connecticut Green Bank
75 Charter Oak Avenue, Suite 1-103
Hartford, CT 06106

Tuesday, January 13, 2026
8:30 – 9:30 a.m.

Staff Invited: Jane Murphy, Brian Farnen, Dan Smith, Bryan Garcia, Bert Hunter, Joe Buonannata, Eric Shrago, and James Desantos

Others invites:

1. Call to order

2. Public Comments

3. Approve Meeting Minutes for October 7, 2025* – 5 minutes

Resolution #1:

Motion to approve the minutes of the Audit, Compliance and Governance Committee meeting for October 7, 2025. Second. Discussion. Vote

4. Operating Procedure Revision – Chair approval required at $150,000** - 10 minutes

Resolution #2:

RESOLVED**,** that the Audit, Compliance, and Governance Committee recommends to the Board of Directors of the Connecticut Green Bank approval of the proposed revisions to the Green Bank Operating Procedures, contingent upon the completion of the public notice and comment period required under Connecticut General Statutes § 1-121 and the absence of any material or substantive revisions resulting therefrom.

5. Information Technology Improvements** - 10 minutes

Resolution #3:

WHEREAS, pursuant to Section 5.2.1 of the Connecticut Green Bank (Green Bank) Bylaws, the Audit, Compliance, and Governance (ACG) Committee is charged with the review and approval of, and in its discretion recommendations to the Board of Directors (Board) regarding, all governance and administrative matters affecting the Green Bank, including but not limited to organizational policies and the Green Bank Employee Handbook.

NOW, therefore be it:

RESOLVED, that the ACG Committee hereby recommends that the Board of the Green Bank approve of the implementation of new information technology policies and of the revisions to the Green Bank Employee Handbook presented on January 13, 2026 and as described in the memorandum to the ACG Committee dated January 6, 2025.

6. Legislative and Regulatory Policy Process and Update – 10 minutes

7. Air Quality Impact Methodology** – 5 minutes

Resolution #4:

RESOLVED, that the Audit, Compliance and Governance Committee hereby recommends to the Board of Directors for approval on its consent agenda the EPA AvERT Model for the Evaluation and Measurement of the environmental impact of Green Bank supported energy storage and electric vehicle projects as well as the estimation of the aforementioned pollutants.

8. Update on Statutory Report Status – 5 minutes

9. Board of Directors Membership Status Update – 5 minutes

10. Adjourn

*Denotes item requiring Committee action
** Denotes item requiring Committee action and recommendation to the Board for approval

Join the meeting now

Meeting ID: 286 817 346 357 5
Passcode: L84rn9hf

Or Call in using your telephone:
Dial +1 860-924-7736

Phone Conference ID: 758 308 752#

Announcements

- **In-Person Option** – if anyone wants to join future BOD or Committee meetings in person, we are inviting you to our offices in Hartford

- **Mute Microphone** – in order to prevent background noise that disturbs the meeting, if you aren't talking, please mute your microphone or phone.

- **Chat Box** – if you aren't being heard, please use the chat box to raise your hand and ask a question.

- **Recording Meeting** – we continue to record and post the board meetings.

- **State Your Name** – for those talking, please state your name for the record.

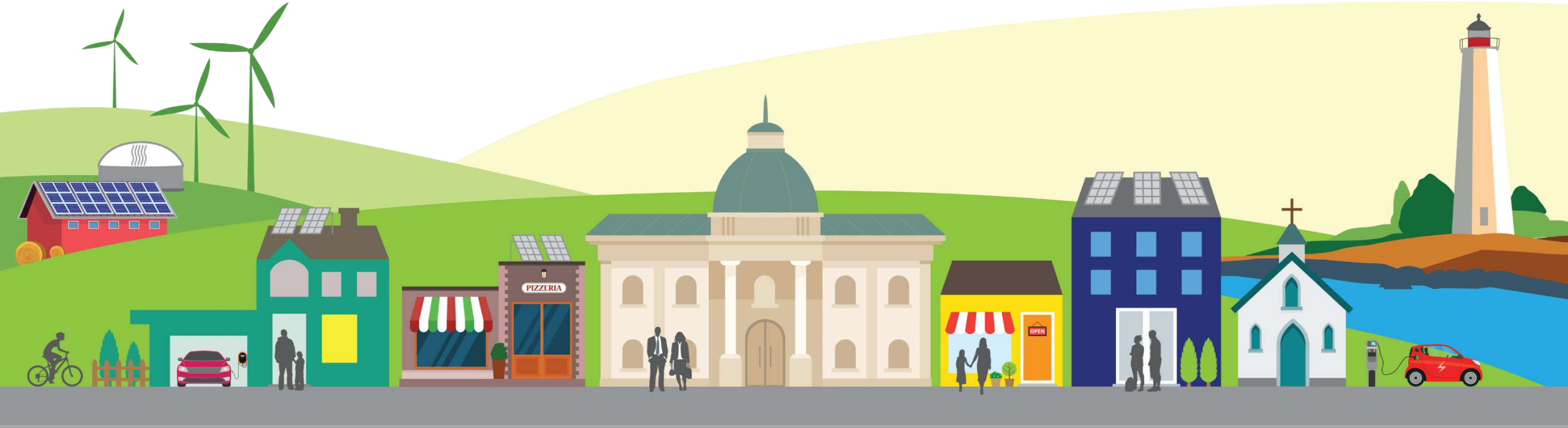
Audit, Compliance, and Governance Committee

January 13, 2026

CONNECTICUT GREEN BANK®

ACG Committee

Agenda Item #1
Call to Order



ACG Committee

Agenda Item #2
Public Comments

ACG Committee

Agenda Item #3
Meeting Minutes for October 7, 2025

Resolution #1

Motion to approve the minutes of the Audit, Compliance and Governance Committee meeting for October 7, 2025. Second. Discussion. Vote.

ACG Committee

Agenda Item #4

Operating Procedure Revision – Chair approval required at $150,000

Operating Procedure Revision – Chair approval required at $150,000

Purpose

As part of the annual governance review, staff is proposing one update to the Green Bank's Operating Procedures.

Proposed Change

Increase the Board Chair approval threshold from $75,000 to $150,000, reflecting the maturity of the organization and increased transaction volume.

What Is Not Changing

The competitive procurement threshold remains $150,000, preserving existing competitive bidding requirements.

Next Steps

Following ACG review, the proposed revisions will be presented to the Board and are subject to the public notice and comment process under CGS § 1-121.

Operating Procedure Revision – Chair approval required at $150,000

CONNECTICUT GREEN BANK

Operating Procedures

(revisions)

Contracts for professional services shall be awarded by the Green Bank in such manner, including on the basis of a sole-source procurement, as the Board determines to be appropriate and in the best interests of the Green Bank in the circumstances, provided that (i) for such contracts requiring an expenditure by the Green Bank up to and including one hundred fifty thousand dollars ($150,000)~~seventy-five thousand dollars ($75,000)~~ over a period of one (1) fiscal year, the President has sole approval authority~~; (ii) for such contracts requiring an expenditure by the Green Bank over seventy-five thousand dollars ($75,000) and up to and including one hundred fifty thousand dollars ($150,000) over a period of one (1) fiscal year, the President and the Chairperson must both approve the expenditure~~; and (~~i~~iii) for such contracts requiring an expenditure by the Green Bank of over one hundred fifty thousand dollars ($150,000) the President and the Chairperson must both approve the expenditure, and such contract shall, whenever possible, be awarded on the basis of a process of competitive negotiation where proposals are solicited from at least three (3) qualified parties.

Resolution #2

RESOLVED, that the Audit, Compliance, and Governance Committee recommends to the Board of Directors of the Connecticut Green Bank approval of the proposed revisions to the Green Bank Operating Procedures, contingent upon the completion of the public notice and comment period required under Connecticut General Statutes § 1-121 and the absence of any material or substantive revisions resulting therefrom.

CONNECTICUT GREEN BANK

Agenda Item #5

Information Technology Improvements

Information Technology Improvements
What are we proposing and why?

- As a result of recent audits, security assessments, and other benchmarking efforts, we are looking to update and create new policies that are intended to safeguard Connecticut Green Bank technology infrastructure and data.
- Our goal is to adopt industry best practices and we are using the National Institute of Standards and Technology ("NIST") Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations as one of those best practices.
- Working with Nexus Dynamics Group and our IT risk consultant (Danielle Simkowski – Assured Compliance Group), we identified four areas where we need to update existing policies/plans or create new ones:
  - Information Security Policy
  - Privacy Policy
  - Business Continuity and Disaster Recovery Plan
  - Incident Response Plan
- We are also proposing edits to the Employee Handbook to reference these new/revised policies and update relevant text.

Information Technology Improvements
Information Security Policy

- **Purpose**: This policy defines how Connecticut Green Bank will protect information and assets through the implementation of security measures. The topics within this policy are developed to consistently implement standards and set expectations with the workforce to minimize risk and safeguard the confidentiality, integrity and availability of information.

- This policy memorializes most existing IT security policies, including on security awareness training, employee vetting, and employee onboarding and offboarding.
- **New:**
  - This policy outlines a new vendor selection and onboarding process, which includes requesting and reviewing a SOC 2 report for the vendor if they will handle or have access to nonpublic or confidential data or have access to critical systems (e.g., Salesforce).
  - One-page user guides will be created in calendar Q1 on the following topics to help employees understand and implement this policy:
    - Physical security procedures
    - Vendor management procedures
    - Confidential and nonpublic information safe handling practices
    - System owner information security procedures

New Policy

Information Technology Improvements
Privacy Policy

- **Purpose:** This policy defines how Connecticut Green Bank will collect, use, disclose, retain and protect personal information.
- The topics within this policy are developed to consistently implement standards and set expectations with the workforce to minimize risk and safeguard the confidentiality of personal information.

- This policy memorializes existing privacy policy and procedures.
- Clarifies that any complaints should be directed to Eric, the Head of Operations.

New Policy

Information Technology Improvements
Business Continuity & Disaster Recovery Plan

- **Purpose**: This plan prepares the Green Bank for unexpected disruptions and outages due to events beyond our control and to recover critical business systems and services as quickly as possible.
- This document is intended to guide our organization in effectively communicating, assigning responsibilities, activating recovery procedures and staying resilient if a disruption occurs.

- **New –** this policy:
  - Identifies a BCDR Lead (Eric), Team (Joe & Barbara J.), and Crisis Management Team (Officers, Eric, Dan, Rudy, and Joe).
  - Identifies preferred recovery times and recovery points for system and function downtimes
  - Lists contact information for Senior Staff, their alternates, and critical vendors and emergency services
  - Communicates an easy way for staff to report actual or suspected incidents
  - Introduces an incident response form to document incidents
  - **This will require staff testing and training**

Revised Plan

Information Technology Improvements
Incident Response Plan

- **Purpose:** This plan provides a standardized response process for cybersecurity incidents and describes the process and completion through the incident response phases (including preparation, detection and analysis, containment, eradication and recovery, and post-incident activities).
- This plan outlines the people, processes and technologies needed to address incidents affecting Connecticut Green Bank's systems, data and networks to minimize harm, while supporting the restoration of business operations.

- **New –** this policy:
  - Identifies an Incident Response Leader (Eric), Handlers (Joe & Barbara J.), and Crisis Management Team (Officers, Eric, Dan, Rudy, and Joe).
  - Categories incidents as low, medium, high, and critical and outlines a response strategy for each
  - Communicates an easy way for staff to report actual or suspected incidents, which a one-page guide will also be created for
  - Introduces an incident response form to document incidents
  - **This will require staff testing and training**

New Plan

Information Technology Improvements
Employee Handbook Updates

Proposed edits to the Employee Handbook reference these policies, enhance IT security, and update related text. The edits are in redline between pages 58-70 in the handbook and include:

- Requiring that any email messages sent with confidential or nonpublic information be encrypted **(page 62)**
- Stating that employees should not open emails or click on attachments from unknown sources **(page 62)**
- Referencing the creation of the newly created reportincident@ctgreenbank.com email address for employees to immediately report potential and actual suspicious activity, incidents and unauthorized disclosure of personal information to the internal Incident Response Team **(page 68)**
- Editing the "mobile application management policy," previously referred to as the "mobile device management policy," to clarify that IT cannot remotely eliminate data associated with pertinent apps **(pages 69-70)**

Resolution #3

NOW, therefore be it:

RESOLVED, that the ACG Committee hereby recommends that the Board of the Green Bank approve of the implementation of new information technology policies and of the revisions to the Green Bank Employee Handbook presented on January 13, 2026 and as described in the memorandum to the ACG Committee dated January 6, 2025.

ACG Committee

Agenda Item #6

Legislative and Regulatory Policy Process and Update

Legislative and Regulatory Policy Process Update

2026 Legislative Session:
Convenes February 4th & Adjourns on May 6th "Short Session"

CGB Outreach - Fall 2025

Dynamic Situation:
Gubernatorial Election Year – Ned Lamont (D), Senator Fazio [R], Former Mayor Erin Stewart [R] New Britain
Senator Fazio current Ranking Member on the Energy & Technology Committee
State Senate & State House of Representatives – Election Year for all members
Representative John Steinberg – Current E&T Chair – Announced he is not running again.

Legislative Priorities:
Energy Affordability will be primary issue. Initiatives from 2025 Legislative Session will resurface.
DEEP Legislative Agenda – supportive role.
PURA Successor Study (Docket No 25-02-14) will guide legislative policy initiatives (NRES/RRES/SCEF). 1/21/25
Budget Adjustments: Federal decisions impacting state programs and climate change initiatives.

Legislative and Regulatory Policy Process Update

PURA COMMISSIONERS:

Thomas Wiehl – Interim Chairman – Formerly Legal & Regulatory Director of Office of Consumer Council (OCC)
David Arconti – Vice Chairman – Confirmed 2025 – Former State Representative (D-Danbury), UI Government Affairs
Janice Beecher – Interim Commissioner – Professor Emiritus at Michigan State University, Utilities Policy – Editor
Holly Cheeseman – Interim Commissioner – Former State Representative (R-East Lyme, Montville, Salem)
Everett Smith – CEO of GoldenSet Capital Partners – Investor in Energy & Sustainable Infrastructure
Has began Tenure at PURA after ethics review

Michael Caron – Appointment not renewed. Term ended when Everett Smith's began.

Next Steps:

2026 Legislative Session – Confirmation of 4 interim Commissioners (Wiehl, Beecher, Cheeseman, Smith)
Executive Nominations Committee approval – Anticipated February 2026
State House of Representatives Approval – Anticipated March 2026
State Senate Approval – Anticipated March 2026

CONNECTICUT GREEN BANK

Agenda Item #7

Air Quality Impact Methodology

Air Quality Impact Methodology

Expand current usage of EPA's Best in Class emissions tool to measure:

- VOC Emissions Impacts
- Ozone Emissions Impacts
- Emissions Impacts from EV conversions
- Emissions Impacts from Battery installations.

Resolution #4

RESOLVED, that the Audit, Compliance and Governance Committee hereby recommends to the Board of Directors for approval on its consent agenda the EPA AvERT Model for the Evaluation and Measurement of the environmental impact of Green Bank supported energy storage and electric vehicle projects as well as the estimation of the aforementioned pollutants.

ACG Committee

Agenda Item #8
Update on Statutory Report Status

Legislative and Regulatory Policy Process Update

2025 Statutory Reporting:			
STATUTORY REFERENCE	DEPARTMENT	DATE(s) FILED	COMPLIANCE
Quarterly Cash Flow	Accounting	3/18/25, 6/25/25, 9/30/25, 12/23/25	YES
Quarterly Human Resources	Human Resources	3/31/25, 7/2/25, 9/30/25, 12/31/25	YES
CGS Sec. 1-123	Operations	12/18/2025	YES
SCRF Notice	Finance	11/24/2025	YES
Green Bank Annual Report	Marketing	12/29/2025	YES
Board Meetings	Cheryl Lumpkin	All Regular & Special Meetings	YES
OpenCT Checkbook Data	Accounting	Due by 3/31/26	TBD

ACG Committee

Agenda Item #9

Board of Direcctors Membership Status Update

ACG Committee

Agenda Item #10
Adjourn

AUDIT, COMPLIANCE AND GOVERNANCE OF THE CONNECTICUT GREEN BANK
Regular Meeting Minutes

Tuesday, October 7, 2025
8:30 a.m. – 9:30 a.m.

A regular meeting of the Audit, Compliance, and Governance Committee of the **Connecticut Green Bank (the "Green Bank")** was held on October 7, 2025.

Committee Members Present: Thomas Flynn, Matthew Ranelli, Lonnie Reed

Committee Members Absent: Joanna Wozniak-Brown

Staff Attending: Priyank Bhakta, Joe Buonannata, Shawne Cartelli, James DeSantos, Mackey Dykes, Brian Farnen, Bryan Garcia, Bert Hunter, Cheryl Lumpkin, Jane Murphy, Tyler Rubega, Ariel Schneider, Eric Shrago, Dan Smith

Others present: Katherine Patnaude and Vinay Singh from PKF O'Connor Davies

1. Call to Order

- Thomas Flynn called the meeting to order at 8:33 am.

2. Public Comments

- No public comments.

3. Approve Meeting Minutes for May 13, 2025

Resolution #1

Motion to approve the minutes of the Audit, Compliance, and Governance Committee meeting for May 13, 2025.

Upon a motion made by Tom Flynn and seconded by Matthew Ranelli, the Audit, Compliance, and Governance Committee voted to approve Resolution 1. None opposed or abstained. Motion approved unanimously.

4. Annual Comprehensive Financial Report (ACFR) Review

- Katherine Patnaude from PKF O'Connor Davies summarized the overall highlights and financial statement highlights of the ACFR for FY 2025 including revenue trends, expense

trends, net position trends, and required communications. She noted the Green Bank received an Unmodified Opinion on its financial statements and there were no uncorrected misstatements or material corrected misstatements. She summarized the future considerations including GASB 103 and GASB 104.

- Tom Flynn thanked the PKF O'Connor Davies team for their effort and then Jane Murphy and the Accounting team for another successful audit.
- Tom Flynn asked what the current total reserve balance for loan losses is. Katherine Patnaude responded it is $25.4 million. Tom Flynn asked regarding the one borrower having financial difficulties if the total is fully reserved. Jane Murphy responded regarding that borrower that one loan is fully reserved, another has an at-risk portion that has been reserved for and the last has no reserve because it is secured by cash flows.
- Brian Farnen commented that the Green Bank is continuing a comprehensive review of investments. Bryan Garcia added that the Green Bank's financial sustainability is very important and all the lessons learned help the team improve that sustainability. He noted that in quarterly reports for the Board there will be a new addition of a schedule for loan loss reserves and a perspective on how the reserves are looked at in context of where the risks might be.
- Tom Flynn asked the auditors if there was any area of more concern than it was in prior years or any areas that would require focus that aren't reportable. Katherine Patnaude responded that there was not, and everything looks really good.
- Lonnie Reed asked for an update on the Green Liberty Bonds and Notes. Bert Hunter summarized an update to the Green Liberty Bonds which had an issuance in the prior week and had been oversubscribed by 2.6 times, so there was strong demand.

Resolution #2

RESOLVED, that the Audit, Compliance and Governance Committee hereby recommends to the Board of Directors for approval the proposed draft Annual Comprehensive Financial Report (ACFR) for the fiscal year ending June 30, 2025.

Upon a motion made by Tom Flynn and seconded by Matthew Ranelli, the Audit, Compliance, and Governance Committee voted to approve Resolution 2. None opposed or abstained. Motion approved unanimously.

5. Under $500,000 and No More in Aggregate than $1,000,000 – Staff Approved Transactions: Proposed Process Change

- Mackey Dykes summarized the history, process, and proposed increase for the Staff Aggregate Approval Authority to be $2,000,000. Bert Hunter added that the transactions included fall within an established program. Mackey Dykes clarified that the approved program frameworks are for C-PACE and for the Solar Loan, though there haven't been any transactions for the Solar Loan and historically it's all been under C-PACE so that would continue to be the majority.
  - Matthew Ranelli and Tom Flynn expressed their agreement that the time has finally come to adjust those limits.

Resolution #3

WHEREAS, the Connecticut Green Bank (the "Green Bank") Board of Directors (the "Board") has authorized Green Bank staff to evaluate and approve funding requests under $500,000, provided such requests are made pursuant to an established approval process,

require the signature of a Green Bank officer, are consistent with the Green Bank's Comprehensive Plan, fall within the approved fiscal budget, and remain within an aggregate limit not to exceed an amount updated from time to time (the "Staff Approval Policy for Projects Under $500,000"); and

WHEREAS, Green Bank staff seeks a recommendation from the Deployment Committee to the Green Bank Board to increase the aggregate not to exceed limit;

WHEREAS, on September 3, 2025, the Deployment Committee recommended that the Board approve an increase of the aggregate not to exceed limit of the Staff Approval Policy for Projects Under $500,000 from $1,000,000 to $2,000,000.

NOW, therefore be it:

RESOLVED, that the Deployment Audit, Compliance and Governance Committee recommends that the Board approve an increase of the aggregate not to exceed limit of the Staff Approval Policy for Projects Under $500,000 from $1,000,000 to $2,000,000.

Upon a motion made by Matthew Ranelli and seconded by Tom Flynn, the Audit, Compliance, and Governance Committee voted to approve Resolution 3. None opposed or abstained. Motion approved unanimously.

6. Legislative Process

- James Desantos discussed adherence to the Legislative Process Document and current status, which is within the (1) Pre-Session phase and noted there are no issues to present to the ACG Committee at this time, but if anything comes up as the process continues then it will be presented and discussed. He gave updates in relation to the Executive Branch Agencies Legislative Proposals, PURA, and a tentative Special Session.
    - Lonnie Reed asked if there has been any change to the lack of a PURA appointment and James Desantos responded that no, there have been no changes.
    - Tom Flynn asked when the changes within PURA start to affect the Green Bank and its mission. Brian Farnen responded he thinks there is still a fair amount of time before it becomes a pressing issue. James Desantos added that mid-December is when things might become more strained. The group discussed the potential timeline and other complications further.

7. Employee Handbook Revisions

a. College Tuition Reimbursement

- Joe Buonannata summarized the history and proposed revision to the Employee Handbook to extend and increase the Student Loan reimbursement policy as part of the Educational Assistance policy.
    - Matthew Ranelli asked if there is any information about how many staff members have used the Student Loan Reimbursement benefit and how much has been spent on that overall. Joe Buonannata responded that 25 staff have used the program over the years and just over $298,000 has been spent.
    - Tom Flynn asked how many of those employees have been retained and Joe Buonannata responded 3 of the employees are no longer with the Green Bank. Tom Flynn asked about the turnover rate for the company overall and Eric Shrago responded

it is about 3% per year, so the percentage of those who have left after receiving the benefit over the last 5 years is lower. Tom Flynn asked for an analysis of the turnover rate to see if the program is having the desired effect to increase retention. Eric Shrago said he would analyze further and follow up on it. Matthew Ranelli asked for additional breakdown of categories of employees using the benefit. Lonnie Reed asked the team to include any positive contributions from the employees who have received the benefit and are still with the Green Bank. Eric Shrago said the Green Bank team will present this information with the policy adjustment proposal at the next Board of Directors meeting.

Resolution #4

WHEREAS, pursuant to Section 5.2.1 of the Connecticut Green Bank (Green Bank) Bylaws, the Audit, Compliance, and Governance (ACG) Committee is charged with the review and approval of, and in its discretion recommendations to the Board of Directors (Board) regarding, all governance and administrative matters affecting the Green Bank, including but not limited to the Green Bank Employee Handbook;

NOW, therefore be it:

RESOLVED, that the ACG Committee hereby recommends that the Board of the Green Bank approve of the revisions to the Green Bank Employee Handbook specifically presented on October 7, 2025 and as described in the memorandum to the ACG Committee dated September 30, 2025.

Upon a motion made by Tom Flynn and seconded by Matthew Ranelli, the Audit, Compliance, and Governance Committee voted to approve Resolution 4 with the additional instruction that the information requested by Tom Flynn be presented at the next Board Meeting. None opposed or abstained. Motion approved unanimously.

8. Governance

- Brian Farnen noted are no revisions at this time and summarized the discussions that came up during the review process. He noted the 2025 Statutory Reporting are complete and in compliance.

9. Board of Directors Membership Status Update

- Brian Farnen noted the Board Membership is full and attendance has not been an issue.

10. Adjourn

Upon a motion made by Tom Flynn and seconded by Matthew Ranelli, the Audit, Compliance, and Governance Committee Meeting adjourned at 9:19 am.

75 Charter Oak Avenue, Suite 1 - 103, Hartford, CT 06106
T 860.563.0015
ctgreenbank.com

CONNECTICUT
GREEN BANK

Memo

To: Audit, Compliance, & Governance Committee - Connecticut Green Bank Board of Directors

From: Brian Farnen (Vice President, General Counsel & Chief Legal Officer)

Date: January 6, 2026

Re: Annual Governance Document Review

On an annual basis, the Legal Department reviews the Green Bank's governance documents and presents any proposed revisions to the Audit, Compliance, & Governance ("ACG") Committee. This year, staff is proposing a single revision to the Operating Procedures relating to Board Chair approval authority. Specifically, the proposed revision increases the Chairperson approval threshold from $75,000 to $150,000.

Given the maturity of the Green Bank's governance framework (now in place for approximately 14 years), the growth and evolution of the organization, and the increasing volume of transactions[1], the Board Chair has indicated a willingness to consider this procedural change. Importantly, staff is not recommending any change to the competitive procurement threshold, which will remain at $150,000 to ensure continued use of a formal competitive process for larger procurements.

Attached for the Committee's review are the proposed revisions to the Operating Procedures.

Upon successful review by the ACG Committee, these governance documents will be considered by the Board of Directors. Please note that approval of the Operating Procedures will also be contingent upon the feedback received through a required public comment period pursuant to CT General Statute § 1-121.

Resolution

RESOLVED, that the Audit, Compliance, and Governance Committee recommends to the Board of Directors of the Connecticut Green Bank approval of the proposed revisions to the Green Bank Operating Procedures, contingent upon the completion of the public notice and comment period required under Connecticut General Statutes § 1-121 and the absence of any material or substantive revisions resulting therefrom.

---

[1] Green Bank staff requested a total of forty-one (41) PSAs, or amendments to existing PSAs, with not-to-exceed amounts over the $75,000 threshold for FY2025 , for a total amount of $11,527,449.80. Approval for eighteen (18) of the forty-one (41) were requested of, and subsequently granted by, Lonnie Reed, Board Chair. The others all gained approval of the full Board of Directors, as either a one-time approval or as strategic selections for FY2025 at the 6/21/2024 BOD meeting or at subsequent meetings of the Board.

Attachment A

Operating Procedures

(revisions)

Contracts for professional services shall be awarded by the Green Bank in such manner, including on the basis of a sole-source procurement, as the Board determines to be appropriate and in the best interests of the Green Bank in the circumstances, provided that (i) for such contracts requiring an expenditure by the Green Bank up to and including one hundred fifty thousand dollars ($150,000)~~seventy-five thousand dollars ($75,000)~~ over a period of one (1) fiscal year, the President has sole approval authority~~; (ii) for such contracts requiring an expenditure by the Green Bank over seventy-five thousand dollars ($75,000) and up to and including one hundred fifty thousand dollars ($150,000) over a period of one (1) fiscal year, the President and the Chairperson must both approve the expenditure~~; and (~~i~~iii) for such contracts requiring an expenditure by the Green Bank of over one hundred fifty thousand dollars ($150,000) the President and the Chairperson must both approve the expenditure, and such contract shall, whenever possible, be awarded on the basis of a process of competitive negotiation where proposals are solicited from at least three (3) qualified parties.

Business Continuity & Disaster Recovery Plan

Effective Date		**Review Frequency**	Annually or at a major change in business function or system
Approval Date		**Approved By**	
Reviewed Date	12/19/2025	**Reviewed By**	Head of Operations

Version History

Version	Date	Prepared By	Approved By	Summary of Modifications
1.0	12/19/2025	Operations Team		First Draft

Table of Contents

Purpose

The purpose of this Business Continuity and Disaster Recovery ("BCDR") Plan is to prepare for unexpected disruptions and outages due to events beyond our control and to recover critical business systems and services as quickly as possible. This document is intended to guide our organization in effectively communicating, assigning responsibilities, activating recovery procedures and staying resilient if a disruption occurs.

Scope

The scope includes all information systems, applications, cloud environments, networks and data owned or managed by the Connecticut Green Bank that are business critical. This policy applies to all employees and relevant external parties and vendors/consultants.

Policy Statement

Connecticut Green Bank will maintain a Business Continuity and Disaster Recovery Plan that identifies critical business processes and the means to restore them in the case of a disaster or interruption. Clear responsibilities, communication avenues and actions required for implementing the plan will be defined.

Objectives

- Ensure the safety of our employees
- Maintain essential operations during disruptions
- Restore critical business operations within recovery objectives
- Protect confidential and nonpublic information and critical assets
- Establish BCDR Team to develop and implement plans
- Establish a Crisis Management Team to minimize risk and damage
- Assess lessons learned to improve this plan and controls to prevent future incidents

Communication and Escalation Plan

This section outlines how information will be shared and communication will flow during a disruption with the Connecticut Green Bank's workforce, vendors, customers, stakeholders, media and regulatory or legal entities.

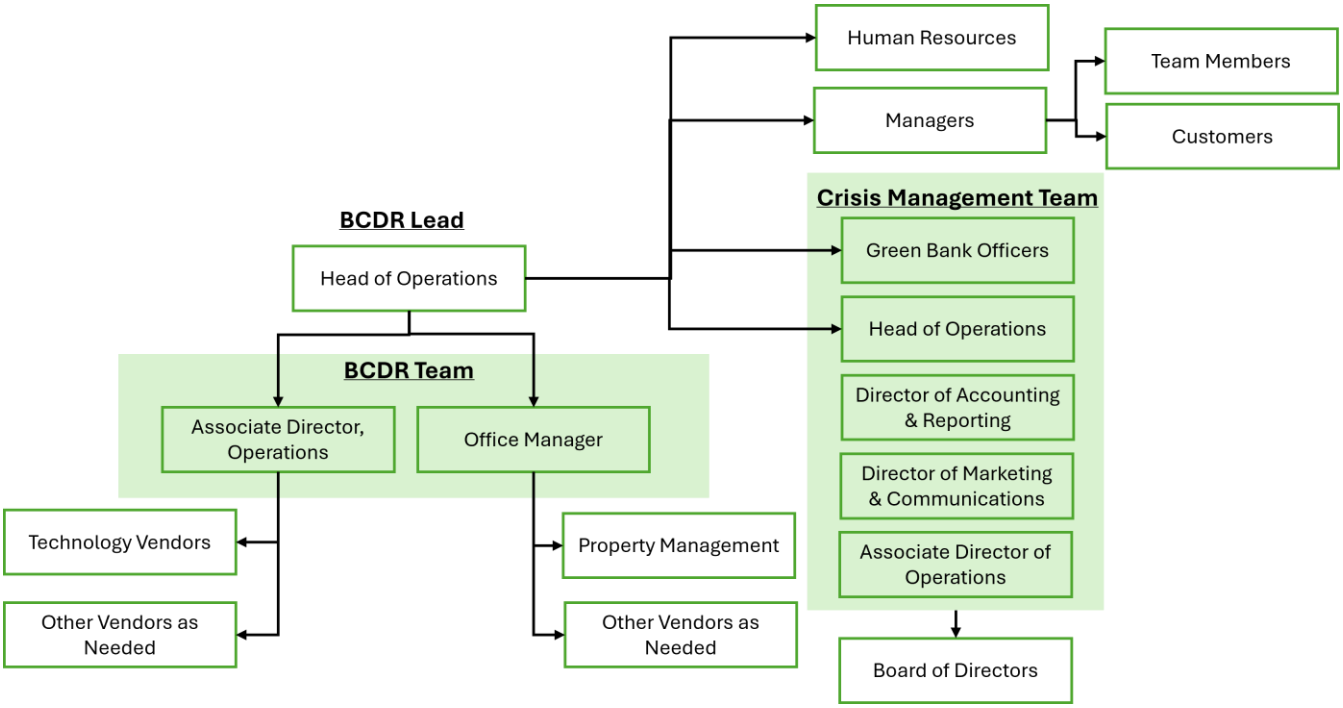
Immediate Emergency Response

During an emergency:

1. Assess your own safety, act accordingly and call 911 if needed
2. Elicit help from a co-worker
3. Act to protect life, then physical property
4. Follow the organization's Health and Safety section of the Employee Handbook

Communication Tree

The following diagram shows the flow of communication in the case of plan activation.



Communication Procedure

In the case of an emergency or disruption:

1. Inform the BCDR Lead, if this person is not available, inform a member of the BCDR Team. Send an email to reportincident@ctgreenbank.com, which will notify the BCDR Lead and Team.
2. The BCDR Team will contact each other and ensure the BCDR Lead is informed
3. The BCDR Lead and BCDR Team will assess the situation and potential damage then contact the appropriate vendors, external contacts, Green Bank Senior Staff and internal departments as necessary
4. The BCDR Lead will mobilize the Crisis Management Team as necessary

5. Depending on the scope of the disruption, Green Bank Senior Staff will inform the Board of Directors

Incident Notification

The BCDR Lead and Team will conduct the initial assessment. They will determine communication needed and appropriate timing depending on the situation.

Audience	Channel	Owner	Timing
Senior Staff	Phone, then email	Head of Operations	Immediate
Critical Vendors	Phone, then email	Associate Director, Operations and Office Manager	Immediate
Legal	Phone, then email	Head of Operations	Immediate
Human Resources	Phone, then email	Head of Operations	Within 1 hour
Managers	Email	Head of Operations	Within 2 hours
Employees	Email	Reporting Managers	As needed
Customers	Email	Account Managers	As needed
Board of Directors	Email	Senior Staff	As needed
Other Vendors	Phone, then email	Associate Director, Operations and Office Manager	As needed

Key Personnel Contact Information

See Appendix A for a list of key personnel and their contact information.

External Contact and Vendor Contact Notification

See Appendix B for a list of contact information for external contacts and vendors.

Customers

Clear and consistent communications of the incident will be developed by the BCDR Team and approved by the Crisis Management Team. All approved communication to customers will be performed by their Account Managers and delivered using the approved method identified.

Personnel Emergency Contact

If the incident has resulted in a situation which would cause concern to an employee's immediate family, Human Resources or the employee's direct manager will notify their emergency contact provided. All emergency contact information for employees is stored and maintained in CORE CT, on SharePoint and printed lists with each office's emergency equipment.

Media Communication and Releases

All incident related information (printed or spoken) will be coordinated and issued through the Crisis Management Team only. No other employees will speak to the media.

BCDR Roles and Responsibilities

The following table describes Connecticut Green Bank's assigned roles and responsibilities as they relate to business continuity and disaster recovery in the case of a disruption or disaster. The goal is to eliminate confusion, speed up recovery efforts and maintain accountability.

Role	Responsibilities
BCDR Lead	This is assigned to the Head of Operations. They are responsible for: • Overseeing the development and maintenance of the BCDR Plan • Leading BCDR tests and training efforts • Performing the initial assessment of a disruption or disaster • Communicating to appropriate departments • Mobilizing the Crisis Management Team • Overseeing plan activation and BCDR efforts • Directing business operations and approving priority of mission critical applications during a disruption or disaster • Updating Senior Staff, the Board of Directors and the Crisis Management Team as necessary • Creating customer communications • Transitioning to normal business operations after recovery • Participate in Incident Close Meeting
BCDR Team	This team is comprised of the Associate Director of Operations and the Office Manager. They report to the BCDR Lead. They are responsible for: • Developing and maintaining the BCDR Plan • Working with department managers as needed to ensure business process priorities are represented • Working with technology vendors to develop recovery and contingency plans for specific scenarios • Under the BCDR Lead's direction, performing the initial assessment of the disruption or disaster and mobilizing appropriate vendors • Maintaining documentation and performing status updates during a disruption or incident • Participating in BCDR Plan testing and training activities • Complete the Incident Response Form • Participate in the Incident Close Meeting
Crisis Management Team	This team is comprised of Green Bank Officers, Head of Operations, Director of Accounting & Reporting, Director of Marketing & Communications, Associate Director of Operations. They are responsible for: • Approving and delivering media and public communications • Handling regulators and stakeholders

	• Contacting the insurance company • Addressing immediate financial needs of the incident, including recovery efforts and related procurement • Assessing financial implications of the incident including lost documents, assets, revenue, etc. • Identifying and addressing legal implications as a result of the incident • Participating in BCDR Plan testing and training activities
Green Bank Senior Staff	Provide feedback on BCDR Plan development and updates prior to the Board of Directors approval, support BCDR Plan efforts and provide approval on related procurement. Stay informed on status updates and incident related communication. Provide direction on mission critical business operations during a disruption or disaster.
Board of Directors	Approve this BCDR Plan and related policies and procedures, oversee and support the BCDR program, document agendas, minutes and signatures showing oversight.
Managers	Ensure compliance with security and privacy policies and procedures, BCDR and Incident Response Plans in their teams, identify and report risks, potential or actual incidents, disruptions or disasters promptly to the BCDR Lead, and perform approved notifications and communications to their teams and customers as required.
Human Resources	Stay informed on status updates and incident related communication. Contact employee emergency contacts as necessary. Oversee and provide guidance on progressive discipline measures in the case an incident or disruption was caused by employee error, negligence or ill intent.
All Staff and Contractors	Follow security and privacy policies and procedures, BCDR and Incident Response Plans, report risks, potential or actual incidents, disruptions or disasters promptly to the BCDR Lead and their manager, complete required security, privacy and related training.
System Owners/ Administrators	Ensure access is authorized, documented and granted based on the principle of least privilege, required security controls are configured, and system is periodically monitored. Stay up-to-date and address system upgrades, new features and updates that may increase risk. Participate in line of business application recovery and testing in the case of a disruption, disaster or incident, validate business data and emergency mode operation procedures.
Third-Party Vendors	Meet contractual security obligations and undergo due diligence audits as applicable. Provide support and recovery activities as needed.

Threat Analysis and Risk Assessment

A risk assessment will be performed on a periodic basis to identify potential threats, evaluate the **likelihood** of the threat occurring and the **impact** if the threat did occur. Connecticut Green Bank will analyze the results of the risk assessment and use the findings and recommendations to anticipate disruptions and put proactive measures in place.

The table below depicts the threats most likely to impact Connecticut Green Bank's business, information systems and critical assets. The **likelihood** and **impact** each threat may have on the organization are rated on a scale from one to five, with five being the highest likelihood and impact and 1 being the lowest. The specific threats with the highest **Priority Score** are considered to have the most risk within the environment and have contingency plans created to minimize risk (See the Contingency Plans for Top Threats section of the Appendix for details).

Threat	Likelihood	Impact	Priority Score
Natural Disasters	2	3	6
Cybersecurity Incidents	3	5	15
Technology Failures and SaaS Downtime	3	5	15
Human Error	2	2	4
Insider Threat	1	2	2
Supply Chain Disruptions	1	3	3
Health Emergencies/Pandemics	2	3	6
Utility Failures	5	2	10
Financial Instability	3	2	6
Regulatory and Compliance Issues	2	2	4
Physical Security Breaches	2	3	6
Compromise of Critical Assets	2	3	6
Sabotage and Vandalism	2	3	6
Terrorism	1	1	1

Business Impact Analysis and Recovery Objectives

The business impact analysis determines which processes and functions are critical to business operations. This analysis defines the recovery objectives for each process and the impact if these business functions were interrupted.

The **Recovery Time Objective (RTO)** is the maximum acceptable amount of time a business function, system or application can be down for before it must be restored to avoid severe consequences to the business (How quickly must operations be restored?). Note that there are critical systems in the cloud that the Green Bank can't control the RTO for. In these cases, the best effort goal is listed in the table below.

The Recovery Point Objective (RPO) is the point in time the business can recover information without experiencing a significant impact and information loss. It defines how far back in time you can afford to go when restoring data (How much data can we afford to lose?). Note that there are critical systems in the cloud that the Green Bank can't control the RPO for. In these cases, the best effort goal is listed in the table below.

This table lists critical business functions, recovery requirements and the estimated impact of disruption.

Business Function	Owner	Recovery Time Objective (RTO)	Recovery Point Objective (RPO)	Impact/Criticality
Banking platform	Head of Accounting	48 hours	0	High
Loan disbursement	Head of Accounting	48 hours	0	High
Asset Management	Head of Operations	5 days	1 month	Medium/High
Customer support	Heads of Programs	48 hours	48 hours	Medium
Regulatory reporting	Heads of Legal, Investments, and Accounting	5 days	1 month	Medium
Intranet (SharePoint)	Head of Operations	24 hours	12 hours	High
Data Warehouse	Head of Operations	24 hours	24 hours	High
Communications Email/Phone	Head of Operations	24 hours	12 hours	High
Website	Head of Marketing	48 hours	48 hours	Medium/High
HR	Head of Operations	14 days	14 days	Medium
Payroll	Head of Accounting	14 days	14 days	Medium
Marketing	Heads of Operations and Marketing	48 hours	0	High

System Description

Physical Environment

As described in the Information Security Policy, there are physical security controls in place to safeguard critical systems, infrastructure, assets and data in all Connecticut Green Bank locations. Facility access controls and visitor procedures are implemented to minimize the risk of unauthorized access.

Property management can be contacted for property or facility incident related assistance (See Appendix B for Property Management contact information). There is a locked box outside the Hartford location for the fire department to access in the case of a related emergency.

Connecticut Green Bank employees are issued key fobs that have 24/7 access to their assigned locations. Fobs are also provided to property managers in both locations for general use and in case emergencies. Green Bank's IT vendor has key fobs with 24/7 access and the building janitorial service provider has restricted access during certain hours. Green Bank maintains two fobs with restricted building access to accommodate visitors as needed (e.g., contractors doing work in the office). The Head of Operations and the Office Manager have master keys to both offices.

Technical Environment

The Green Bank utilizes a variety of cloud systems for key business operations. Central to those systems, is Office 365 used for collaboration, document management and communication (Email, File Sharing, Phones, and Chat). Users of this environment can connect globally from any machine. For some business functions, the Green Bank utilizes a data warehouse which is stored in Microsoft Azure using both IaaS and Saas products. Access to these systems is either through a VPN connection from one of the Green Bank's offices or through Microsoft Azure application gateways. Backups are configured in Microsoft 365 and Azure.

The Green Bank has also implemented cloud applications to perform business functions. These systems are controlled by "system owners" and are listed in the Critical Systems Inventory spreadsheet including details such as vendors and subject matter experts for each system.

As described in the Information Security Policy, technical security controls and a vendor management procedure are in place to safeguard company systems, data and assets. Patch management, antivirus and malware protection are in place on all endpoints. The Green Bank has also implemented a SIEM via their third-party vendor to centralize logs and detect events.

There is an infrastructure closet in the Green Bank's Hartford location. See Appendix C: IT Diagrams for details.

Critical Systems

Connecticut Green Bank maintains a Critical Systems Inventory to prioritize recovery efforts. This inventory is used in the development of contingency plan strategies to align strategies with defined priorities.

Off-Site Documentation

The following documentation has been identified as critical to the organization and to the recovery efforts in the case of a disaster. Connecticut Green Bank will maintain copies of these documents in a safe, secure and accessible off-site location.

- Business Continuity and Disaster Recovery Plan
- Incident Response Plan
- Employee Handbook
- Critical Systems Inventory
- Critical Assets Inventory

Alternate Work Facilities

In the event the Connecticut Green Bank physical offices are unavailable for employees to access and work, the organization will permit the following:

- As outlined in the Telecommuting section of the Employee Handbook, all employees will work from home. Due to the hybrid work environment, all employees are required to take their laptops home with them on a nightly basis. If the disruption or incident happens after hours or an employee does not have their device with them, employees can access the web version of Microsoft Office with their personal device and coordinate with their supervisor.
- Members of the BCDR Team and Crisis Management Team will be permitted to work from home unless or until an alternate location has been identified for them to report to. If the disruption or incident happens during business hours, these employees will take their devices and related work items with them. If the disruption or disaster happens after hours or an employee does not have their device with them, employees can access the web version of Microsoft Office with their personal device and coordinate with their supervisor.

Continuity Strategies for Critical Services

If a disruption or disaster occurs, the following strategies will be implemented to maintain critical services and business functions during down time.

Critical Service/Business Function	Continuity Strategy
Customer Service Delivery	Heads of Operations, Heads of Marketing and Heads of Programs will coordinate on email communications to impacted external parties and develop any continuity strategies for performing critical functions during recovery mode.
IT Operations	The organization's third-party vendor will continue to assist in the continuity of business functions.
Email	Marketing will update the Green Bank's website and social media accounts to notify the public.
Phones	Marketing will update the Green Bank's website and social media accounts to notify the public.
Finance, Legal, HR	Heads of Operations will coordinate with Green Bank leadership to manage internal communication to employees and any relevant external parties and develop any continuity strategies for performing critical functions during recovery mode.
Marketing	Head of Marketing and Heads of Programs will coordinate on email communications to impacted external parties and develop any continuity strategies for performing critical functions during recovery mode.

Business Continuity and Disaster Recovery Phases

Alert/Verification/Activation Phase

Upon the discovery of a potential incident, disaster or disruption the following steps must be taken to alert the required contacts.

Incident Notification

When a potential or actual incident is detected the BCDR Lead and Team must be immediately notified to allow them to begin incident response procedures. Green Bank personnel will be asked to report incidents by emailing reportincident@ctgreenbank.com so they can effectively communicate incidents to the BCDR Lead and Team in a timely manner. In the case of incidents in Microsoft 365 or the network, the BCDR Lead and Team will be promptly notified by the IT vendor.

Plan Activation

The following criteria will activate the plan. The plan is activated when:

- The primary office locations are inaccessible
- Communications are down (phone, email)
- A critical system becomes unavailable
- An event disrupts customer-facing services

The BCDR Lead and Team will meet and decide the extent to which the BCDR Plan must be invoked, including:

- Assess the disaster and its impact on the business to determine which elements of the plan should be activated
- Inform the required teams, vendors, Green Bank Senior Staff, employees, customers, etc.
- Determine if escalation to the Crisis Management Team and Board of Directors is needed
- Allocate responsibilities
- Begin documenting the incident using the Incident Response Form in Appendix D.

Declaring an Incident

The BCDR Lead, along with the input from the BCDR team, Crisis Management team, Green Bank Senior Staff, and vendors, is responsible for declaring an incident. They will then activate the various employees, vendors and external contacts required depending on the disaster and the elements of the plan invoked.

If an incident is not declared, the BCDR Lead and Team will continue to address and manage the situation through its resolution. The Incident Response Form will be completed with this status noted.

If an incident is declared, the BCDR Lead and Team will initiate recovery efforts.

Assess the Damage and Determine a Recovery Strategy

Once a disaster is declared, the BCDR team will gather as much information as possible and determine which employees, vendors and external contacts to engage. Along with the BCDR Lead and depending on the incident, the Crisis Management Team, they will:

1. Gather information about the incident and identify safety and security issues.
2. Conduct a Detailed Damage Assessment and collect evidence where possible.
    a. Assess the damage to the affected property, assets, documents and systems. Include vendors when applicable to properly gauge damage, determine the best recovery strategy and estimated cost.
    b. Begin completing the Incident Response Form and, if needed, provide to the Crisis Management Team.
3. Consider Financial and Legal Implications.
    a. Analyze the damage assessment and assess the impact of the incident on the financial state of the organization. Identify the immediate financial needs for recovery and determine the best strategy to cover costs.
    b. Determine any legal actions that may result from the event, either by or against the organization. Determine the best strategy to address these and communicate to appropriate parties including the BCDR Lead and Team.
4. Determine the recovery strategy and procedures needed to recover business critical functions in a prioritized manner while maintaining the security of confidential and nonpublic information. See the Contingency Plans for Top Threats section of the Appendix for detailed recovery procedures for specific incidents.
5. Update the Incident Response Form.

Business Recovery Phase

Complete the required communications to begin the business recovery phase per the recovery strategy decided upon. During this phase the BCDR Team will:

1. Engage appropriate vendors
2. Monitor progress and communicate updates as needed
3. Mobilize identified employees to test and confirm business unit operations, system functionality and data integrity
4. Work as a central point of contact for incident updates from vendors, employees, etc.
5. Update and maintain the Incident Response Form

Resume Business as Usual

During the recovery phase a plan to reestablish normal business functions will be created. Depending on the size and complexity of the incident, this may be included in the recovery

strategy and procedures. The goal is to ensure all information collected when working in recovery mode is securely updated in required systems, data integrity checks are performed, and the business can function as usual.

Plan Testing

This BCDR Plan will be periodically tested to ensure the accuracy and effectiveness of business continuity strategies, disaster recovery procedures and contingency plans. Updates will be made to the BCDR Plan based on the results of these tests.

The following tests will be conducted:

- Annual tabletop exercises/simulations based on top scenarios
- Annual plan review and updates

Plan Training

The BCDR Lead and members of the BCDR and Crisis Management Teams will receive training on this BCDR Plan and related procedures to ensure they are able to perform required efforts quickly and decisively.

Plan Management

The Green Bank will maintain this plan in accordance with other security polices to comply with required frameworks, regulations and company standards. If modifications are made to this plan, they will be documented and approved prior to implementation across the workforce. This plan will be reviewed annually internally at the staff level or as business needs and regulatory requirements evolve and approved by the Head of Operations. Any substantive changes will be presented for Board of Directors' review and approval prior to implementation. This plan will be made available to employees and centrally stored with other company policies and procedures.

Compliance & Monitoring

The Green Bank takes violations of security policies and procedures very seriously. Suspected or actual violations will be documented, investigated and tracked per the Progressive Discipline Policy in the Employee Handbook. Non-compliance with this plan may result in disciplinary action, up to and including termination of employment.

Related Documentation

- Incident Response Plan
- Information Security Policy
- Critical Systems Inventory
- Critical Assets Inventory
- Security Risk Assessments
- Privacy Policy
- Employee Handbook

Appendices

Appendix A: Key Personnel Contact Information

These contacts will be updated internally as necessary.

Name / Title	Contact Option	Contact Number
Bryan Garcia President and CEO **Crisis Management Team**	Phone – Work	860-257-2170
	Phone – Mobile	203-675-9464
	Email – Work	Bryan.Garcia@ctgreenbank.com
	Alternate	Cheryl Lumpkin (cell: 860-308-0049)
Bert Hunter Executive Vice President and Chief Investment Officer **Crisis Management Team**	Phone – Work	860-257-2174
	Phone – Mobile	203-918-0013
	Email – Work	Bert.Hunter@ctgreenbank.com
	Alternate	Mariana Trief (cell: 617-717-8087)
Brian Farnen Vice President, General Counsel and Chief Legal Officer **Crisis Management Team**	Phone – Work	860-257-2892
	Phone – Mobile	203-400-8380
	Email – Work	Brian.Farnen@ctgreenbank.com
	Alternate	Alex Kovtunenko (cell: 203-240-116)
Mackey Dykes Executive Vice President & Officer Financing Programs **Crisis Management Team**	Phone – Work	860-257-2175
	Phone – Mobile	229-869-3363
	Email – Work	Mackey.Dykes@ctgreenbank.com
	Alternate	Alysse Buzzelli (cell: 203-231-9914)
Eric Shrago Executive Vice President of Operations **BCDR Lead** **Crisis Management Team**	Phone – Work	860-257-2897
	Phone - Mobile	646-522-0348
	Email - Work	Eric.Shrago@ctgreenbank.com
	Alternate	Joe Buonannata (cell: 860-462-3614)
Jane Murphy Executive Vice President of Finance and Administration **Crisis Management Team**	Phone – Work	860-258-7809
	Phone - Mobile	860-214-1503
	Email - Work	Jane.Murphy@ctgreenbank.com
	Alternate	Dan Smith (cell: 413-563-1603)
Sergio Carrillo Managing Director, Incentive Programs	Phone – Work	860-258-7826
	Phone - Mobile	610-235-9503
	Email - Work	Sergio.Carrillo@ctgreenbank.com
	Alternate	Sara Pyne (cell: 860-459-4887)
Leigh Whelpton Director of Environmental Infrastructure Programs	Phone – Work	860-257-2362
	Phone - Mobile	513-520-6101
	Email - Work	Leigh.Whelpton@ctgreenbank.com
	Alternate	Austin Dziki (cell: 860-617-8910)
Sara Harari Director of Innovation	Phone – Work	860-249-0806
	Phone - Mobile	781-645-9463
	Email - Work	Sara.Harari@ctgreenbank.com
	Alternate	Stefanie Keohane (cell: 860-989-5541)
Rudy Sturk Director of Marketing and Communications	Phone – Work	860-259-1154
	Phone - Mobile	203-738-9009
	Email - Work	Rudy.Sturk@ctgreenbank.com

Crisis Management Team	Alternate	Robert Schmitt (cell: 860-908-6905)
Joe Buonannata Associate Director, Operations **Crisis Management Team** **BCDR Team**	Phone – Work	860-259-1592
	Phone - Mobile	860-462-3614
	Email - Work	Joe.Buonannata@ctgreenbank.com
	Alternate	Barbara Johnson (cell: 860-301-8831)
Barbara Johnson Office Manager **BCDR Team**	Phone – Work	860-258-7817
	Phone - Mobile	860-301-8831
	Email - Work	Barbara.Johnson@ctgreenbank.com
	Alternate	Mary Vigil (cell: 860-908-2537)

Appendix B: External Vendor Contact Information

These contacts will be updated internally as necessary.

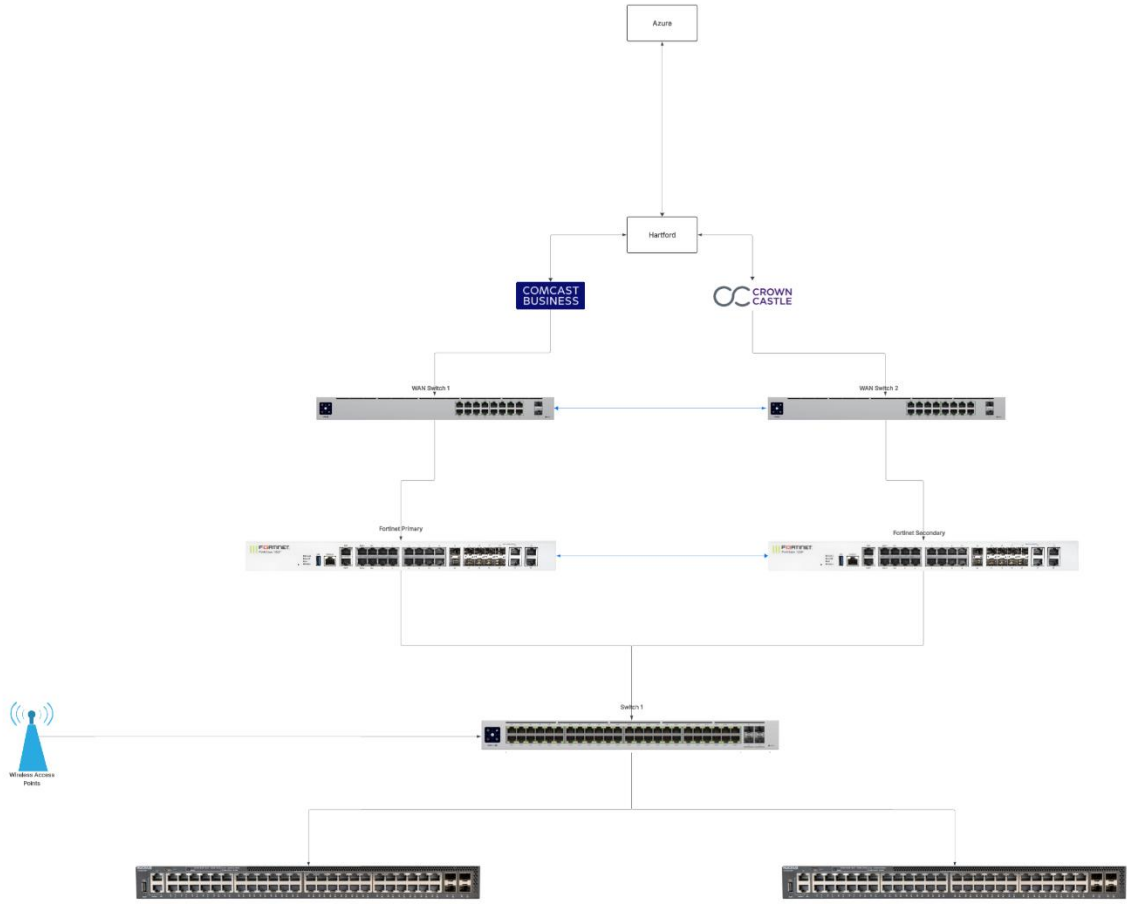
Title / Name/ Account Number Contact Options		Contact Number
Landlord / Property Manager **Hartford Office:** **TRIO PROPERTIES** **Capewell Lofts/Atlantic Works**	**Phone Numbers**	Kristen Klopp, Property Manager (o) 860-244-2260; (c) 860-966-0848 Jeremy Browning, TRIO Properties 860-244-2260
	Email	kklopp@trioproperties.com; jbrowning@trioproperties.com;
	Website / Portal	www.AtlanticWorksHartford.com
Stamford Office: **MOUNTAIN DEVELOPMENT CORP.** 56 Livingston Avenue Suite 200	**Phone Numbers**	Lisa Parisi, Property Manager 203-690-2156 Kurt Neuert, Onsite Property Manager 203-223-5080
	Email	Lparisi@mountaindevelopment.com kneuert@mountaindevelopment.com
	Website / Portal	www.mountaindevelopment.com
IT Resources **Nexus Dynamics Group** 493 Little City Road Higganum CT 06441	**Phone Numbers**	William Vinopal C: 626-592-9346 Support P: 203-599-3440
	Email	support@choosenexus.com Wvinopal@choosenexus.com
	Website / Portal	www.choosenexus.com
Security / Alarm **SONITROL** 19 Tuttle Place Middletown, CT 06457	**Phone Numbers**	Chris Goff: 860-616-7558 Urgent: 800-322-3500 Main: 860-616-7501
	Email	Chris.goff@sonitrolnewengland.com
	Website / Portal	www.sonitrolnewengland.com
Office Supplies **SUBURBAN STATIONERS** 691 High Street Middletown, CT 06457	**Phone Numbers**	Jeremy Bourret, CEO 860-347-0299
	Email	Jeremy@suburbanop.com
	Website / Portal	http://shop.suburbanop.com/
	Account / Info	38482-CONNECTICUT GREEN BANK
Bank	**Phone Numbers**	Customer Service (888)-932-2256 Bank Contact: Lawrence Davis (o) 860-692-1351 (c) 860-508-7757
	Email	lmdavis@websterbank.com

WEBSTER	**Website / Portal**	www.websterweblink.com
Phone System **Nexus Dynamics Group** **493 Little CIty Road** **Higganum CT 06441**	**Phone Numbers**	William Vinopal 860-592-9346 Strategic Advisor
	Email	wvinopal@choosenexus.com
	Website / Portal	Choosenexus.com
Accounting Software **Intacct**	**Phone Numbers**	Marlaina Luciano – (978) 533-1250 Customer Support - (877) 704-3700
	Email	Marlaina Luciano Marlaina.Luciano@sage.com
	Website / Portal	www.sageintacct.com
	Account / Info	Customer Id: C3815
Insurance	**Phone Numbers**	Roy Ivins Phone: (203) 397-5050 Cell: (203) 623-3167 USI - Lynette Haaf (203) 634-5754
	Email	Roy Ivins (rmivins@rmiassociatesllc.com)
	Website / Portal	www.usi.com
	Account / Info	Client Code - CONNEGRE1
Insurance **Solar Policies** **(CTSL2, CTSL3, CSS, CGB-CSCU)**	**Phone Numbers**	Roy Ivins Phone: (203) 397-5050 Cell: (203) 623-3167 Gallagher - Tyler Wooldridge Office (479) 494-1737 Mobile: (417) 631-
	Email	Roy Ivins (rmivins@rmiassociatesllc.com) Tyler Wooldridge Tyler_Wooldridge@ajg.com
	Website / Portal	www.ajg.com
	Account / Info	Account Number – CTSOLAR-01
Printers/Copiers **RYAN Business Systems**	**Phone Numbers**	Kathy Ryan, President (860) 339-0521, (800) 842-1916 Ryan Business Systems, Inc.
	Email	kathyryan@ryanbusiness.com
	Website /Portal	www.ryanbusiness.com
	Account / Info	455 Govenors Hwy, South Windsor, CT 06074
CRM **Salesforce**	**Phone Numbers**	Wade Shelton, Account Exec 703-297-7134
	Email	Wshelton@salesforce.com
	Website / Portal	https://www.salesforce.com/ ctgreenbak.lightning.force.com/lightning/page/home
Salesforce	**Phone Numbers**	Victoria Ritter, Renewals Manager 703-673-3513 888-66-CARAH Fax: 703-871-8505
	Email	Victoria.ritter@carahsoft.com

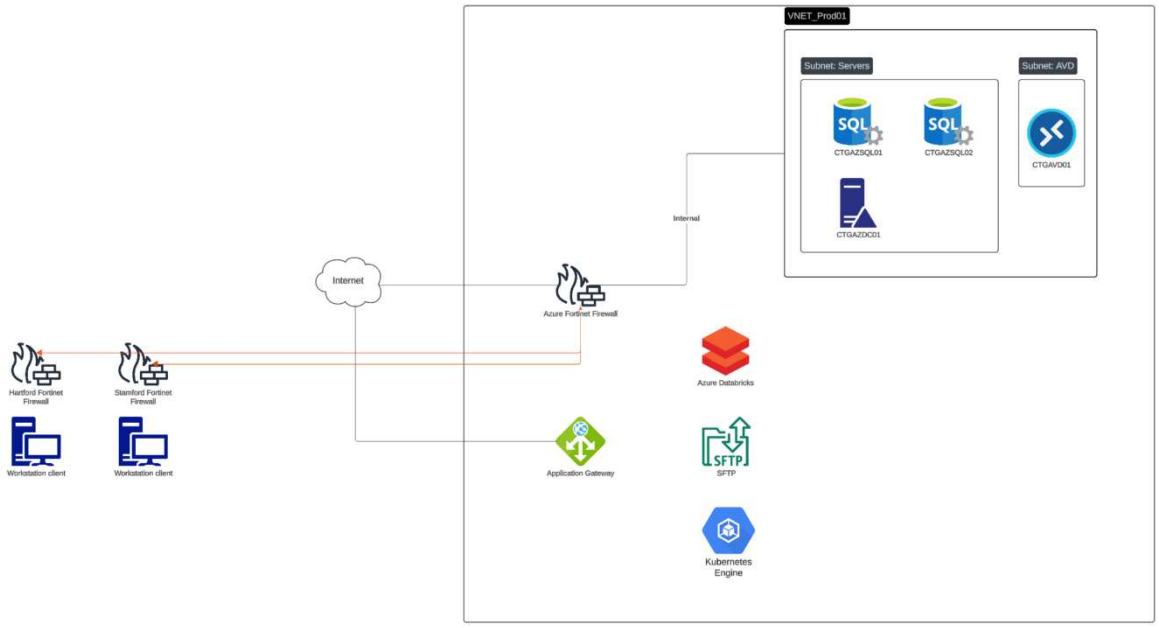
(billing contact) **Carahsoft Technology Corp**	**Website / Portal**	www.carasoft.com
	Account / Info	CGB001
NGEN **(Smart-E Web Platform)**	**Phone Numbers**	Kevin Southworth, VP & Co-founder Joel Schneider, Developer
	Email	Kevin.southworth@webascender.com Joel.schneider@webascenter.com
	Website / Portal	https://ngen.ctgreenbank.com/ https://www.webascender.com/
POWERCLERK	**Phone Numbers**	Chris French, Senior Account Executive, Utilities 425-242-7039 C: 781-879-9783
	Email	chrisf@cleanpower.com
	Website / Portal	
LOCUS **Also Energy, Inc.** **5400 Airport Blvd. Ste. 100** **Boulder, CO 80301**	**Phone Numbers**	Jeff Muench, Sr. Bs. Dev. Mgr., Residential and Distribution Sales 866-303-5668 Direct: 212-500-2098
	Email	Jeff.Muench@alsoenergy.com
	Website / Portal	https://alsoenergysupport.setmore.com/
Hospital **HARTFORD HOSPITAL** 80 Seymour Street Hartford, CT 06102	**Main Number**	860-545-5000 1-800-222-1222 https://hartfordhospital.org/
		Poison Control Center (911)
		Emergency Management Office
		1-800-286-5700
Eversource	**Phone Numbers**	Electricity: 800-286-2000 Gas: 877-944-5325

Appendix C: IT Diagrams

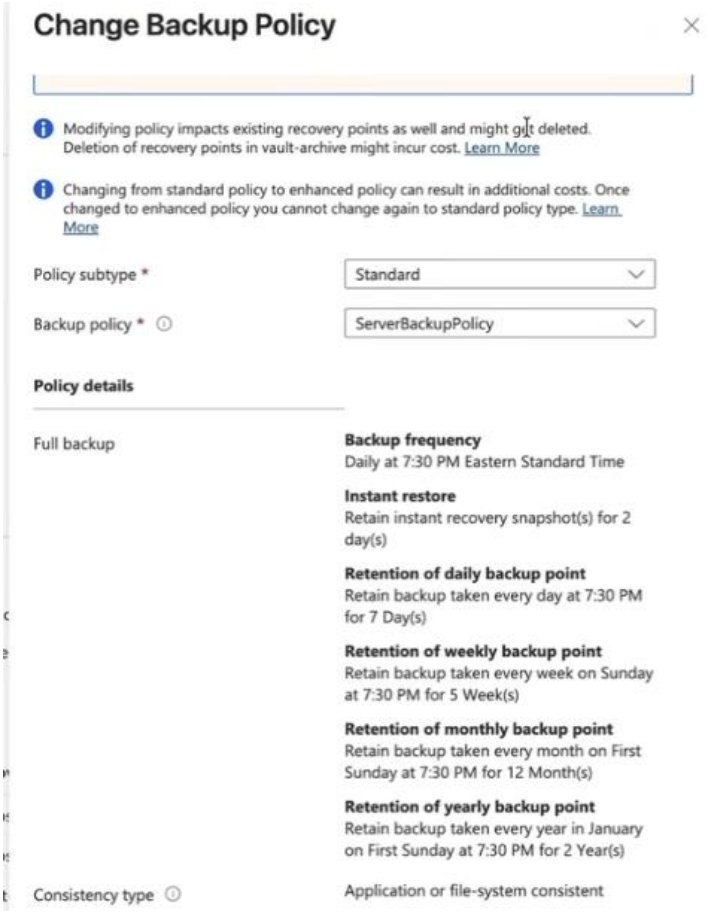
Hartford Network Diagram



Azure Diagram

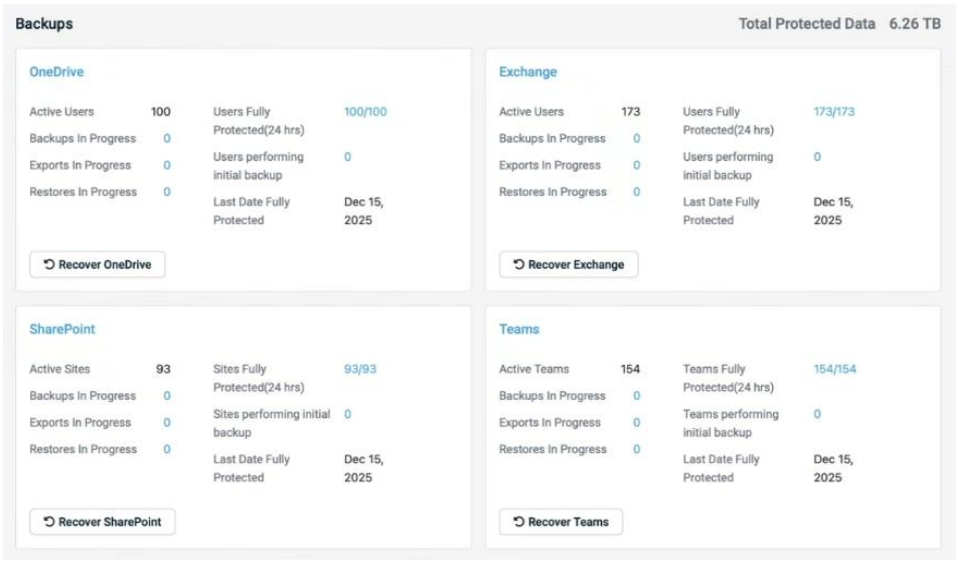


Azure Backup Strategy

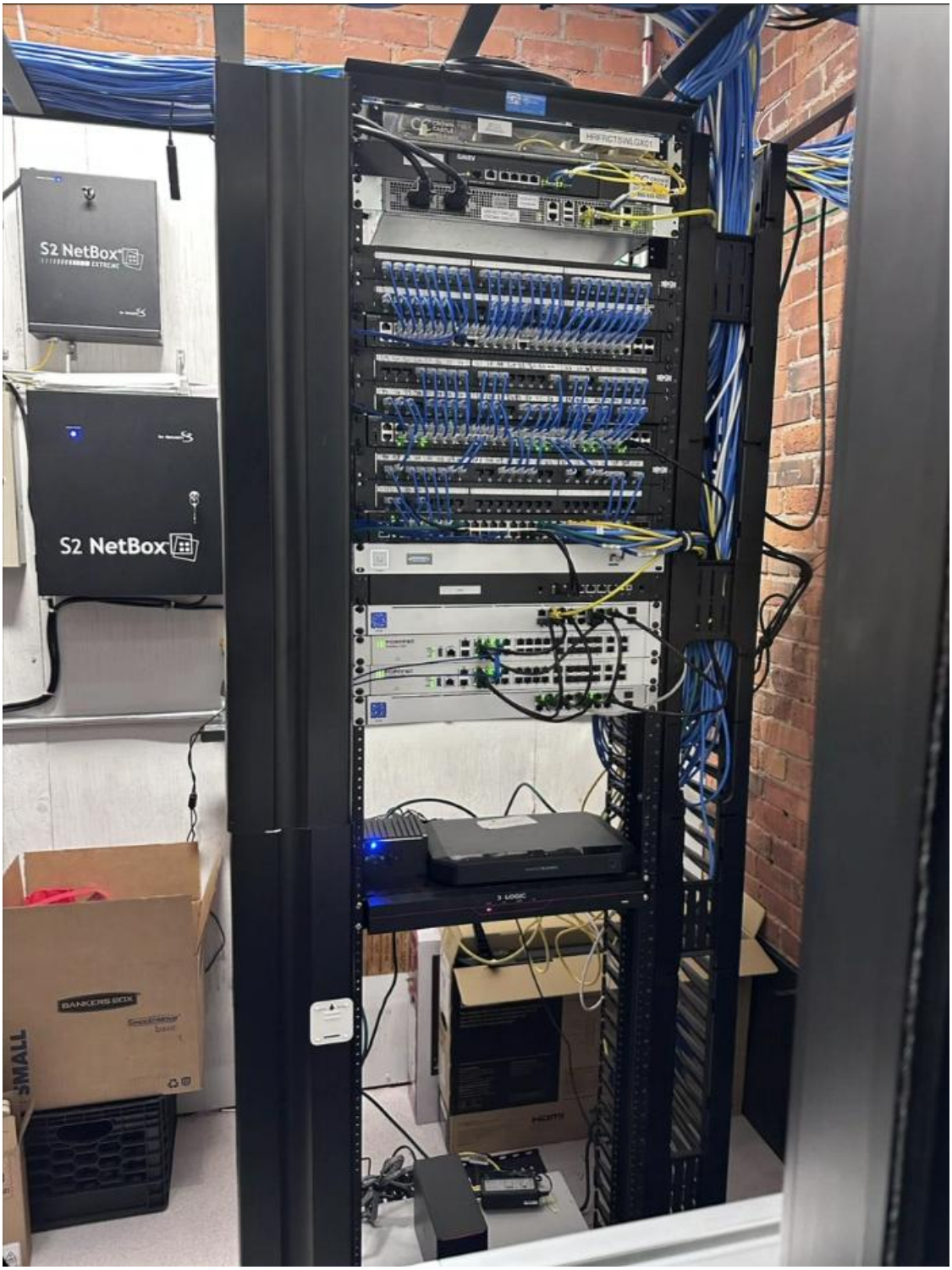


Microsoft 365 Policy

The standard Microsoft 365 backup policy is enabled.



IT Server Rooms – Hartford & Stamford



Hartford 1

Stamford 1

Appendix D: Incident Response Form

Reporting Individual	
Name:	**Job Title**:
Email:	**Phone**:
Incident Information	
Date Incident was Detected:	**Time Incident was Detected**:
Location of Incident:	**Type of Incident:**
How was the incident detected?	**Help Desk Ticket Number:**
Incident Description:	
When was it reported?	**How was it reported?**
Describe Initial Notifications: (BCDR/Incident Response Lead, BCDR/Incident Response Team, Crisis Management Team, Green Bank Senior Staff, HR, vendors, law enforcement, etc.)	
Initial Impact Assessment	
Describe Impact on Business:	
Severity: Low / Medium / High / Critical	**Actual Incident declared?** Yes / No

Describe Initial Actions Taken and Initial Communication (If a incident was NOT declared include reason and actions to resolve incident):		
Describe Declared Disaster Notifications		
Internal:	**Method:**	**Completed By:**
Vendors:	**Method:**	**Completed By:**
Customers:	**Method:**	**Completed By:**
Law Enforcement:	**Method:**	**Completed By:**
Property Management:	**Method:**	**Completed By:**
Insurance:	**Method:**	**Completed By:**
Other:	**Method:**	**Completed By:**
Damage Assessment		
Scope of the incident:		
Symptoms of the incident:		
Root cause of the incident:		
Affected systems:		
Affected assets:		
Affected accounts:		
Affected property:		
Affected documents:		
Describe digital data compromised:		
What regulations apply to the data breached?		
Was evidence gathered to support incident findings and mitigation activities?		
Financial Considerations:		

Legal Considerations:			
Recovery Strategy			
Was a top threat contingency plan activated? Yes / No			
Document the containment, response, eradication, and recovery actions taken below to address prioritized critical business functions.			
Recovery Action	**Date & Time**	**Performed By**	**Details**
Recovery Action	**Date & Time**	**Performed By**	**Details**
Date and Time Incident Mitigated:		**Date and Time Normal Business Operations Resumed:**	
Was the Recovery Time Objective (RTO) met?		**Was the Recovery Point Objective (RPO) met?**	

Were systems and business functions tested to confirm recovery?	**Was data integrity validated?**
Describe activities to resume normal business operations and confirm all information collected while working in recovery mode was securely updated in required systems:	
Incident Review	
Describe corrective actions needed to prevent similar incidents in the future:	
What precursors or indicators should be watched for in the future to detect similar incidents?	
What additional tools or resources are needed to detect, analyze, and mitigate future incidents?	
Was communication effective throughout the incident?	
What changes would you make to the recovery process to minimize risk and harm to the organization?	

What changes would you recommend improving the Business Continuity and Disaster Recovery Plan?
What changes would you recommend improving the Incident Response Plan?
Comments
Incident Status: Active / Closed

Appendix E: Contingency Plans for Top Threats

Contingency Plan for Technology Failures or SaaS Downtime

Risk Scenarios Covered

- Cloud service provider outage/SaaS downtime
- Email or telecommunications outage
- Hardware failure (critical infrastructure or assets)

Procedure

Detection and Initial Response

1. Green Bank employees become aware of a system, application, database, communications or hardware issue or monitoring alerts detect a failure or incident and notify an employee or third-party provider.
2. Green Bank employees and/or the third-party provider alert the BCDR Lead and Team.
3. The BCDR Team and system owners begin an initial investigation to identify the scope (impacted systems, accounts, data, locations, etc.) and impact of the incident.
4. The BCDR Team determines which vendors and employees need to be engaged, including if the Crisis Management Team needs to be notified.
5. The BCDR Team begins documenting the event in the Incident Response Form.
6. The BCDR Lead or designee may activate the plan and declare an incident. If the plan is activated, the BCDR Lead and Team will notify affected stakeholders.

Identify Alternate Operations, Contain Incident and Conduct Damage Assessment

1. The BCDR Team will work with system owners and related vendors to identify which business functions are impacted and determine alternate methods (manual or digital depending on the situation) of completing critical business processes until normal business operations can be resumed. While creating this plan, ensure confidential and nonpublic data remains secure.
2. The BCDR Team will work with software, communications or hardware vendors to further identify details about the incident, conduct a damage assessment and, if needed, contain the incident.
3. Update the Incident Response Form.
4. Provide the updated Incident Response Form to the Crisis Management Team if necessary so they can assess financial and legal implications of the incident.
5. Notify stakeholders of any additional information that would affect them that was obtained during this phase.

Recovery Strategy

1. Maintain contact with key vendors related to the outage to monitor their progress and estimated times for system availability and data recovery. Communicate important updates to affected stakeholders as they are received.
2. Determine a plan to validate data and test system functionality when the systems become available. Identify subject matter experts to engage in completing the activities in this plan.
3. Establish a plan to resume normal business operations after recovery. This should include how data from alternate operations during recovery gets securely updated in systems when they become available.
4. Once systems do become available:
    a. Validate user access
    b. Conduct a test of system functionality. Ensure critical business processes can be performed, and normal operations are restored. Communicate any issues with the system vendor and continue to work with them until a resolution is reached.
    c. Confirm integrations and automations are working as intended.
    d. Validate data to ensure there were no data integrity issues during the outage. Communicate any issues with the system vendor and continue to work with them until a resolution is reached.
    e. Securely update systems with data collected from alternate operations during recovery.
    f. Confirm all data and systems are updated and normal operations are in place.
    g. Notify Green Bank Senior Staff, employees and customers as necessary.
5. Monitor affected systems.
6. Complete the Incident Response Form as the above recovery strategy takes place. Once normal business operations are resumed, ensure the entire form is completed. Present to the BCDR Lead in the Incident Close Meeting for direction on any follow-up actions from the incident.
7. Close the incident if all systems are restored and validated and the Incident Close Meeting is performed.

Contingency Plan for Cybersecurity Incident

Risk Scenarios Covered

- Business email compromise
- Phishing or social engineering attack
- Ransomware
- Malware/virus outbreak
- Data breach

- Distributed denial of service attack
- Network intrusion
- Credential compromise
- Insider threat
- Compromise of third-party vendor

Procedure

Detection and Initial Response

1. Green Bank employees or IT vendor become aware of a system, application, database, communications or hardware issue or monitoring alerts detect a failure or incident and notify an employee or third-party provider.
2. Green Bank employees and/or the third-party provider alert the BCDR Lead and Team.
3. System owners will validate the accuracy of the alert and/or reported issue.
4. The BCDR Team and system owners begin an initial investigation to identify the scope (impacted systems, accounts, data, locations, etc.) and impact of the incident. *The Incident Response Plan is initiated*.
5. The BCDR Team determines which vendors and employees need to be engaged, including if the Crisis Management Team needs to be notified.
6. The BCDR Team begins documenting the event in the Incident Response Form.
7. The BCDR Lead or designee may activate the plan and declare an incident. If the plan is activated, the BCDR Lead and Team will notify affected stakeholders.

Identify Alternate Operations, Contain Incident and Conduct Damage Assessment

1. Identify which business functions are impacted and determine alternate methods (manual or digital depending on the situation) of completing critical business processes until normal business operations can be resumed. While creating this plan, ensure confidential and nonpublic data remains secure.
2. Work with software, communications or hardware vendors to further identify details about the incident, conduct a damage assessment and contain the incident (disconnect affected systems from the network, block malicious Ips, domains or credentials, disable compromised accounts, quarantine malware, etc.). Work to stop the damage while preserving evidence. Obtain evidence and save with incident documentation.
3. Update the Incident Response Form.
4. Provide the updated Incident Response Form to the Crisis Management Team if necessary so they can assess financial and legal implications of the incident.
5. Notify stakeholders of any additional information that would affect them that was obtained during this phase.

Recovery Strategy

1. Use the *Incident Response Plan* to implement the appropriate phases to recovery.
2. Depending on the situation, work to remove malware, malicious scripts, and backdoors, reset passwords, remove unauthorized accounts, reimage compromised systems, etc.
3. Maintain contact with key vendors related to the outage to monitor their progress and estimated times for system availability and data recovery. Communicate important updates to affected stakeholders as they are received.
4. Determine a plan to validate data and test system functionality when the systems become available. Identify subject matter experts to engage in completing the activities in this plan.
5. Establish a plan to resume normal business operations after recovery. This should include how data from alternate operations during recovery gets securely updated in systems when they become available.
6. Once systems do become available:
    a. Validate user access and system integrity
    b. Conduct a test of system functionality. Ensure critical business processes can be performed, and normal operations are restored. Communicate any issues with the system vendor and continue to work with them until a resolution is reached.
    c. Confirm integrations and automations are working as intended.
    d. Validate data to ensure there were no data integrity issues during the outage. Communicate any issues with the system vendor and continue to work with them until a resolution is reached.
    e. Securely update systems with data collected from alternate operations during recovery.
    f. Confirm all data and systems are updated and normal operations are in place.
    g. Notify Green Bank Senior Staff, employees and customers as necessary.
7. Monitor affected systems
8. Complete the Incident Response Form as the above recovery strategy takes place. Once normal business operations are resumed, ensure the entire form is completed. Present to the BCDR Lead in the Incident Close Meeting for direction on any follow-up actions from the incident.
9. Close the incident if all malicious activity is eradicated, systems are restored and validated and the Incident Close Meeting is performed.

Contingency Plan for Utility Failure

Risk Scenarios Covered

- Internet failure
- Electrical power failure
- Water service interruption

- HVAC or climate control failure
- Natural gas or heating failure
- Facility mechanical systems failure

Procedure

Detection and Initial Response

1. Green Bank employees become aware of a system, application, database, communications or hardware issue or monitoring alerts detect a failure or incident and notify an employee or third-party provider.
2. Green Bank employees and/or the third-party provider alert the BCDR Lead and Team.
3. Ensure all employees are safe and identify if an immediate evacuation needs to take place.
4. The BCDR Team begins an initial investigation to identify the scope (impacted systems, equipment, locations, etc.) and impact of the incident.
5. The BCDR Team will notify property management and determine which other utility providers, vendors and employees need to be engaged, including if the Crisis Management Team needs to be notified.
6. The BCDR Team begins documenting the event in the Incident Response Form.
7. The BCDR Lead or designee may activate the plan and declare a disaster. If the plan is activated, the BCDR Lead and Team will notify affected stakeholders.

Identify Alternate Operations, Contain Incident and Conduct Damage Assessment

1. Determine if employees need to work in the approved alternate work locations identified.
2. Determine if mobile hotspot or other options are available to access cloud-based systems, especially to perform critical business functions.
3. Identify which business functions are impacted and determine alternate methods (manual or digital depending on the situation) of completing critical business processes until normal business operations can be resumed. While creating this plan, ensure confidential and nonpublic data remains secure.
4. Work with software, communications or hardware vendors to further identify details about the incident, conduct a damage assessment and, if needed, contain the incident.
5. Update the Incident Response Form.
6. Provide the updated Incident Response Form to the Crisis Management Team if necessary so they can assess financial and legal implications of the incident.
7. Notify stakeholders of any additional information that would affect them that was obtained during this phase.

Recovery Strategy

1. If the building is unsafe for occupancy or the outage significantly affects the ability for employees to perform job functions, notify employees of the need to relocate to their approved alternate work locations.
2. Determine if failover to a secondary Internet Service Provider is required. If so, communicate and facilitate this implementation.
3. If certain systems are affected such as cooling or heating systems, work to shut them down to minimize damage.
4. If there is a power outage or climate control for critical infrastructure is impacted, work to shut down systems gracefully or shut down non-critical infrastructure to reduce the heat load. Maintain core services for as long as the uninterrupted power supply allows.
5. If utilities impact the fob system granting physical access, switch to mechanical processes or deploy door entry security personnel until the issue is addressed.
6. Reset breakers, alarms and mechanical systems as needed.
7. Maintain contact with key vendors related to the outage to monitor their progress and estimated times for system availability and data recovery. Communicate important updates to affected stakeholders as they are received.
8. Determine a plan to test system functionality when the systems become available.
9. Establish a plan to resume normal business operations after recovery. This should include how data from alternate operations during recovery gets securely updated in systems when they become available.
10. Once systems do become available:
    a. Securely update systems with data collected from alternate operations during recovery.
    b. Confirm all data and systems are updated and systems are operating as intended.
    c. Notify Green Bank employees, senior staff to resume to normal operations and report back to Green Bank facilities. Update any customers and vendors as necessary.
11. Monitor affected systems.
12. Complete the Incident Response Form as the above recovery strategy takes place. Once normal business operations are resumed, ensure the entire form is completed. Present to the BCDR Lead in the Incident Close Meeting for direction on any follow-up actions from the incident.
13. Close the incident if all systems are restored and validated and the Incident Close Meeting is performed.

Employee Handbook

Last Update: January 2026 ~~October 2025~~

Table of Contents

SECTION 1: INTRODUCTION

Employee Welcome

Welcome to the Connecticut Green Bank ("Green Bank")! We are pleased that you are joining our staff and embarking on a career with us. The Green Bank develops, invests in, and promotes clean sustainable energy sources for the benefit of Connecticut ratepayers. Our most important resource in achieving that vision is you – the employee. The staff at the Green Bank work together and depends upon one another to achieve our vision: a planet protected by the love of humanity. We want you to know how much we appreciate the contribution you are making to the continued successful operation of our agency.

This handbook was developed to describe some of the expectations of our employees and to outline the policies, programs, and benefits available to eligible employees. These policies and programs are general guidelines under continuous review and are subject to change or discontinuance at any time. All employees should familiarize themselves with the contents of this handbook, for it will answer many questions about employment at the Green Bank.

Please read your handbook carefully and keep it for further reference. Please contact Human Resources if you have any questions or concerns about the information set forth in this handbook. Again, welcome and we wish you the best in your career at the Green Bank.

Agency Purpose and Structure

The Green Bank was established by the Governor and Connecticut's General Assembly on July 1, 2011, through Public Act 11-80 as a quasi-public agency that superseded the former Connecticut Clean Energy Fund. As the nation's first "Green Bank", we leverage public and private funds to drive investment and scale-up clean energy and environmental infrastructure deployment in Connecticut. The Green Bank's statutory purposes are:

- To develop programs to finance and otherwise support clean energy investment in residential, municipal, small business, and larger commercial projects and such other programs as the Green Bank may determine.
- To support financing or other expenditures that promote investment in clean energy sources to foster the growth, development and commercialization of clean energy sources and related enterprises.
- To stimulate demand for clean energy and the deployment of clean energy sources within the state that serves end-use customers in the state.

The Green Bank's purposes are codified in Section 16-245n(d)(1) of the General Statutes of Connecticut and restated in the Green Bank's Board approved Resolution of Purposes.

Vision:
A planet protected by the love of humanity.

This statement was inspired by many people including Mary Evelyn Tucker of the Yale Divinity School, the late Mother Jennifer from the Daughters of Mary of the Immaculate Conception, and the late Maya Angelou, particularly her poem "On the Pulse of Morning." This poem speaks to the struggle for social and environmental justice and is as poignant today as it was when it was written. We cannot have environmentalism with humanitarianism.

Mission:
Confront climate change by increasing and accelerating investment into Connecticut's green economy to create more resilient, healthier, and equitable communities.

Goals:
To achieve its vision and mission, the Green Bank has established the following three goals:

1. To leverage limited public resources to scale-up and mobilize private capital investment in the green economy of Connecticut.
2. To strengthen Connecticut's communities, especially vulnerable communities, by making the benefits of the green economy inclusive and accessible to all individuals, families, and businesses.
3. To pursue investment strategies that advance market transformation in green investing while supporting the organization's pursuit of financial sustainability.

The vision, mission, and goals support the implementation of Connecticut's clean energy policies, be they statutorily required (e.g., CGS 16-245ff), planned (e.g., Comprehensive Energy Strategy), or regulatory in nature. For more information about the Green Bank, please visit www.ctgreenbank.com.

Objectives and Scope

This Employee Handbook has been prepared to acquaint you with policies and procedures relating to employment at the Green Bank and to provide a reasonable understanding of expectations so that staff may work together effectively. It is a guide to the Green Bank's policies, but it does not include every single policy. All employees are expected to be familiar with and abide by the policies in this Handbook.

This Handbook also provides information concerning Green Bank benefits. Please note that Green Bank benefit plans are defined in legal documents such as insurance contracts and official plan texts. This means that if a question ever arises about the nature and extent of plan benefits or if there is conflicting language, the formal language of the plan documents governs over the wording in this Handbook. Plan documents are available for inspection.

This Handbook is not, nor is it intended to be, an express or implied contract of employment, an agreement for employment for any specified period of time, or a guarantee of benefits or working conditions between an employee and the Green Bank. The Green Bank does not recognize any contract of employment unless it is documented in writing and signed by the employee and the President and CEO. The Green Bank reserves the right to unilaterally revise, delete, or add to the policies, procedures, and benefits within this handbook at any time with or without advance notice. Revisions of policies, procedures, and benefits may be made and applied immediately, prospectively, or, if not prohibited by law, made retroactively to a prior date. Additionally, the Green Bank reserves the right to make exceptions or vary from any of the rules, benefits, or policies contained in this handbook at its managerial discretion.

At Will Statement

Employment with the Green Bank is at will, which means that either party may terminate the relationship at any time and for any reason, with or without cause. No manager, supervisor, or other agent of the Green Bank has the authority to alter the at-will employment relationship by, for example, making a commitment, express or implied, of guaranteed or continued employment to any employee. An employee's at-will employment status can only be altered by a written contract of employment that is specific as to all material terms and is signed by both the employee and the President and CEO of the Green Bank.

Administration of Policy

The President and CEO has overall responsibility for directing the implementation and administration of policies and procedures. On a day-to-day basis, it is the responsibility of the

Vice President of Operations and each supervisor to administer all policies and procedures in a manner consistent with the handbook.

SECTION 2: EMPLOYMENT

Orientation

During your first few days of employment, you will participate in an orientation program conducted by Human Resources and various members of the Green Bank, including your supervisor. During this program, you will receive important information regarding the performance requirements of your position, basic company policies, your compensation, and benefit programs. You will be asked to complete all necessary paperwork at this time, such as medical benefit plan enrollment forms, beneficiary designation forms, and appropriate federal and state tax forms. You will be required to present the Green Bank with information establishing your identity and your eligibility to work in the United States in accordance with applicable federal law. During your first few weeks, you may be asked to prepare a short bio and be scheduled to have your photograph taken for inclusion on our website and in our annual report.

Please use this orientation program to familiarize yourself with the Green Bank and our policies and benefits. We encourage you to ask any questions you may have so that you will understand all the guidelines that affect and govern your employment relationship with us.

Status of Employment

Employees of the Green Bank are exempt from classified service as provided in Public Act 11-80 of the Connecticut General Statutes. Unlike employees in the classified service, Green Bank employees do not have tenure. Continued employment is predicated on satisfactory performance of duties, a satisfactory record of attendance, and appropriate conduct with the general public and other employees on the Green Bank staff as well as continued available work. All Green Bank employees are considered at-will employees.

Conditions of Employment

All new and rehired employees work on an introductory basis for the first six months after their date of hire. Acceptance as a regular employee of the Green Bank is contingent upon successful completion of this introductory period, which is intended to provide the employee the opportunity to demonstrate their ability to achieve a satisfactory level of performance and to determine whether the new position meets their expectations. The Green Bank uses this period to evaluate the capabilities, work habits, and overall performance of the new employee.

During the six-month introductory period, if an employee's performance is not satisfactory, the employee may be terminated or may be required to serve an extended introductory period. Any significant absence (in excess of five consecutive days) will automatically extend an introductory period by the length of the absence.

The existence of the introductory period as described above does not change an employee's at-will status. Employees and the Green Bank may terminate the employment relationship at any time and for any reason during and after the introductory period.

Additionally, when an employee is promoted or transferred to a new position within the Green Bank, they will be required to serve another six-month introductory period to assess their job performance in the new position. Benefits, eligibility, and employment status are not changed during a secondary introductory period.

Staff Relations

The Green Bank's success depends on its employees' skills and abilities and the manner in which they are used to meet our goals. Our employees are our most important resource to help us succeed. The Green Bank is committed to free and open communication. Usually, it is the

employees performing the work who have the most knowledge about the tasks and processes they use. We encourage employees to help us by taking every opportunity to make us aware of problems of any kind and suggesting ways we can improve. Employees should feel free to discuss any concern or suggestions they have with their supervisor or any member of management. It is our intent that as a result of open communication, the Green Bank and all of its employees will enjoy a mutually prosperous and satisfying relationship.

Our experience has shown that when employees deal openly and directly with supervisors, the work environment can be excellent, communications can be clear, and attitudes can be positive. When you have a suggestion, question, problem, or concern, your supervisor is in the best position to respond quickly and accurately; however, you should feel free to discuss the issue with the staff in Human Resources.

The working environment at the Green Bank is one that puts staff, supervisors, and administration in a close relationship of mutual respect. Attendance at and participation in group meetings and staff meetings is important. Employees are encouraged and expected to use these meetings as opportunities for raising issues to improve client services, program operation, and staff relations. It is generally during these meetings that most business-related matters are communicated. If an employee is absent from any of these meetings, it is their responsibility to catch up with the business discussed.

Customer Service Deliverables

Customer service is a priority at the Green Bank. We all have internal and external customers. To that end, we expect each one of our employees to be accountable for the following customer deliverables:

- To respond promptly to customer requests for information or assistance.
- To act as a member of the Green Bank team and pitch in and assist other staff members as requested.
- To provide a work product that is complete, well-organized, and useful to the customer.

Equal Employment Opportunity

In order to provide equal employment and advancement opportunities to all individuals, employment decisions at the Green Bank will be based on merit, qualifications, abilities in relation to the staffing requirements, and business needs. The Green Bank is an equal opportunity employer and does not discriminate in employment opportunities or practices on the basis of race, color, religious creed, sex, marital status, national origin, age, ancestry, mental retardation, physical or learning disability, past or present history of mental disorder, sexual orientation, special disabled veterans or veterans of the Vietnam War status, or any other legally protected status, except in those cases where there is a legitimate, compelling and documented occupational qualification that precludes the hiring or promotion of individuals in any of these protected groups. The Green Bank will make reasonable accommodations for qualified individuals with known disabilities unless doing so would result in an undue hardship to the Green Bank. This equal opportunity policy extends to all aspects of the employment relationship, including recruitment, hiring, training, compensation, promotions/transfers, job assignments, discipline, and termination. All other policies, such as employee benefits, are also administered based on fair and equal treatment.

Any employees with questions or concerns about any type of discrimination in the workplace are encouraged to bring these issues to the attention of their immediate supervisor or Human Resources. Employees can raise concerns and make reports without fear of reprisal, either verbally or through the grievance procedure. Anyone engaging in any type of unlawful

discrimination will be subject to disciplinary action, up to and including termination of employment.

Disability Policy (ADA)

As an employer, the Green Bank will not discriminate against any employee or person seeking employment on the basis of a disability, in compliance with the spirit and regulations of the Americans with Disabilities Act (ADA) and all applicable Connecticut laws. The purpose of the ADA is to assure that individuals with covered disabilities who are able to perform the essential duties of their job, with or without reasonable accommodation, are given equal opportunity and treatment by their employer and fellow employees. If a qualified employee or employee candidate has an ADA recognized disability; they cannot be denied equal opportunity for employment.

In accordance with the ADA, the Green Bank does not discriminate on the basis of disability in the administration of or access to its programs, services, or activities, and is committed to equal employment opportunity for employees and job applicants with disabilities. Employees who violate the ADA by discriminating against an individual with an ADA recognized disability would be subject to disciplinary action up to and including dismissal. Rumors and gossip regarding any employee who has an ADA recognized disease or is assumed to have an ADA recognized disease would not be tolerated under any circumstances. Employees who need a reasonable accommodation must request such accommodations through their supervisor. Employees may be required to submit medical documentation to support their request.

Immigration Law Compliance

All job offers extended to successful candidates are contingent upon the receipt of the required documentation and completion of INS Form I-9.

Only those successful applicants who provide the required documentation and complete Form I-9 will be permitted to begin work.

Former employees who are rehired must also complete the form if they have not completed a Form I-9 with the Green Bank within the past three years, or if their previous Form I-9 is no longer available or valid.

Conflict of Interest

This policy establishes the general framework within which the Green Bank wishes the business to operate.

Employees have an obligation to conduct business within guidelines that prohibit actual or potential conflicts of interest and should not have a financial interest in any client. A conflict of interest may exist when the interests or concerns of any director, officer, staff, client, or said person's relatives, or any party, group, or organization in which said person has an interest or concern, may be seen as competing or conflicting with the interests or concerns of the Green Bank. No "presumption of guilt" is created by the mere existence of a relationship with outside firms.

The employee concerned must disclose any possible conflict of interest to the President and CEO. If it is not clear to the employee whether a particular situation or relationship constitutes a conflict of interest, the employee should contact the President and CEO.

When a conflict of interest exists regarding any matter requiring action by the Board of Directors, the President and CEO shall call it to the attention of the Board of Directors (or its committee).

Outside Employment

Employees may hold a job with another company as long as they satisfactorily perform their job responsibilities with the Green Bank. Employees who have additional outside employment for which they receive pay must keep their supervisor and the Human Resources Manager informed of such employment. This outside employment must not interfere with the employee's effectiveness in performing their job responsibilities and must not conflict with the Green Bank's public image. All employees will be judged by the same performance standards and will be subject to the Green Bank's scheduling demands, despite any existing outside work requirements.

If the President and CEO and/or their designee decides that an employee's outside work interferes with performance or the ability to meet the requirements of the Green Bank as they are modified from time to time, the employee may be asked to terminate the outside employment if they wish to remain with the Green Bank. Inappropriate behavior believed to be a result of outside employment (abuse of sick time, refusal of overtime, unsatisfactory performance, etc.) will be addressed through normal performance management and/or disciplinary procedures.

Outside employment will present a conflict of interest if it has an adverse impact on the Green Bank. Employees with outside employment must abide by the confidentiality standards that protect the Green Bank's clients.

Employment of Relatives

The Green Bank is committed to the objective treatment of all employees based upon their job performance and the operational needs of the Green Bank. The employment of relatives may cause serious conflicts and problems with favoritism and employee morale. In addition, real or apparent partiality in treatment at work and personal conflicts from outside the work environment can be carried into day-to-day working relationships. Therefore, it is the policy of the Green Bank that relatives of employees will not be considered for employment.

If the relative relationship is established after employment, and there will be a direct reporting relationship or the related individuals will be working within the same department, the parties may be separated by reassignment or termination, if it is deemed necessary by the Human Resources Department and/or the President and CEO and/or their designee.

A relative is any person who is related by blood or marriage, or whose relationship with the employee is similar to that of persons who are related by blood or marriage.

Confidential Nature of Work

The protection of confidential information and trade secrets, as defined below, is vital to the interest and the success of the Green Bank. The improper disclosure of confidential information would harm the Green Bank and/or its employee or clients if such information were improperly disclosed to third parties. Accordingly, employees may not at any time during and after termination of employment with the Green Bank, use for any purpose or disclose any confidential information to any third person or party, except as specifically authorized in the course of employment and required for carrying out job duties.

Confidential information includes, but is not limited to, the following examples:

- Any work performed by Green Bank employees for a client, portfolio company, or applicant.
- Any client, portfolio company or applicant information.
- Compensation data, including salary information.
- Personnel information.
- Financial information.
- Pending projects and proposals.
- Any other information not subject to the State Freedom of Information Act.

Confidential information should not be discussed with others (including family and friends), nor should employees discuss office matters or the affairs of clients, portfolio companies, or applicants generally with each other outside the office or any place where they might be overheard, e.g., on the street, in elevators or elevator lobbies, or at lunch counters. Except when they are certain that it is proper to do so, employees are cautioned against disclosing to callers anything being undertaken by the Green Bank or its employees, clients, companies, or applicants. Likewise, it is important not to leave confidential information on desks at the end of the day or while a visitor is in the office which would allow easy unauthorized access to such information.

Upon termination of employment with the Green Bank or whenever requested by the Green Bank, employees must promptly deliver to the Green Bank all work product and all documents and other tangible embodiments of the confidential information, and any copies thereof.

The best way to adhere to this policy is to not disclose any information if you are not sure whether such information is confidential information of the Green Bank. Also, if you have any question as to whether certain information is considered confidential, please consult your department manager.

Violations of this policy may provide grounds for legal action against an employee and may result in disciplinary action up to and including termination, even if the employee does not actually benefit from the disclosed information.

Categories of Employment

It is the intent of the Green Bank to clarify the definitions of employment classifications, so those employees understand their employment status and benefit eligibility.

Full-Time Regular Employees

Employees who are not in a temporary or introductory status and who are regularly scheduled to work a minimum of 40 hours per week are considered full-time regular employees. Full-time regular employees are eligible for Green Bank benefits, subject to the terms, conditions, and limitations of each benefit program. Such employees must have successfully completed the six-month introductory period.

Part-Time Regular Employees

Employees who are not assigned to a temporary or introductory status and who are regularly scheduled to work less than 40 hours per week are considered part-time regular employees. Part-time regular employees receive all legally mandated benefits (such as Social Security and Workers' Compensation Insurance). Part-time employees who work at least 20 hours per week are generally eligible for other Green Bank benefit programs on a prorated basis, based on the ratio of their standard hours of work per week to the full-time standard for that position. Such employees must have successfully completed the six-month introductory period.

Exempt Employees

Exempt employees will not receive any overtime pay. Exempt employees may be granted compensatory time at the discretion of the President and CEO and/or their designee in accordance with the compensatory time policy outlined in Section 4.

Non-Exempt Employees

Non-exempt employees are paid based on the number of hours actually worked and are eligible for overtime pay. Overtime pay will be paid at the rate of one and one-half times (1½) the non-exempt employee's regular rate of pay for all time worked in excess of 40 hours per week. Overtime pay is based on actual hours worked. Thus, if a non-exempt employee is absent during a week when overtime hours have occurred, the absent hours reported will not be considered hours worked in determining a time and one-half overtime payment. An accurate record of non-exempt regular and overtime hours must be maintained for purposes of pay. Time sheets are to be signed by the staff member and by their supervisor, then submitted to Human Resources for processing.

Introductory Employees

Employees who work on an introductory basis as specified in the "Conditions of Employment" are considered introductory employees. Introductory employees who satisfactorily complete the six-month introductory period will be notified of their new employment classification. Any significant absence will automatically extend the introductory period by the length of the absence. If an employee changes jobs during the introductory period, a new six-month introductory period shall begin.

Temporary Employees

Employees who are hired as interim replacements to temporarily supplement the work force or to assist in the completion of a specific project are considered temporary employees. Temporary employees hired from temporary agencies for specific assignments are employees of their respective agencies and not the Green Bank. Employment assignments in this category are of a limited duration. Employment beyond any initially stated period does not in any way imply a change in employment status.

Consultants

Those independent contractors who are on contract to provide services to the Green Bank. Persons in this category are not Green Bank employees.

Selection Process, Interviewing and Hiring

The President and CEO and/or their designee must approve all new positions or changes to existing position descriptions. Vacant positions to be filled may be posted internally and, if necessary, posted externally. The immediate supervisor, the President and CEO, any manager or director within the Green Bank, and/or any person the President and CEO designates, may be involved in the interview selection process. The President and CEO has the ultimate responsibility for appointing the candidate to the position.

The Green Bank, through the actions and approval of the President and CEO, reserves the right to transfer or reclassify positions and employees within the Green Bank and restructure their job duties and position without going through the above public process when it is in the best interest of the Green Bank.

Promotion Policy

The Green Bank is committed to providing employees with opportunities for career advancement. Employees may apply for posted positions for which they are qualified, provided any such position represents a promotion or advancement.

The Green Bank is committed to implementing a fair and equitable "in-house" promotion policy that will aid in the development of staff to their fullest potential. Full and equal opportunity will be extended to all employees in accordance with the Green Bank's affirmative action plan.

There is an established career path for most positions within the Green Bank. The career path progression for each position can be found in the job description for that position. If an employee is being promoted within the established career path and within their department, such promotion can be made without posting the position. A current employee shall be eligible for reclassification or promotion to an existing or new position only if such employee has at least six months of service with the Green Bank and meets the minimum qualifications for such position.

If the position is not within the established career path progression, the position will be posted, and the selection process outlined above will be followed.

Employment Applications

The Green Bank relies upon the accuracy of information contained in the employment application, as well as the accuracy of other data presented through the hiring process and employment. Any misrepresentations, falsifications, or material omissions in any of this information or data may result in the Green Bank's exclusion of the individual from further consideration for employment or, if the person has been hired, termination of employment.

Employment Reference Checks

The Green Bank wishes to ensure that applicants are qualified and have a strong potential to be productive and successful. It is the policy of the Green Bank to check the employment references of all applicants, and no offer of employment can be made until Human Resources has received satisfactory reference checks.

Human Resources will respond to all reference check inquiries from other employers only with the approval of the employee or past employee and in accordance with applicable law.

Performance Management and Review

The Green Bank has a performance management and review process. The objectives of this process are to:

- Provide clear communication between the supervisor and employee.
- Identify the employee's work objectives and expected results.
- Identify the employee's performance strengths and weaknesses.
- Assess the need for training.
- Aid in decisions about future work assignments.
- Determine the employee's suitability for continued employment.
- Determine the employee's eligibility to receive a merit compensation award.

The Green Bank believes that all employees should receive prompt, thorough feedback regarding their performance. Formal performance assessments for new hires and newly promoted employees are conducted at the completion of their six-month introductory employment period. Once an employee has received the performance assessment of their

introductory employment period, formal written performance appraisals are conducted annually. Performance evaluations provide employees with the opportunity to express any concerns they have about their jobs, career aspirations, and future with the Green Bank. If an employee is having difficulty in their job, interim evaluations may be conducted to help the employee understand what performance improvements are needed.

All performance assessments are reviewed by the appropriate department head, the President and CEO and/or their designee, and Human Resources.

Personnel Files

The Green Bank maintains a confidential personnel file on each employee. The personnel file includes such information as the employee's job application, resume, records of training, documentation of performance appraisals and salary increases, written warnings or reprimands, and written commendations. Personnel files are the property of the Green Bank, and access to the information they contain is restricted. Generally, only supervisors and management personnel of the Green Bank who have a legitimate reason to review information in a file are allowed to do so unless otherwise required by law.

Employees will be notified when information is added to their personnel file.

Employees who wish to review their own files should contact Human Resources. With reasonable advance notice, employees may review their own personnel file in the Human Resources Office in the presence of a Human Resources employee.

Updating Personnel Records

Employees must notify Human Resources of any changes in personal mailing addresses, telephone numbers, number and names of dependents, individuals to be contacted in the event of an emergency, etc.

It is the responsibility of each individual employee to promptly notify the Green Bank of any such changes in personnel status.

It is also the responsibility of each individual employee to review bi-weekly payroll deductions (tax withholding, FICA, etc.) for accuracy and report any errors promptly to Human Resources.

SECTION 3: WAGES AND SALARY ADMINISTRATION

General Policy

It is the policy of the Green Bank to maintain a fair compensation program that provides equitable payment for work performed, is competitive with the identified labor market, and ensures compliance with federal and state legislation.

A salary range has been assigned to each position. The compensation for each employee shall be within the minimum and maximum of the range established for the grade to which the position has been assigned. In rare instances, the President and CEO may approve a salary outside the range for a specific position. Periodically, the Green Bank may revise job descriptions, evaluate individual jobs to ensure they are being compensated appropriately, and review job specifications as business needs dictate. Salary ranges may also be adjusted for annual inflation at the discretion of the Board of Director's Budget, Operations, and Compensation Committee.

Hours of Work

The standard workweek for full-time regular employees is currently a minimum of 40 hours. Regular daily work hours are from 8:00 a.m. to 5:00 p.m. Monday through Friday. Where workload or schedules require, some departments may operate outside these regular hours. Supervisors should notify employees of their work schedule. Each employee is responsible for informing Human Resources of any permanent change in their usual work hours.

Flexible Time

Under the flextime policy, an employee may be permitted to start and end the workday at times that differ from the standard hours of operation.

Flextime schedules are at the discretion of management and must be approved in advance by the employee's supervisor and the Department Head.

Employees participating in flextime must have regular daily starting and quitting times that do not vary from day to day. All full-time regular employees must be at work during the core hours of 9:00 a.m. to 3:30 p.m. No flextime schedules shall begin before 7:00 a.m. or end later than 6:00 p.m.

All employees participating in flextime must work their full scheduled hours per day and take at least a one half-hour lunch break.

Pay Periods

Staff members are paid on a bi-weekly basis. Each paycheck will include earnings for all work performed through the end of the previous payroll. Thus, a new employee can expect to receive their paycheck up to four weeks from the first day they commenced work for the Green Bank. Employees may have pay directly deposited into their bank accounts if they provide advance written authorization. Direct deposit applications may be obtained from Human Resources.

Employees will receive an itemized statement of wages for each pay period. For those employees not participating in Direct Deposit, paychecks will be distributed directly to the staff member after 3:00 p.m. every other Thursday. All paychecks not distributed by the end of the business day will be returned to Human Resources. If a staff member is absent from work and desires other arrangements to receive their paycheck, they will have to contact Human Resources directly to make such arrangements.

Lunch Periods

Employees are generally entitled to a one (1) hour lunch period. All employees must take a minimum of a half-hour for lunch. Scheduling of lunch periods is between the hours of 12:00 P.M. and 2:00 P.M. Lunch hours should be scheduled so that there is coverage at all times and employees who work in tandem with other employees should coordinate the schedule of their lunch hours. If employees must attend to personal business during the workday, they should do so during their scheduled lunch break period. Employees should not work through their lunch period in order to leave early without prior authorization from their supervisor.

Time Sheets

The Green Bank participates in self-service time reporting to the State of Connecticut's payroll system, Core-CT. Accurately recording time worked is the responsibility of every employee. Time worked is all the time actually spent on the job performing assigned duties. Time sheets must be accurately filled out in accordance with Core-CT time reporting guidelines and approved by the supervisor. Each employee shall personally record their own time, which includes the time they begin and end work and any time that is charged against their leave balances (personal time, vacation time, sick time, etc.). Altering, falsifying, tampering with time records, or recording time on another employee's time sheet may result in disciplinary action, up to and including termination of employment.

Employee time sheets for each two-week pay period must be completed in Core-CT by noon on the Friday after the pay period. All time sheets must be approved and initialed by the employee's supervisor, including any corrections and backup. Working time is logged in 15 minutes increments. Non-exempt employees, who report to work more than seven minutes late, but less than 15 minutes, must log their starting time at 15 minutes after the normal starting time. Time lost due to reporting to work late may not be made up by staying late at the end of the day or working through lunch periods, unless the employee obtains the prior authorization of their supervisor.

Attendance and Punctuality

The ability of the Green Bank to operate smoothly and efficiently depends on regular attendance and punctuality. Absenteeism and tardiness are disruptive and place a burden on other employees. To maintain a productive work environment, the Green Bank expects employees to be consistently reliable and punctual in reporting for work.

In the rare instances when employees cannot avoid being late to work or are unable to work as scheduled, they should personally notify their supervisor before the anticipated tardiness or absence. If the supervisor is not available, employees should notify the Human Resources Manager so that they can arrange for coverage during the absence. Employees should also inform their supervisor or the Human Resources Manager of the reason for their tardiness or absence. In case of an emergency where advance notification is not possible, employees must report the absence or tardiness as soon as possible.

An employee's supervisor is responsible for monitoring an employee's attendance. The supervisor should deal with abuses of reporting time. Occurrences of abuse should result in counseling of the employee by the supervisor. Supervisors and Human Resources will monitor unscheduled occasions of absence and Human Resources will determine the action to be taken upon the accumulation of a certain number of unscheduled occasions of absence within a given time period, taking into consideration the following:

- Numbers of days taken.
- The number of unscheduled occasions of absence.
- The pattern of absences.

- The employee's past records.
- The reasons for the unscheduled occasions of absence.

Although the specific action taken in each instance will be determined by Human Resources in its discretion, the chart below illustrates the actions likely to be taken upon the accumulation of a certain number of unscheduled occasions of absence within a given time period.

Number of Occasions	Within this Time Period	Action Likely to Be Taken
3	3 months	Your attendance record will be reviewed with you to determine contributing problems and possible solutions.
5	6 months	Your attendance record will be reviewed with you to determine contributing problems and possible solutions AND this counseling session will be recorded in a written memo, a copy of which will be maintained in your personnel file.
9	12 months	Your attendance record will be reviewed with you to determine contributing problems and possible solutions AND this discussion will be documented and a copy will be maintained in your personnel file. An "Unsatisfactory" or "Below Threshold" performance appraisal will be given to you for unsatisfactory attendance and dependability unless you give your supervisor documentation explaining the occasions to their satisfaction. You will also be notified that receiving two "Unsatisfactory" or "Below Threshold" performance appraisals in a row (for poor attendance or any other reason) is just cause for dismissal.

Poor attendance and excessive tardiness, including failing to report the same in a timely manner, may lead to disciplinary action, up to and including termination of employment. For example, an employee who does not report to work and who has not notified their supervisor of this absence may be terminated unless an acceptable explanation is provided for both the absence and the failure to report.

Absence from the Office

If an employee must be out of the office for business or personal matters, the supervisor must be advised and a formal request should be submitted via SharePoint. The employee also should make every attempt to keep their schedule up to date on their Outlook Calendar. If the supervisor is not available, the appropriate department head or the President and CEO and/or their designee should be notified. Employees who are working outside the office at meetings or other events should leave a telephone number where they can be reached. These employees are also responsible for checking in and receiving messages.

Procedures for Absences from the office

1. Pre-schedule all vacation time use. Vacation leave shall be requested as far in advance as possible and is subject to the Green Bank's operating needs.
2. Pre-schedule all absences, if possible. You should attempt to schedule all absences (including late arrivals and early departures) in advance with your supervisor. Pre-scheduled and approved use of sick and other types of leave, such as vacation, a doctor's visit, or a funeral, will not be counted as an unscheduled occasion of absence.
3. Unscheduled absences. If it is not possible to pre-schedule an absence (including a late arrival or early departure), you must:
    - notify your supervisor within a ½ hour of the start of the workday.
    - give the reason for the absence.
    - give an estimate of how long the absence will be.

    If the absence is continuous or lengthy, notify your supervisor on a daily basis, or as otherwise required by your supervisor.
4. Exhaustion of sick leave accruals. If you are absent because of illness or injury, but have exhausted your sick leave accruals, you must:
    - For each absence, have your physician complete a state medical certificate form explaining the reason for your absence, and submit the completed form to Human Resources.
    - If you wish to use other accrued leave in place of your exhausted sick leave, you must make such a request in writing and submit it to your supervisor or to Human Resources with the completed medical certificate form.
    - If you fail to follow this procedure, you will be charged with an unscheduled occasion of absence and unauthorized leave for the day.
    - If you have exhausted all other accrued leave time in addition to your sick leave time, you will be charged with unauthorized leave for the day.
5. Extended Leaves. If you will be absent for an extended period of time because you are sick or injured, you must:
    - Obtain a medical certificate form from Human Resources.
    - Have the form completed by the treating physician stating the reason for the absence and your anticipated return to work date.
    - Return the form to Human Resources at the time you return to work.

Telecommuting

To attract and retain the best workforce to accomplish the mission of Connecticut Green Bank, we offer the option for employees to telecommute. Telecommuting is a management option that allows an employee to work at home or an alternate work site; it is not an employee entitlement. The purpose of telecommuting as outlined in Connecticut General Statute 5-248i(a)[1] is to: (1) increase worker efficiency and productivity; (2) benefit the environment; and (3) reduce traffic congestion. Telecommuting does not change the hours of work. An employee may be considered for this option when the following minimum criteria are met:

1. The employee has requested to telecommute by completing a telecommuting agreement on SharePoint which will outline the terms and conditions of their telecommuting arrangement.
2. Green Bank has determined that the employee's job can be readily and effectively completed at an alternate site.
3. Green Bank determines that the employee's absence from the office is not detrimental to office operations, overall productivity, the working conditions of other employees, or services to clients and customers.

[1] https://www.cga.ct.gov/current/pub/chap_067.htm#sec_5-248i

4. The employee's performance has been satisfactory or better.
5. The employee agrees to abide by the guidelines of the Telecommuting Policy outlined in their telecommuting agreement.

The Green Bank provides a flexible and customized telecommuting option for all its employees. The general guidelines are as follows:

- A request to telecommute one or two days a week or for inclement weather is automatically approved
- Telecommuting days do not have to be consistent every week, and the employee is responsible for identifying the days they are working remotely on their Outlook calendar.
- You are responsible for remaining logged into Microsoft Teams when telecommuting and coming into the office as needed for meetings, seminars, etc.

The Green Bank provides a flexible and customized telecommuting option for all its employees. Positions are placed within the following four (4) categories based on the discretion of the President and CEO, Vice President of Operations, and Human Resources:

- **Category 1**: Essential In-Office
- **Category 2**: Workplace Flexibility
- **Category 3**: Hybrid Workplace
- **Category 4**: Part-Time

Category 1: Essential In-Office:
This category applies to employees whose job responsibilities are focused on in-office activities. Employees must be in the Green Bank office at least three (3) days per workweek and up to two (2) days can be remote.

Category 2: Workplace Flexibility:
This category applies to employees whose job responsibilities require frequent in-person meetings and events throughout Connecticut. Employees must be in the Green Bank office at least two (2) days per workweek and up to three (3) days can be remote.

Category 3: Hybrid Workplace:
This category applies to employees whose primary residence is greater than 60 miles from the employee's assigned Green Bank office (Hartford or Stamford) and whose position is deemed eligible for greater than standard workplace flexibility. Employees must come to the Green Bank office at least 20% (i.e., 45 business days) of a year to remain in compliance with this policy. Travel to and lodging in Connecticut are not reimbursable except for when on official Green Bank business (e.g., conferences, meetings, etc.) per the Green Bank's Expense Reporting Policy. Employees must maintain an average score of Meets+ (i.e., 4) or better on their most recent performance appraisal to remain eligible for this option. **This category can be applied on an exception basis based on business need. No more than 15% of the Green Bank's workforce can be designated to this category at a given time.**

Category 4: Part-Time:
This category applies to positions which have been deemed necessary only a part-time basis. Employees in this category must work a minimum of 20 hours per week and no more than 32 hours per week. Part-time employees may not be required to report in-person to a Green Bank office unless otherwise agreed to with their manager.

	Category 1: Essential In-Office	**Category 2: Workplace Flexibility**	**Category 3: Hybrid Workplace**	**Category 4: Part-Time**
Days in Office per Workweek	3	2	45 days per year	0
Travel & Lodging Reimbursable for Regular Business	No	No	No	Yes, as required and pre-approved by manager
Travel & Lodging Reimbursable for Meetings, Events, Conferences, etc.	Yes	Yes	Yes	Yes, as required and pre-approved by manager
Eligible for Director-Level	Yes	Yes	Yes	Yes
Eligible for Senior Staff	Yes	Yes	Yes, based on position[2]	No

Additional details on these categories are available through Human Resources.

Overtime and Overtime Pay

Under the federal Fair Labor Standards Act (FLSA), employees who are covered by FLSA shall be paid time-and-one-half for all hours worked in excess of 40 hours per week. Each position at the Green Bank is determined to be exempt or non-exempt in consultation with the President and CEO, Operations staff, and the Green Bank's attorneys. Exempt employees will not receive any overtime pay. Non-exempt employees are paid based on the number of hours actually worked and are eligible for overtime pay based on actual hours worked. Thus, if a non-exempt employee is absent during a week when overtime hours have occurred, the absent hours reported will not be considered hours worked in determining overtime payment. An accurate record of non-exempt regular and overtime hours must be maintained for purposes of pay. Time sheets are to be submitted by the staff member and reviewed and approved by their supervisor through Core-CT for processing.

Merit Compensation

On an annual basis, the President and CEO may recommend for approval by the Board of Directors an allocation of funds for merit compensation increases for the staff. A maximum percentage salary increase will be set by the President and CEO for those employees with exceptional performance evaluations. Employees shall be compensated according to job performance as determined through the performance management process as administered by the Green Bank.

[2] Director-level or higher positions leading programs that are outlined within the Green Bank's Comprehensive Plan are not eligible for Senior Staff under Category 3: Hybrid Workplace.

SECTION 4: TYPES OF LEAVE

Vacation Policy

Regular full-time employees will accrue and must use vacation time in accordance with the following schedule:

Years of Service	Vacation Earned	Must Use Annually
0 - 2 years	15 days per year	10 days
2 - 10 years	20 days per year	15 days
Over 10 years	25 days per year	20 days

Vacation time is paid at the employee's base pay rate. The maximum number of vacation days an employee will be eligible to earn annually will be 25 days. Generally, an employee may not take more than four (4) consecutive weeks at one time in one year. Under extraordinary circumstances, the President and CEO and/or their designee may grant exceptions.

All employees will be limited to a maximum carryover annually of 5 days (40 hours) of vacation time accrued during the calendar year. In extraordinary circumstances, such as unusual work circumstances, deadlines, or demands, the President and CEO may increase the allowable annual carryover to ten (10) days. The additional time that is carried over must be used during the next calendar year, in addition to all other vacation time required to be used during that calendar year as outlined in the grid above.

Maximum Aggregate Carryover

The maximum aggregate vacation balance permitted to be carried into a new calendar year for employees hired after January 1, 1998, including all vacation hours previously accrued shall be 30 days (240 hours). With approval, the President and CEO may allow a one-time exception to carryover vacation in excess of 30 days (240 hours) into a new calendar year. If the exception is granted, the employee's vacation balance must be at 30 days (240 hours) by December 31st of the new calendar year. Vacation accruals above this amount will be automatically reduced to the maximum aggregate carryover of 30 days/240 hours and all unused vacation time over 30 days (240 hours) will be forfeited.

Employees will be allowed to accrue more than this amount during a given year, however, tThe maximum aggregate accrual for which an employee will be compensated upon separation is 240 hours. In the event of an involuntary termination where the employee is not given the opportunity to utilize their vacation balance over 240 hours prior to separation, the effective date of the termination will be adjusted to incorporate the employee's unused vacation time over 240 hours and the employee will be paid out in a lump sum for the remaining balance of 240 hours.

Maximum Vacation Hours Paid Out Due to Termination/Resignation

The maximum number of vacation days/hours to be paid upon termination/resignation for employees hired after January 1, 1998 shall be 30 days/240 hours. The maximum for employees hired prior to January 1, 1998 shall be 120 days/960 hours.

Advancing Vacation Time

Vacation time will not be advanced under any circumstances. If an employee wishes to take vacation time, but does not have accrued time available, they may request to take unpaid leave. Such leave may be granted at the discretion of the employee's supervisor and or/ the department head.

*Note – Once an employee is at the maximum vacation balance of 30 days, they must utilize all of their annual accruals or forfeit them.

Accrual Period

Vacation days are accrued and credited on a monthly basis and can be taken when earned. Employees begin to accrue vacation days the first full month after their date of hire. However, vacation is not earned in any calendar month in which an employee is on leave of absence without pay for more than five working days.

Scheduling

To the extent possible, and with sufficient advance notice, vacations will be scheduled as requested by the employee provided that staffing requirements be met as determined by the supervisor. The supervisor will settle conflicts between employees with regard to desired vacation schedules.

A request should be filled out by the employee in SharePoint and approved by the Supervisor. Whenever possible, if requesting less than one week of vacation, the request should be presented three days prior to the time requested and if requesting one week or more the request should be presented and approved at least three weeks prior to leave.

Compensatory Time

The President and CEO and/or their designee may grant compensatory time for extra time worked by exempt employees, excluding members of the senior management team, for these unique situations provided it conforms to the following criteria:

1. As a general rule, exempt employees at the Green Bank work 40 hours per week. However, these employees are expected to work the number of hours necessary to get the job done. There are some occasions that require an exempt employee to work a significant number of extra hours in addition to the normal work schedule. This does not include the extra hour or two a manager might work to complete normal work assignments in a normally scheduled workday.
2. The Senior Management Team is defined as those exempt employees with a direct reporting relationship to the President and CEO and are at a level of Director or above.
3. The exempt employee must receive **written authorization in advance** to work extra time by the President and CEO and/or their designee in order to record the extra hours as compensatory time. The authorization must include the employee's name and outline the reason(s) for compensatory time. Proof of advance authorization must be retained for audit purposes.
4. The amount of extra time worked must be significant in terms of total and duration and **occur on weekends or state holidays**.
5. Extra time worked must be completed at an approved work location.
6. Compensatory time shall not accumulate by omitting lunch hours or other changes that do not extend the exempt employee's normal workday.
7. Compensatory time shall not accumulate for travel or commuting purposes.
8. The number of extra hours worked and the compensatory time taken must be recorded on the appropriate time sheet and maintained by the Green Bank. In no case shall an exempt employee be permitted to take compensatory time before it is earned.
9. All compensatory time earned January 1 through June 30 will expire on December 31 of the same year, and compensatory time earned July 1 through December 31 will expire on June 30 of the following year. All compensatory time balances will be set to zero on these dates. Any time not used by these dates will not be available.
10. In no event will compensatory time be used as the basis for additional compensation and shall not be paid as a lump sum at termination of employment.
11. No more than 8 hours can be earned in a twenty-four hour period.

Personal Leave

All Green Bank full time employees are granted three days paid personal leave each calendar year for purposes not covered by vacation or sick leave. Personal days do not require prior approval of the employee's supervisor; however, employees should still notify their supervisor with as much notice as possible. Personal time may not be accumulated or carried over to the next calendar year. Employees will not be compensated for unused personal time upon termination of employment. Personal leave days for part-time employees will be pro-rated.

General Leave of Absence

Occasionally, an employee may request time off without pay for reasons not covered by any of the other policies. In these cases, the employee should submit a written request for a leave of absence to their manager with a copy to the President and CEO and/or their designee. The request should clearly state the reason for the request and provide any supporting information to aid in the approval decision. The reason, and the requested length of the leave, will be considered by the President and CEO in their decision as to whether the employee's medical and other insurance benefits should continue during the leave, if approved. The decision will also be influenced by any limitations imposed by individual insurers.

Bereavement Leave

The Green Bank will grant an employee up to five consecutive workdays off in the event their immediate family member dies. If a death occurs while the employee is on vacation, five days absence with pay may be granted in lieu of the employee's vacation period. The immediate family is defined as an employee's spouse, parent, brother, sister, child, grandparent, grandchild, in-law, legal guardian, or permanent resident of the employee's household. Additional time may be granted if approved by the supervisor and charged against vacation or personal time. Employees should notify their supervisor as soon as possible if they have a need for bereavement leave.

Sick Leave

Full-time employees earn 10 sick leave days per year. Part-time employees earn sick leave according to the same schedule as full-time employees but prorated according to their standard part-time hours per week. Sick time is not earned in any calendar month in which an employee is on leave of absence without pay more than five working days.

Sick leave is intended for use in situations such as the following:

- Family illness - the event of a critical illness or severe injury to a member of the employee's immediate family in which the assistance of the employee is required.
- Medical Appointments – for medical, dental, eye examinations, or treatment for which arrangements cannot be made outside of working hours
- Other bereavement - up to three days per calendar year to attend the funeral of persons other than those of the employees' immediate family.

Terminating employees will not be compensated for the balance of unused sick leave except in the case of retiring employees. Qualified retirees will receive payment for one-quarter of accumulated unused sick leave up to a maximum of 60 days.

Sick Leave - Medical Certification or Examination

The Green Bank may require certification of illness from an employee's physician or a medical examination with another physician to verify the need for continued absence. To be certain that

an employee's health permits their safe return to work, the Green Bank may require medical certification or an examination by a physician regarding fitness for duty.

An acceptable medical certificate, signed by a licensed physician or other health care provider, will be required to substantiate time off if the medical/sick leave:

- Consists of more than five consecutive working days.
- Is to be applied contiguous to, or in lieu of, time taken off as vacation.
- Recurs frequently or habitually, and the employee has been notified.
- When the employee's presence at work will expose others to a contagious disease.

Sick Leave Bank
The Green Bank's Sick Leave Bank is a pool of sick days that has been established by employees of the Green Bank who have made a donation of their accumulated sick days. The Bank is available to members to draw up to ten (10) eight- hour sick days per year in the unfortunate event that they experience a qualified illness or injury.

Sick Leave Bank members will receive benefits in the form of paid sick leave if all of the following requirements are met:

- the member has a medical condition that prevents them from working that has been verified by a Medical Certificate OR a member's immediate family member has a medical condition that has been verified by a Medical Certificate and requires the Sick Leave Bank member's care.
- the member has been out on approved medical leave (paid or unpaid) as described above for at least two consecutive weeks.
- the member has exhausted all of their sick, personal leave and compensatory time and vacation time in excess of 30 days.
- the member has not been disciplined for an absence-related reason for the past 12 months (however a committee comprised of HR and Management may waive this requirement).
- the member has completed a Sick Leave Bank Withdrawal Request Form and it has been approved by human resources.

All requests for utilization of the sick leave bank must be in accordance with the Sick Leave Bank Policy. Please contact Human Resources for a complete copy of the Sick Leave Bank policy.

Family Medical Leave

Purpose

This policy establishes guidelines for leave available to employees of the Green Bank under the federal Family and Medical Leave Act of 1993 ("FMLA") and highlights relevant provisions of Connecticut law.

Eligibility

Employees who have worked at the Green Bank for at least twelve (12) months, and who have worked at least 1,250 actual work hours during the twelve (12) months immediately preceding the start of a leave, are eligible for unpaid leave under the FMLA. ("Hours worked" does not

include time spent on paid or unpaid leave). Employees must have worked at the Green Bank for at least six (6) months to be eligible for family/medical leave under Connecticut law.

Reasons for Leave

Leaves under either the state family/medical leave or federal FMLA or a combination of the acts may be taken for the following reasons:

- The birth of employee's child or adoption of a child by the employee (both).
- The placement of a foster child with the employee (federal only).
- The "serious illness" (state) or "serious health condition" (federal) of a child, spouse, or parent of an employee.
- The "serious illness" (state) or "serious health condition" (federal) of the employee.

Family Medical Leave Documentation Requirement

The following documents must be submitted in support of an FMLA request:

- **Birth of child:** "Employee Request" (Form HR-1) and Medical Certificate (Form P-33A-Employee) indicating the pre-delivery disability period (if applicable), delivery date and post-partum disability period (if applicable).
- **Adoption:** (both state and federal) or foster care (federal only) of child: "Employee Request" (Form HR-1) and letter from the adoption/foster care agency confirming the event and its effective date.
- **Serious illness/health condition of child, spouse, or parent:** "Employee Request" (Form HR-1) and Medical Certificate (Form P-33B-Caregiver).
- **Serious illness/health condition of employee:** "Employee Request" (Form HR-1) and Medical Certificate (Form P-33A-Employee) (only if employee is on paid or unpaid leave for more than five days).

Length of Leave
Under federal FMLA, employees are entitled to 12 weeks of unpaid leave in a twelve-month period. Under state family/medical leave, employees are entitled to a maximum of twenty-four (24) weeks of unpaid leave within a two-year period. The state entitlement is applied **after** the employee has exhausted any sick leave accruals that may be applicable. The state policy allows the substitution of personal leave and vacation accruals; however, this will not extend the 24-week entitlement period.

The 12-month entitlement period for family or medical leave is measured from the initial date of an employee's first leave under this policy, until the end of the applicable 12 or 24-month period. **For leaves eligible under both the FMLA and state family/medical leave, the entitlement periods will run concurrently.**

Requests for Leave
Requests for a family or medical leave must be submitted to Human Resources at least thirty (30) days before the leave is to commence, if possible. If thirty (30) days' notice is not possible, please submit your request as soon as practicable under the circumstances. For leaves taken because of the employee's or a family member's serious health condition, the employee must submit a completed medical certification form before the leave begins, if possible. This form may be obtained from Human Resources. If advance certification is not possible**,** the employee must provide the medical certification within fifteen (15) calendar days of the employer's request for the medical certification. Failure to submit a certification, or submission of an incomplete certification, may delay the use of FMLA leaves, or result in denial of such leave. If an

employee takes leave to care for their own serious health condition, immediately upon return to work the employee must provide medical certification that the health condition which created the need for the leave no longer renders the employee unable to perform the functions of the job. This certification must be submitted to Human Resources.

Use of Paid Leave
Employees have the option of substituting their accrued paid personal leave and accrued paid vacation for any unpaid portions of federal FMLA taken for any reason other than the employee's own serious health condition. However, where the leave is for the employee's own serious health condition, accrued paid sick leave shall be substituted for unpaid portions of federal FMLA prior to the employee electing the substitution of accrued paid personal and accrued paid vacation leave. The amount of unpaid leave entitlement is reduced by the amount of paid leave that is substituted.

Medical Insurance and Other Benefits
During approved FMLA and/or state family/medical leaves of absence, the Green Bank will continue to pay its portion of medical insurance premiums for the period of unpaid family or medical leave. The employee must continue to pay their share of the premium and failure to do so may result in loss of coverage. If the employee does not return to work after expiration of FMLA leave, the employee will be required to reimburse the Green Bank for payment of medical insurance premiums during the family or medical leave, unless the employee does not return because of a serious health condition or other circumstances beyond the employee's control.

Employees who have state-sponsored group life insurance will be billed directly for the same amount they contributed prior to the leave. In the case of any other deductions being made from paychecks (disability insurance, life insurance, deferred compensation, credit union loans, etc.), employees must deal directly with the appropriate vendor to discuss payment options.

During a leave, an employee shall not accrue employment benefits such as seniority, pension benefit credits, sick, or vacation leave. However, employment benefits accrued by the employee up to the day on which the leave begins, which remain unused at the end of the leave, will not be lost upon return to work. Leave taken under this policy does not constitute an absence under the Green Bank's attendance policy.

Reinstatement
Except for circumstances unrelated to the taking of a family/medical leave, an employee who returns to work following the expiration of a family/medical leave is entitled to return to the job held prior to the leave or to an equivalent position with equivalent pay and benefits. In cases involving the serious health condition of an employee, the Green Bank will require the employee to produce a fitness-for-duty report on which the physician has certified the employee is able to return to work. This requirement protects the employee, co-workers and the public from the negative consequences that can result when an individual returns to work before being medically ready to do so. Therefore, employees who are notified of the need for a fitness-for-duty certification will not be allowed to return to work without it.

Paid Parental Leave

Purpose/Objective

Green Bank will provide eight (8) weeks (320 hours) of paid parental leave to employees following the birth of an employee's child or the placement of a child with an employee in connection with adoption or foster care. The purpose of paid parental leave is to enable the

employee to care for and bond with a newborn or a newly adopted or newly placed child. This policy will run concurrently with other leave options, namely the federal and state Family and Medical Leave Act (FMLA), CT Paid Leave, and the Green Bank's disability policies, as applicable.

Eligibility

Eligible employees must meet the following criteria:

- Have been employed with the Green Bank for at least six (6) months.
- Be a full- or part-time, regular employee (temporary employees and interns are not eligible for this benefit). Part-time employees must work at the Green Bank between 20 – 32 hours per week.

In addition, employees must meet one of the following criteria:

- Have given birth to a child.
- Be a spouse or committed partner of the birthing parent.
- Have adopted a child or been placed with a foster child (in either case, the child must be age 17 or younger). The adoption of a new spouse's child is excluded from this policy.

Amount, Time Frame and Duration of Paid Parental Leave

- Eligible employees will receive eight (8) weeks of paid parental leave per birth, adoption or placement of a child/children which can be used in hourly increments.
- The fact that a multiple birth, adoption or placement occurs (e.g., the birth of twins or adoption of siblings) does not increase the eight (8)-week total amount of paid parental leave granted for that event.
- In no case will an employee receive more than eight (8) weeks of paid parental leave in a rolling 12-month period, regardless of whether more than one birth, adoption or foster care placement event occurs within that 12-month time frame.
- Each hour of paid parental leave is compensated at 100 percent of the employee's regular, straight-time weekly pay. Paid parental leave will be paid on a biweekly basis on regularly scheduled pay dates.
- Approved paid parental leave may be taken at any time during the twelve (12)-month period immediately following the birth, adoption, or placement of a child with the employee. Paid parental leave may not be used or extended beyond this twelve (12)-month time frame.
- Employees must take paid parental leave during the twelve (12)-month time frame indicated above and any unused paid parental leave will be forfeited at the end of that time frame.
- Upon termination of the individual's employment at the Green Bank, they will not be paid for any unused paid parental leave for which he or she was eligible.

Coordination with Other Policies

- Paid parental leave taken under this policy will run concurrently with leave under the FMLA; thus, any leave taken under this policy that falls under the definition of circumstances qualifying for leave due to the birth or placement of a child due to adoption or foster care, the leave will be counted toward the 12 weeks of available FMLA leave per a 12-month period. All other requirements and provisions under the

FMLA will apply. In no case will the total amount of leave—whether paid or unpaid—granted to the employee under the FMLA exceed 12 weeks during the 12-month FMLA period. Please refer to the Family and Medical Leave Policy for further guidance on the FMLA.After the paid parental leave (and any short-term disability leave for employees giving birth) is exhausted, the balance of FMLA leave (if applicable) will be compensated through employees' accrued sick, vacation and personal time. Upon exhaustion of accrued sick, vacation and personal time, any remaining leave will be unpaid leave. Please refer to the Family and Medical Leave Policy for further guidance on the FMLA.

- The Green Bank will maintain all benefits for employees during the paid parental leave period just as if they were taking any other Green Bank paid leave such as paid vacation leave or paid sick leave.
- If a Green Bank holiday occurs while the employee is on paid parental leave, such day will be charged to holiday pay.

Requests for Paid Parental Leave

- The employee will provide their supervisor and Human Resources with notice of the request for leave at least 30 days prior to the proposed date of the leave (or if the leave was not foreseeable, as soon as possible). The employee must complete the necessary HR forms and provide all documentation as required by Human Resources to substantiate the request.

As is the case with all Green Bank policies, the organization has the exclusive right to interpret this policy.

Military Leave

Military leave with pay for required military training is available to members of the National Guard or Reserve components of the Armed Forces. Required military leave must be verified through the submission of a copy of the appropriate military orders to Human Resources. A maximum of three (3) weeks per calendar year is allowed for annual field training.

When an employee is ordered to duty at the expiration of their field training, as evidenced by special orders, they shall receive additional time off with pay provided the period of absence in any calendar year shall not exceed thirty (30) days. No such employee shall be subjected, by reason of such absence, to any loss or reduction of vacation or holiday privileges.

Extended Military Leave (Induction)

Any employee who shall enter the Armed Forces shall be entitled to a leave of absence without pay for the time served in such service, plus ninety (90) days. An employee who leaves employment for the purpose of entering the Armed Forces of the United States shall be reinstated to their former position and duties, providing they apply for return to employment within ninety (90) days after receiving a certificate of satisfactory service from the Armed Forces.

This section shall not apply to any employee who has been absent from their employment for a period of more than three (3) years in addition to war service or compulsory service and the ninety (90) day period provided for because of voluntary reenlistment.

Jury Duty

The Green Bank recognizes that every citizen has an obligation to perform jury duty when required. The Green Bank encourages cooperation of its employees with this important civic duty.

If an employee is notified to appear in court to qualify to serve as a juror, the staff member must inform Human Resources by presenting the notice in advance of the court appearance date. The employee will receive time off to serve and will receive their regular salary during the period of jury service.

Failure to provide such notice will result in the Green Bank charging that time to either personal or vacation leave.

On any day during which the employee's attendance on the jury is not required, they shall report to work as usual. On any day in which the court releases jurors before 1:00 p.m., the employee is expected to report to work for the balance of the day.

Holidays

Holiday time off will be granted to all full-time regular employees on the 13 holidays listed below.

Part-time employees will be paid only if they are scheduled to work on the date that the holiday falls and their pay for the holiday shall be pro-rated based on their part-time schedule. Temporary employees after ninety (90) days will receive holiday pay if normally scheduled to work on the day of the week on which the holiday falls.

If a recognized holiday falls during an eligible employee's paid absence (e.g., vacation or sick leave), holiday pay will be provided instead of the paid time off benefit that would otherwise have applied.

Paid holidays at Green Bank are as follows:

New Year's Day
Martin Luther King's Birthday
Lincoln's Birthday
Washington's Birthday
Good Friday
Memorial Day
Juneteenth
Independence Day
Labor Day
Columbus Day
Veteran's Day
Thanksgiving Day
Christmas Day

Inclement Weather

When traveling in snow presents a significant danger to staff and clients, cancellations and late openings for the State of Connecticut will be announced on WTIC-AM 1080 or on-line at the Connecticut Department of Emergency Management and Homeland Security website. The President and CEO and/or their designee will inform department managers about any early closing times established during the day.

On inclement weather mornings when no cancellation or late openings have been announced, all employees (except those with an approved inclement weather telecommuting agreement) are expected to make a reasonable effort to be at work on time. Any employee who is unable to get to work is expected to notify their supervisor promptly and will have to utilize their personal leave accruals. Failure to notify your supervisor will be treated as an unexcused absence. Those employees with an approved inclement weather telecommuting agreement shall be subject to the terms and conditions of that agreement.

In the event of a situation where our offices will be closed because of a power outage, the following steps will be taken:

- Senior Staff will work to contact their teams.
- An email will be sent to all Green Bank staff and advise them that our offices are closed and inform them of next steps.

Community Service Days

Each employee may take up to one paid workday per year to perform community service. Prior approval by the employee's supervisor is required. The community service must be for 501 c 3 or equivalent non-profit organizations. The purpose of this policy is to encourage a range of community service activities by Green Bank employees. This day with pay will not be charged against any leave balance of the employee. Prior to the date of community service, each employee must provide a written request to their supervisor. Human Resources will determine whether the proposed service and organization meets the intent of the policy. A letter from the organization will be required as documentation of participation.

SECTION 5: EMPLOYEE BENEFITS

Employees of the Green Bank are eligible to participate in the medical, dental and retirement benefits offered to employees of the State of Connecticut. In addition, there are certain benefits offered by the Green Bank that are available to our employees. A summary of these benefits follows.

Workers' Compensation

All employees are covered under the State of Connecticut Workers' Compensation insurance program. This program covers any injury or illness sustained in the course of employment that requires medical, surgical, or hospital treatment. The Green Bank pays the full premium for this coverage. There is no cost to the employee.

Employees who sustain work-related injuries or illnesses should inform their supervisor immediately. No matter how minor an on-the-job injury may appear, it is important that it be reported immediately. Consistent with applicable state law, failure to report an injury within a reasonable period of time could jeopardize your claim. Supervisors are responsible for calling **MedInsights** at (800) 828-2717 toll-free as quickly as possible, to report any work-related injury sustained by an employee. Supervisors must provide **MedInsights** with the employee's name, home address, home telephone number, description of the injury, and the date and place the injury occurred. Supervisors should also notify Human Resources and the President as quickly as possible of any on the job injury sustained by an employee.

Neither the Green Bank nor the insurance carrier will be liable for the payment of benefits for injuries sustained during an employee's voluntary participation in any recreational, social, or athletic activity sponsored by the Green Bank after normal working hours.

Medical Insurance

Employees become eligible for coverage in a comprehensive health insurance program on the first day of the first full month of employment. Enrollment is limited to the date of hire or open enrollment periods (normally the month of May) as outlined by the employer. The details of the plan options and their coverage will be explained by Human Resources and are listed in the explanatory booklets provided by the insurer. A portion of the cost of the medical insurance for dependents must be covered by employee contributions.

Dental Insurance

Employees become eligible for coverage in a dental insurance program on the first day of the first full month of employment. The details of this insurance coverage will be explained by Human Resources and are listed in the explanatory booklet provided by the insurer.

Deferred Compensation

The Deferred Compensation Plan, created in accordance with Section 457 of the Internal Revenue Code, allows you to defer money earned during your peak earning years and receive its value later when you may be in a lower tax bracket. Amounts you elect to defer are before tax dollars and any interest earned or any gains on these dollars are allowed to accumulate without federal income tax obligations until you receive your money.

Participation in the Plan is voluntary. It is your decision, which should be made after considering all options, as well as your plans for the future. A Deferred Compensation Plan is not intended for savings and investments of a short-term nature since monies deferred are generally not available until you separate from State service. For more information regarding deferred compensation, contact Human Resources.

Retirement Plan

Employees of the Green Bank are provided retirement benefits under the State of Connecticut Retirement Plan (SERS). The benefits provided by the plan are described in the Summary Plan Description given to all eligible employees.

Dependent Care Assistance Program

Green Bank employees are eligible to participate in the State of Connecticut Dependent Care Assistance Program (DCAP). With DCAP you have the opportunity to deposit a portion of your pay into a Dependent Care Spending Account. These dollars are deducted on a pre-tax basis and are used to reimburse you for eligible dependent care expenses. These "pre-tax" dollars are exempt from federal and state income taxes.

When you contribute pre-tax dollars to a reimbursement account, you lower your taxable income; therefore, you pay fewer taxes and increase your spendable income. To receive more information, contact Human Resources.

Life Insurance

Upon employment, the Green Bank provides life insurance coverage at no cost to the employees that work at least 30 hours per week. In the event of an employee's death, life insurance benefits are payable to the person they have named as beneficiary. Other benefits such as dismemberment, loss of sight, continuation of insurance are explained in the group certificate. All eligible employees will receive a certificate showing the face value of the policy upon receipt of the application by the insurance company. The amount of coverage is equal to two times the employee's annual salary up to a maximum of $150,000 worth of coverage.

Group Life Insurance

Upon date of hire, employees can elect to participate in group life insurance offered by the State of Connecticut. Employees become eligible for coverage under the State of Connecticut group life insurance plan after six months of employment. The details of this coverage will be explained by Human Resources and are listed in the plan booklet provided by the insurer. The cost of this option is fully borne by the employee.

Supplemental Group Life Insurance

The State of Connecticut also offers supplemental group life insurance to employees whose gross annual income is at least $45,000. New employees are eligible for this insurance after six months of employment. This benefit is available for present employees to be initiated or increased during open enrollment, which is usually in May. The cost of this option is fully borne by the employee.

Other Insurance

There are several options for insurance available to our employees through the State of Connecticut. Human Resources will provide updates on these options periodically. Please contact Human Resources for further information.

Disability Insurance

The Green Bank provides short-term and long-term disability insurance coverage for all full-time employees. Disability coverage for new employees will commence on the first day of the second full month of employment. Please refer to your certificate booklet for full details, limitations, and provisions of the plan.

Connecticut Higher Education Trust Program

Green Bank employees are eligible to participate in the State of Connecticut's Higher Education Trust Program, Connecticut's 529 College Savings Program (CHET). With CHET, you have the opportunity to deposit a portion of your pay into a higher education savings account. These dollars are deducted on a pre-tax basis and are "pre-tax" dollars are exempt from federal and state income taxes. To receive more information, contact Human Resources.

Employee Assistance Program

The Employee Assistance Program offers assistance to employees having problems of a personal nature that may affect job performance. Services are also available for family members. Some examples of such problems would be drug or alcohol abuse, marital or family difficulties, or other situations that might have an adverse effect on an employee's emotional health. Participation in the program is confidential and free. It will generally include private consultation with a trained counselor who will advise the employee on what services are appropriate to their need. The counselor will normally refer the employee to qualified providers of treatment or counseling and advise the employee on what services are or are not covered by their health insurance. Any employee needing assistance should contact UCONN EAP at 860-679-2877 or toll-free (in CT) 800-852-4392. The UCONN EAP website is https://health.uconn.edu/occupational-environmental/employee-assistance-program/

Participation in the EAP program does not excuse employees from complying with normal agency policies or from meeting normal job requirements during or after receiving EAP assistance. Nor will participation in the EAP prevent the Green Bank from taking disciplinary action against any employee for performance problems that occur before or after the employee's seeking assistance through the EAP.

The EAP program is there for you and is totally confidential and voluntary.

Credit Union

Green Bank employees may participate in the Connecticut State Employee's Credit Union. Payroll deductions may be arranged. For more information, visit https://www.csecreditunion.com/.

An employee can open an account by completing an application card and a payroll deduction authorization form, which are available in Human Resources. A check or money order made payable to the Connecticut State Employee's Credit Union must accompany the application and the normal processing time is four (4) weeks.

A change in deduction form may be obtained from Human Resources for employees wishing to stop their deductions. This form must be submitted to CSECU, Inc. The change will take approximately four (4) weeks to become effective.

Other Payroll Deductions

Payroll deductions may be made for U.S. Savings Bonds and the Connecticut State Employees Campaign for charitable giving. Automobile insurance and homeowner's insurance can also be arranged through payroll deduction utilizing a program established by the State of Connecticut. For more information, contact Human Resources.

Direct Deposit

Direct deposit of paychecks to the banking institution of your choice is available. Forms are available from Human Resources. Upon termination of employment, a final paycheck will be issued and not deposited directly.

Benefits Continuation (Cobra)

The federal Consolidated Omnibus Budget Reconciliation Act (COBRA) gives employees and their qualified beneficiaries the opportunity to continue health insurance coverage under the Green Bank's health plan when a "qualifying event" would normally result in the loss of eligibility. Some common qualifying events are resignation, termination of employment, or death of an employee; a reduction in an employee's hours or a leave of absence; an employee's divorce or legal separation, and a dependent child no longer meeting eligibility requirements. Under COBRA, the employee beneficiary pays the full cost of coverage at the Green Bank's group rates plus an administrative fee. The Green Bank will provide each employee with a written notice describing rights granted under COBRA when the employee becomes eligible for coverage under the health insurance plan.

Educational Assistance

Any employee who has satisfactorily completed six months of service (and receives a rating of "meets expectations" or higher as a result of their six month review) and is either continuing their education in a job related area, in an area that will assist the employee in upward mobility or promotional opportunities, or is making principal and/or interest payments on qualifying debt incurred in the pursuit of such an educational opportunity shall be eligible to receive educational assistance as follows:

- **Tuition assistance**: for credit courses at accredited institutions of higher education, full-time employees will be reimbursed 100% of the cost of tuition and laboratory fees up to a maximum course cost per credit hour aligned with that of the University of Connecticut (please see Human Resources for the current limit). Non-credit hour-based tuition can be approved at the manager's discretion based on the relevance to the employee's current position, job responsibilities, and promotional path job responsibilities and career pursuits.
- **Student loan reimbursement**: Employees may also be reimbursed for their payment of their student debt as defined by Internal Revenue Code (IRC) provision 127 Employees will be reimbursed for actual payments of principal and interest on these loans up to $5,250, or the allowable inflation-adjusted limit, per calendar year. Human Resources will notify all staff of the year's allowable limit at the beginning of each calendar year beginning January 1, 2026.
- Employees may apply for both types of assistance in the same calendar year. The maximum aggregate dollar limit of tuition assistance and student loan reimbursement per employee per calendar year is $10,000.

Part-time employees who work at least 20 hours per week will be eligible for both forms of educational assistance on a pro-rated basis based on their work schedule. The employee must maintain an overall rating of "meets expectations" during the annual review process to continue to be eligible for either type of assistance under this program.

Requests for tuition and student loan assistance must be submitted via the Educational Assistance form on SharePoint and will be reviewed and approved by the employee's department head and the President and CEO and/or their designee based on individual merits. For tuition assistance, the request should be submitted prior to enrolling in a course/program, and management will consider its relevance to the employee's current position, job responsibilities and promotional path prior to approval of the tuition assistance request. In addition, the employee must maintain a grade point average (GPA) of C for undergraduate courses and B for graduate courses to continue receiving tuition assistance under this program.

If an employee's GPA falls below these minimums, further eligibility for tuition assistance will be suspended until the required GPA is achieved.

Employees are financially responsible to reimburse the Green Bank for payments made on their behalf under this program if they resign from their employment with the Green Bank within (6) months of the signed date on the most recent consent authorization section of the Educational Assistance Form.

Employee Tax Liability: The Green Bank follows the current IRS guidelines pertaining to annual reporting of employee educational benefits. Employees should consult with their tax advisor regarding this matter.

Employees interested in applying for tuition assistance under this program should follow the steps below to assure prompt reimbursement.

1. Complete the Tuition Assistance section of the Educational Assistance Form on SharePoint and submit it.
2. The request will be reviewed and if appropriate, approved by your department head and the President/Designee.
3. Once approved, you are enrolled in the program. Submit a copy of course registrations, invoices, and any other related documents to the Vice President of Operations for review and payment approval through a payment request on SharePoint. Tuition reimbursements will only be made to the extent the employee submits evidence of tuition payments at least in the amount requested (not to exceed statutory maximums and overall program limits).
4. Upon completion of the semester, submit a copy of your grades and current GPA to the Vice President. Failure to do so may render you ineligible for tuition assistance for future course.

Employees interested in applying for student loan assistance under this program follow the steps below to assure prompt reimbursement.

1. At any point during the calendar year, complete the Student Loan Reimbursement section of the Educational Assistance Form and submit it. You will be asked to submit documentation showing an active student loan account where payments are being made regularly.
2. The request will be reviewed and if appropriate, approved by your department head and the President/Designee.
3. Once approved, submit a copy of proof of loan payments and any other related documents to the Vice President of Operations for review and payment approval through a payment request on SharePoint. Student loan reimbursements will only be made to the extent the employee submits evidence of loan payments of at least in the amount requested and not more than annual allowable amount per Human Resources.
4. If you submit requests in subsequent calendar years, you will need to demonstrate payment(s) of the amount that the Green Bank has paid to you over the course of the program.

Employees interested in applying for both forms of assistance under this program should complete and submit an Educational Assistance form for each type of assistance and follow the applicable steps for both parts above.

Training

All employees of the Green Bank are encouraged to take advantage of any job-related training opportunities that will enhance their job performance. The Green Bank will pay the cost of any training deemed necessary for its employees.

The following is the procedure for signing up for and attending training:

1. The supervisor and employee will work together to develop a training plan for the employee based on the requirements of the job and the employees specific training needs.
2. The employee initiates a training request form and forwards it to their supervisor for approval.
3. The supervisor determines if the training is necessary, job-related, and if there is adequate office coverage for the employee to attend the training.
4. The employee attends the training and receives a certificate or attendance confirmation.
5. Upon return to the office, the employee forwards a copy of that certificate or attendance confirmation to Human Resources to be added to the personnel file.
6. The employee is responsible for sharing information learned at training that might be useful to other staff. The employee is also responsible for utilizing or practicing the subject material (i.e., computer training) and will be held accountable for the training material.

In addition, there are several training programs mandated for our employees by the State of Connecticut – sexual harassment prevention, diversity training, workplace violence prevention training and ethics training. Human Resources will work with employees to ensure they attend these mandatory training sessions.

Gym Membership

The Green Bank will cover the cost of membership to the Capewell Lofts gym for all employees based in the Hartford office who register with Operations. Employees based in the Stamford office can expense monthly membership to the gym co-located in the Canal Street complex up to $30 per month.

SECTION 6: TRAVEL AND ENTERTAINMENT POLICY

Travel and Entertainment Policy

This policy provides guidelines and establishes procedures for employees incurring business travel and entertainment expenses on the Green Bank's behalf.

Our objective is to provide employees with a reasonable level of services and comfort while traveling on Green Bank business. In order to accomplish this objective all employees must have a clear understanding of the policies and procedures for business travel and entertainment.

Green Bank staff should book the most economical and reasonable travel and lodging options (e.g., driving versus flying, direct versus connecting routes, inquiring if a state government rate discount is available, and weighing the best option of train, plane, and automobile transportation to reach your final destination). Reimbursement may be denied if it is deemed that the employee is not making a reasonable effort to book cost-effective travel.

Responsibility and Enforcement

The employee is responsible for complying with the travel and entertainment policy.
An expense report form must be completed by the employee within 30 days of incurring the expense to request reimbursement for travel and entertainment expenses.

The employee's supervisor is responsible for reviewing and approving expense reports prior to their submission.

The Green Bank assumes no obligation to reimburse employees for expenses that are not in compliance with this policy or are not submitted within 30 days of incurring the expense.

Who to Call About Travel Policy Questions

Any questions, concerns, or suggestions regarding this travel policy should be directed to the Finance Department.

Airline Class of Service

All air travel must be in Coach class. Employees are expected to use the lowest reasonable airfare available.

Upgrades for Air Travel

Upgrades at the expense of the Green Bank are **NOT** permitted. Upgrades are allowed at the employee's personal expense.

Unused/Voided Airline Tickets

Unused airline tickets or flight coupons must never be discarded or destroyed as these documents may have a cash value. To expedite refunds, unused or partially used airline tickets must be returned immediately to the designated department employee. Do not send unused tickets to the airlines or include them with expense reports.

Lodging

Employees are entitled to stay in a single room with a private bath. Employees may accept room upgrades to suites or executive floor rooms if the upgrade does not result in additional cost to the Green Bank.

Room Guarantee / Cancellation and Payment Procedures

It is the responsibility of the employee to cancel the room prior to the deadline if business needs require a change in travel plans (cancellation deadlines are based on the local time of the property). Employees should request and record the cancellation number for potential billing disputes.

Travel Insurance Coverage

Expenses for additional travel insurance coverage will not be reimbursed.

Rental Car

Guidelines

Employees may rent a car at their destination when:

- It is less expensive than other transportation modes such as taxis, Uber, Lyft, airport limousines and airport shuttles.
- Entertaining customers.
- Employees may reserve rental cars in advance if that is the most reasonable and cost-effective means of transportation.

Categories

The Green Bank reimburses the costs of Compact or Intermediate class rental cars. Employees may book a class of service one-level higher when:

- Entertaining customers.
- The employee can be upgraded at no extra cost to the Green Bank.
- Transporting excess baggage such as booth displays.
- Pre-approved medical reasons preclude the use of smaller cars.

Insurance

Employees should decline all insurance coverage when renting a car for Green Bank use as the Green Bank has suitable coverage in our general liability policy to cover these situations.

Cancellation Procedures

Employees are responsible for cancelling rental car reservations. Employees should request and record the cancellation number in case of billing disputes. Employees will be held responsible for unused car rentals that were not properly cancelled.

Return

Every reasonable effort must be made to return the rental car:

- **To the original city unless pre-approved for a one-way rental.**
- **Undamaged (i.e., no bumps, scratches, or mechanical failures).**
- **On time, to avoid additional hourly charges.**
- **With a full tank of gas.**

Reimbursement for Personal Car Usage

Employees will be reimbursed for business usage of personal cars on a fixed scale as determined by the Green Bank's mileage allowance. The mileage allowance is updated once a year in January and follows the mileage allowance set by the Internal Revenue Service. When working out of the office or out of town, any commute time clocked which is less than your normal daily commute is not reimbursable. Employees will not be reimbursed for any repairs to

their personal car even if these costs result from business travel. To be reimbursed for use of their personal car for business, employees must provide on their expense report:

- **Purpose of the trip.**
- **Date and location.**
- **Receipts for tolls, parking.**

Ground Transportation to and from Terminals

The most economical mode of transportation should be used to and from airports and bus and rail terminals when the employee is not accompanying a customer. The following modes of transportation should be considered:

- **Public transportation (buses, subways, taxis, Uber, Lyft).**
- **Hotel and airport shuttle services.**
- **Personal car.**

Personal/Vacation Travel

Combining Personal with Business Travel

Personal vacation travel may be combined with business travel provided there is no additional cost to the Green Bank. Corporate credit cards must **NOT** be used to pay for personal/vacation travel.

Spouse / Companion Travel

A spouse or other individual may accompany an employee on a business trip at the employee's expense. The Green Bank will not reimburse travel and entertainment expenses incurred by a spouse or other individual accompanying an employee on business unless:

- **There is a bona fide business purpose for taking the spouse or other individual.**
- **The expense incurred would otherwise be reimbursable; and**
- **There is prior approval from the President.**

Telephone Usage

Business Phone Calls

Employees will be reimbursed for using their personal cell phone or home phone for business phone calls that are reasonable and necessary for conducting business. Expenses must be substantiated with the original telephone bill. The finance department maintains a cell phone reimbursement policy. If you are contemplating using a cell phone for business purposes on a regular basis, contact the finance department to obtain a copy of the policy.

Airphone Usage

Employees will be reimbursed for using an airphone only in an emergency or if critical business issues necessitate its use.

Meals and Entertainment

Personal Meal Expenses

Personal meals are defined as meal expenses incurred by the employee when dining alone on an out-of-town business trip. Employees will be reimbursed for personal meals according to actual and reasonable cost incurred.

Business Meal Expenses

Business meals are defined as those taken with clients, prospects, or associates during which a specific business discussion takes place. Employees will be reimbursed for business meal expenses according to actual and reasonable cost.

Business Meals Taken with Other Employees
Employees will be reimbursed for business-related meals taken with other employees only in the following circumstances:

- **When a client is present.**
- **When, for confidentiality reasons, business must be conducted off Green Bank premises.**
- **When traveling together for business.**

Meal costs for social occasions, such as employee birthdays; secretary's day, etc. are not classified as business meals or entertainment expenses.

Entertaining Customers
Entertainment expenses include events that include business discussions, which take place during, immediately before or immediately after the event, are eligible for reimbursement for entertaining customers, with the prior approval from the President.

Tipping
Tips included on meal receipts will be reimbursed. Any tips considered excessive will not be reimbursed. As a general rule, employees should not tip more than 15% to 20% of the cost of the meal.

Other types of tips for porters, maid service, etc. should be reasonable.

Payment for Meals and Entertainment
When more than one employee is present at a business meal, the most senior level employee should pay and expense the bill.

Documentation Requirements
A receipt must be submitted with the expense report for any individual meal or entertainment expense. If a receipt is lost or destroyed, the President or Vice President Finance and Administration must approve the expense. In addition, for business meals and entertainment expenses, the following documentation is required and must be recorded on the expense report:

- **Names of individuals present, their titles, and company name.**
- **Name and location of where the meal or event took place.**
- **Exact amount and date of the expense.**
- **Specific business topic discussed.**
- **In the case of entertainment events, the specific time the business discussion took place (i.e., before, during or after the event).**

Corporate Charge Card

The President and CEO and/or their designee must approve the issuance of a corporate charge card.

Personal Use of Corporate Charge Card
Corporate charge cards are intended for business use. Corporate charge cards must **NOT** be used for personal expenses and use of the corporate charge card for personal expenses will result in termination of the card.

Reporting Lost / Stolen Charge Cards
A lost or stolen corporate charge card must be reported to the card issuer and the Managing Director of Operations as soon as the employee discovers it is missing. Statistics on stolen charge cards indicates that unauthorized use of stolen cards is greatest in the first few hours after the theft.

Expense Reporting

An expense report form is required to be completed via SharePoint to request reimbursement for incurred eligible travel and entertainment expenses.

The form will automatically calculate mileage reimbursements, total expenses by day and by type and calculate the net amount due the employee.

The expense report is to be completed and submitted for reimbursement in a timely manner. Expense reports should be submitted within one week of incurring the expense. The Green Bank will assume no obligation to reimburse employees for expenses that are not submitted within 30 days of incurring the expense.

The type of expense and dollar amount must be separated on a **daily basis**. For example: a hotel bill may include meals, lodging and telephone expenses. Each category must be split and entered in the appropriate space on the expense report form with expenses allocated for each travel day.

Approval / Authorization Process
All expense reports must be approved by the employee's immediate supervisor and the Finance Department. The President and CEO's expense report will be approved by the Executive Vice President Finance and Administration. Individuals approving expense reports are responsible for ensuring:

- **The correctness, reasonableness, and legibility of entries.**
- **Applicable receipts are attached.**
- **Charges are consistent with policy and were incurred for business purposes.**
- **Expenses are adequately explained.**
- **The expense report is signed by the employee.**

In accordance with present rules and guidelines, charges that are questionable should be discussed with the employee and resolved **before** the expense report is approved.

Expense Report Review
The Finance Department will review each employee expense report for:

- **Approval signatures.**
- **Business purpose.**
- **Correct totals.**
- **Supporting documentation and receipts.**
- **Policy compliance.**

The Finance Department will not reimburse any expense that is not in compliance with the Green Bank's travel and entertainment policy.

Examples of Acceptable Documentation:

- **Air/Rail – original passenger coupon.**

- **Hotel – hotel folio plus charge card receipt or other proof of payment.**
- **Car Rental – rental car agreement plus charge card receipt or other proof of payment.**
- **Meals/Entertainment – charge card receipt or cash register receipt.**
- **Receipts for all miscellaneous expenses over $10.00.**

Receipts must include the name of the vendor, location, date, and dollar amount of the expense. When a receipt is not available, a full explanation of the expense and the reason for the missing receipt is required.

Incorrect or Incomplete Expense Reports

Expense reports that are incorrect or incomplete will be returned to the employee for corrective action and may result in delay or non-reimbursement of specific items. Violating Green Bank policy or altering of receipts can result in disciplinary action up to and including termination.

Employees Will Not Be Reimbursed for the Following Items:

- **Airline club membership dues.**
- **Airline headsets.**
- **Airline drinks.**
- **Airline or personal insurance.**
- **Annual fees for personal credit card.**
- **Barbers and hairdressers.**
- **Birthday lunches.**
- **Car washes.**
- **Cellular phone repairs. (note that employees will be reimbursed for business use on their cellular phones pursuant to the Green Bank Mobile Communications Policy.**
- **Childcare.**
- **Clothing (i.e., socks, pantyhose, etc.).**
- **Expenses for travel companions/family members.**
- **Expenses related to vacation or personal days while on a business trip.**
- **Flowers or gifts for employees or customers (unless approved by the President or a Vice President).**
- **Gum, candy, or cigarettes.**
- **Health club facilities, saunas, massages.**
- **Hotel movies.**
- **Hotel room refrigerator items.**
- **Hotel laundry and valet services unless the trip exceeds five consecutive days.**
- **Interest or late fees incurred on a personal credit card.**
- **Loss/theft of cash advance money or Company-paid airline tickets.**
- **Loss/theft of personal funds or property.**
- **Magazines, books, newspapers, subscriptions.**
- **Mileage for travel between home and office/work site.**
- **"No show" charges for hotel or car service.**
- **Optional travel or baggage insurance.**
- **Parking or traffic tickets.**
- **Personal accident insurance.**
- **Personal entertainment, including sports events.**
- **Personal toiletries.**
- **Pet care.**
- **Postage costs, postcards (sent to fellow employees).**
- **Shoeshine.**
- **Short term airport parking (except for 1-day trips only**

- **Unexplained or excessive expenses which are not within the intent of Green Bank policy will not be reimbursed.**

All employees must review this policy and sign the acknowledgement form found in the Appendix and return it to Human Resources.

SECTION 7: GENERAL RULES OF CONDUCT

Ethical conduct is a core value of the Connecticut Green Bank and all board members and employees of the Green Bank are expected to maintain the highest professional standards in the conduct of their duties. In particular, Green Bank employees are considered to be "state employees" and members of the Green Bank's Board of Directors are considered to be "public officials". A copy of the Public Officials and State Employees Guide to the Code of Ethics (the "Guide") is included at end of handbook for reference. You may also access both the Code of Ethics and the Guide on the Office of State Ethics website at www.ct.gove/ethics by clicking on "Statutes and Regulations" and "Public Official and State Employee Information", respectively.

General Rules of Conduct

To ensure orderly operations and provide the best possible work environment, Green Bank expects employees to follow rules of conduct that will protect the interests and safety of all employees and the organization. Although it is not possible to list all the forms of behavior that are unacceptable, the following are examples of infractions that may result in disciplinary action, up to and including termination of employment:

- Theft or inappropriate removal or possession of property of the Green Bank, clients or other employees.
- Dishonesty or misrepresenting, falsifying, or providing misleading records including, but not limited to, employment applications or resumes, time keeping records, client records, expense requests, etc.
- Working under the influence of alcohol or illegal drugs.
- Possession, distribution, manufacturing, sale, transfer, or use of alcohol or illegal drugs in the workplace, while on duty.
- Fighting, wrestling, horseplay, or threatening violence in the workplace.
- Use of obscene or vulgar language, insubordination or other disrespectful conduct including, but not limited to, refusal to perform assigned work.
- Taking any action detrimental to the Green Bank, fellow employees, clients, or visitors.
- Unsafe behavior and/or violation of safety or health rules.
- Sexual or other unlawful or unwelcome discrimination or harassment.
- Possession of dangerous or unauthorized materials, such as explosives or firearms, in the workplace.
- Excessive absenteeism, tardiness, or any absence without notices.
- Unauthorized use of telephones, mail system, or other employer-owned equipment for personal use or other unauthorized operation.
- Sleeping, loafing, failure to demonstrate a professional behavior in carrying out assigned tasks.
- Soliciting, gambling, taking orders, selling tickets, collecting, or contributing money for any unauthorized cause.
- Engaging in outside business activities that conflict with the Green Bank's interests or interfere with proper performance of job duties.
- Failure to report a work-related injury immediately.
- Unauthorized use or the willful damage, abuse, or destruction of Green Bank property or the property of others.
- Violation of the Green Bank's personnel policies and/or rules.
- Unsatisfactory work performance.

The examples listed above are not intended to cover all situations that may result in disciplinary action but are only intended to be guidelines as to what are considered improper standards of

work conduct. Also, this policy does not alter the at-will nature of an employee's employment with the Green Bank.

If any employee's behavior or interactions jeopardize positive working relationships with clients and render the employee unable to fulfill the responsibilities of their position, or place the Green Bank at risk of liability, the employee will be subject to review and possible disciplinary actions.

It is important for all employees to conduct themselves in a way that is fair to each other and to our common objective of delivering quality services.

Personal Appearance

The nature of our business at the Green Bank puts us in frequent contact with clients and the public. We enjoy an excellent reputation among the energy community in Connecticut. While there are many reasons for this reputation, one of the ways to help maintain it is for all staff to present a professional image to the community. It is important that they have confidence in the staff, and the staff members have confidence/pride in themselves when doing business. To help present this image and foster public confidence, staff members must dress appropriately for their work assignments and use common sense and good judgment in their appearance.

Employees with questions regarding what is deemed appropriate dress for their work assignments should discuss this with their supervisor. The Green Bank reserves the right to determine individual compliance with the policy in all questionable cases.

Personal Appearance Guidelines
Staff will wear clean and well-maintained attire appropriate to the type of work they do. Shoes are required and must also be well-maintained. Good grooming is required.
Formal business attire may be expected for internal and external events such as board meetings, hearings, presentations, and meetings.

Business casual attire and jeans is acceptable for being in the office and other occasions where clients are not present.

In compliance with this policy, the following are examples of unacceptable attire:

- torn, patched/faded clothing
- athletic wear, e.g., shorts, T-shirts, skorts, etc.
- halter tops
- tube tops
- rubber soled flip flops, shorts (any pants or slacks that ends above the knee)
- shirts with slogans or large letter advertising

Freedom from Harassment

The Green Bank is committed to treating its employees with dignity and respect. All employees have a right to be free from racial or ethnic slurs, unwelcome sexual advances, or any other verbal or physical conduct that constitutes harassment. The Green Bank is committed to providing a work environment that is free of discrimination and unlawful harassment.

Sexual harassment is unlawful under federal and state law. The Green Bank's statement on Sexual Harassment and the Equal Employment Opportunity Commission "Guidelines on Discrimination Because of Sex" provides that unwelcomed sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature constitute sexual harassment when:

- Submission to such conduct is made either explicitly or implicitly a term or condition of an individual's employment.
- Submission to or rejection of such conduct by an individual is used as the basis for employment decisions affecting that person.
- Such conduct has the purpose or effect of unreasonably interfering with an individual's work performance or creating an intimidating, hostile, or offensive working environment.

Actions, words, jokes, or comments based on an individual's sex, race, ethnicity, age, religion, or any other legally protected characteristics will not be tolerated. As an example, sexual harassment (both overt and subtle) is a form of employee misconduct that is demeaning to another person, undermines the integrity of the employment relationship, and is strictly prohibited.

Sexual, racial, ethnic, or other unlawful harassment of employees by supervisory or non-supervisory employees of the Green Bank, or by non-employees (including clients) will not be tolerated. All members of the Green Bank management and supervision have the explicit responsibility to take immediate corrective action to prevent any sexual, racial, ethnic, or other harassment.

Any employee who wishes to report an incident of unlawful harassment should promptly report the matter to their supervisor. If the supervisor is unavailable or the employee prefers to report the incident to someone other than the supervisor, they should immediately contact the Human Resources designee or any other available manager.

Anyone engaging in unlawful harassment will be subject to disciplinary action, up to and including termination of employment.

Sexual Harassment

Title VII of the Civil Rights Act of 1964, which is a federal law and Connecticut law, prohibit sexual harassment. The Green Bank will not tolerate sexual harassment in the workplace. No employee-either male or female-should be subject to unwelcome verbal or physical conduct that is sexual in nature or shows hostility to the employee because of the employee's gender. Sexual harassment does not refer to occasional compliments of a socially acceptable nature. It refers to behavior that is not welcome, that is personally offensive, that debilitates morale, and that, therefore, interferes with work effectiveness.

Management Responsibility

Management at all levels of the Green Bank are responsible for preventing sexual harassment in the workplace. This responsibility includes immediately reporting conduct by anyone, whether a coworker, supervisor, or non-employee, that may constitute sexual harassment, even if the conduct was sanctioned and regardless of how awareness of conduct was gained.

Prohibition Against Sexual Harassment

The Green Bank strictly enforces a prohibition against sexual harassment of any of its employees. Sexual harassment prohibited by state and federal law and by this policy includes the following conduct:

- Unwelcome verbal or physical conduct of a sexual nature when submission to such conduct is made either an explicit or implicit term or condition of any individual's employment (such as promotion, training, timekeeping, overtime assignments, leaves of absence); or

- Unwelcome verbal or physical conduct of a sexual nature when submission to or rejection of such conduct by an individual is used as the basis for employment decisions; or
- Unwelcome verbal or physical conduct of a sexual nature when the conduct has the purpose or effect of substantially interfering with an individual's work performance or creating an intimidating, hostile or offensive working environment; or
- Unwelcome verbal or physical non-sexual conduct that denigrates or shows hostility toward a person because of their gender when the conduct has the purpose or effect of substantially interfering with an individual's work performance, or creating an intimidating, hostile, or offensive work environment.
- Sexual harassment is a form of sexual discrimination, and neither sexual harassment nor discrimination will be tolerated.

Examples of Conduct Prohibited by This Policy Include:

- Offering or implying an employment-related reward (such as a promotion or raise) in exchange for sexual favors or submission to sexual conduct.
- Threatening or taking a negative employment action (such as termination, demotion, denial of a leave of absence) if sexual conduct is rejected.
- Unwelcome sexual advances or repeated flirtations.
- Graphic verbal commentary about an individual's body, sexual prowess, or sexual deficiencies.
- Sexually degrading or vulgar words to describe an individual.
- Leering, whistling, touching, pinching, brushing the body, assault, coerced sexual acts, or suggestive, insulting, or obscene comments or gestures.
- Asking unwelcome questions or making unwelcome comments about another person's sexual activities, dating, personal or intimate relationships, or appearance.
- Conduct or remarks that are sexually suggestive or that demean or show hostility to a person because of that person's gender (including jokes, pranks, teasing, obscenities, obscene or rude gestures or noises, slurs, epithets, taunts, negative stereotyping, threats, blocking of physical movement).
- Displaying or circulating pictures, objects, or written materials (including graffiti, cartoons, photographs, pinups, calendars, magazines, figurines, novelty items) that are sexually suggestive or that demean or show hostility to a person because of that person's gender.
- Retaliation against employees complaining about such behaviors.
- Harassment consistently targeted at only one sex, even if the content of the verbal abuse is not sexual.
- Sexually suggestive or flirtatious letters, notes, e-mail, or voice mail

This policy covers all employees. The Green Bank will not tolerate, condone, or allow sexual harassment whether engaged in by fellow employees, supervisors, and associates or by outside clients, opposing counsel, personnel or other non-employees who conduct business with this agency.

General Harassment

Actions, words, jokes or comments based on an individual's sex, race, ethnicity, age, religion, or any other legally protected characteristic will not be tolerated. Such conduct can unreasonably interfere with work performance and create an intimidating, hostile and offensive work environment.

We expect all employees to consider at all times the effect your words and actions may have on those with whom you work. While you may feel that your behavior is harmless, it is the way your words and actions are perceived by others that counts.

Please do not assume that the agency is aware of a harassment situation. It is in your best interest and your responsibility to bring your complaints and concerns to management's attention so that the issue may be resolved.

Complaint Process

Should you ever experience any job harassment problem, please exercise the steps in our agency Grievance Procedure (outlined in Section 7 of this handbook), or at your option, you may directly contact Human Resources. You may expect prompt and concerned reaction to your problem. Any employee engaging in unlawful harassment will be subject to disciplinary action, up to and including termination.

Sanctions

Any employee found to have engaged in sexual harassment or sexual discrimination will be subject to appropriate discipline, up to and including discharge.

No Retaliation

This policy also prohibits retaliation against employees who bring sexual harassment charges or assist in investigating charges. Retaliation in violation of this policy may result in discipline up to and including termination. Any employee bringing a sexual harassment complaint or assisting in the investigation of such a complaint will not be adversely affected in terms and conditions of employment, nor discriminated against or discharged because of the complaint.

All employees must review this policy and sign the acknowledgement form found in the Appendix and return it to Human Resources.

Confidential Disclosure Policy

Instructions: Please read this Confidential Disclosure Policy form carefully, then sign and return this form to Human Resources.

I understand that in connection with my work for the Green Bank, I may be exposed to or given confidential, nonpublic, or proprietary information belonging to the Green Bank and others, including, but not limited to, information concerning trade secrets, business, products, finances, personnel information, customer personal information (PI), and plans of the Green Bank or the Green Bank's clients, portfolio companies and applicants, (the Confidential Information). Without limitation, examples of Confidential Information are drawings, manuals, notebooks, reports, models, inventions, formulas, processes, machines, compositions, computer programs, accounting methods, financial information, business and marketing plans and information systems.

Some of the Confidential Information may belong to or relate to "publicly held" companies and may include "inside information" which is not available to the public.

My employment by the Green Bank creates a relationship of special confidence and trust between me and the Green Bank with respect to the Confidential Information.

I agree as follows:

1. I will not, either during or subsequent to my employment by the Green Bank, (1) publish or otherwise disclose Confidential Information except to persons who may from time to time be designated by the Green Bank as proper and authorized recipients of such Confidential Information or (2) use the Confidential Information (including any inside information) either for the benefit of myself or for the benefit of anyone other than the Green Bank. If I have any questions regarding whether any information is Confidential, I will ask my supervisor for instructions and will not disclose such information unless otherwise instructed by my supervisor.
2. The Confidential Information will remain at all times the property of the Green Bank or the rightful owners thereof notwithstanding its disclosure to me.
3. I will promptly disclose to the Green Bank all materials, innovations, studies, writings, or other works created or developed by me as a result of tasks assigned to me by the Green Bank or exposure to the Confidential Information ("Work Product"). I agree that all ("Work Product") shall be the sole property of the Green Bank and that the Green Bank shall be the sole owner of all copyrights and other intellectual property rights related thereto. I hereby assign to the Green Bank any and all rights which I may have or acquire in any Work Product and agree to assist the Green Bank in every way (but at the Green Bank's expense) to obtain or enforce copyrights and other interests in the Work Products as the Green Bank may desire.
4. Upon termination of my employment with the Green Bank or whenever requested by the Green Bank, I will promptly deliver to the Green Bank all Work Product and all documents and other tangible embodiments of the Confidential Information and any copies thereof.

Confidential Disclosure Policy

This agreement supersedes and replaces any existing agreement between the Green Bank and me relating generally to the same subject matter. It may not be modified or terminated, in whole or in part, except in writing signed by an authorized representative of the Green Bank. Discharge of my undertakings in this agreement shall be an obligation of my executors, administrators, or other legal representatives or assigns.

All employees must review this policy and sign the acknowledgement form found in the Appendix and return it to Human Resources.

Computer Use Policy

Purpose

Your Green Bank assigned computer is a resource and is subject to the same rules as other Green Bank resources. The purpose of this policy is to ensure that employees understand the guidelines governing company owned computer and other electronic communications (including tablet computers and mobile phones) use with regard to Internet access, email, other electronic communications, software licensing, security, and personal use, in particular.

This policy cannot provide rules and guidance to cover every possible situation. Instead, it is designed to express the Green Bank's philosophy and set out the general principles that employees should apply when using company computers and technology. These policies apply to all Green Bank employees and staff (consultants, third-party contractors, and administrators).

This policy does not cover health and safety issues.

Issues not directly addressed in this policy or in some other written form are to be decided by HR and/or Green Bank management should the need(s) and situation(s) arise. Further policy documents are forthcoming to cover specific areas of acceptable use as technology is deployed.

Unless otherwise stated, violation of these policies, including the Green Bank's information security and privacy policies, may result in disciplinary action, up to and including termination and/or legal action.

Commented [JB1]: To include links to the approved policies

General

The Green Bank provides employees and staff with personal computers (PCs), printers and other computer equipment as necessary to perform their job. Employees should not expect the latest hardware or software releases to be provided unless there is a business reason to do so.

The Green Bank encourages the use of email, voicemail, online services, the Internet, and Intranet as they can make communication more efficient and effective. In addition, they can provide valuable sources of information about vendors, customers, competitors, technology and new products and services. Pursuant to the Freedom of Information Act (FOIA), no employee shall have any expectation of privacy in any Green Bank work product.

Everyone connected with the organization should remember that electronic media and services provided by the company are company property and their purpose is to facilitate and support company business. Data stored and/or accessed on company equipment, regardless of origin, purpose, or design should also be considered to be within, at least, company purview, oversight, and audit rights. The company reserves the right to access data of any sort, stored or located on company provided equipment.

The following are examples of **non-business**-related activities that are prohibited:

- Streaming music or video.
- Shopping.
- Booking a vacation.
- Using instant messaging.
- Viewing personal social media accounts.
- Accessing personal email accounts.
- Viewing personal pictures over the web.
- Downloading unauthorized computer software or pornographic materials.

E-Mail

All employees and staff are supplied with a company email address and the means by which to access their account. These details are provided by the Green Bank as part of our IT orientation process. E-mail messages are considered public records and are subject to the Freedom of Information Act. Furthermore, e-mail, both incoming and outgoing, is not confidential and is monitored by the Information Technology Department. All e-mail correspondence is saved on the ~~network~~ Green Bank's backup solution and is easily retrievable. You should take great care to scrutinize what you include in an e-mail message. E-mail messages may exist on the system indefinitely and may be recoverable even after you have deleted the message.

All employees must create and use a business email signature, based on the approved template that is generated by the Marketing department.

All non-company email services, such as Gmail, Hotmail, Yahoo, etc. are never to be used for company purposes. If third-party email services must be used, it will be provisionally and under

direct supervision of the Operations Department. Never is an employee or staff member to use a personal email account to correspond with clients.

Electronic media (email, web browsers, etc.) must not be used for knowingly transmitting, retrieving or storage of any communication that:

- Is discriminatory
- Is harassing or threatening
- Is derogatory to any individual or group
- Is obscene or pornographic
- Is defamatory
- Is engaged in any purpose that is illegal or contrary to Green Bank's policy or business interests
- Contains unencrypted personal information
- Contains unencrypted intellectual property

Further, all forms of mass email (including 'virus warnings', 'good luck' and similar messages) are unacceptable unless for an approved business purpose.

The transmission of usernames, passwords, or other information related to the security of the Green Bank's computers is prohibited. If a password protected file absolutely must be emailed, the password should be sent in a separate email from the document or communicated in another manner.

Employees should avoid sending unnecessary informational emails to large parts or all of the organization. However, we recognize the business need for companywide emails, but there will be a strictly monitored and governed use of such behavior and practice. Failure to comply with these guidelines could result in disciplinary action.

Email Disclaimer
An email disclaimer is automatically added through our exchange server to the end of all e-mail being sent outside the office. Do not add your own disclaimer to messages. The company disclaimer is as follows:

NOTICE TO RECIPIENT: This e-mail is (1) subject to the Connecticut Freedom of Information Act and (2) may be confidential and is for use only by the individual or entity to whom it is addressed. Any disclosure, copying or distribution of this e-mail or the taking of any action based on its contents, other than for its intended purpose, is strictly prohibited. If you have received this e-mail in error, please notify the sender immediately and delete it from your system.

External email and participation in online forums
Employees should be aware that any messages or information sent using the company systems are statements identifiable and attributable to the company. Thus, an email carries the same weight in law as a letter written on company stationery.

Employees should note that even with a disclaimer, as described above, a connection with the company still exists and a statement could be imputed legally to the Green Bank. Therefore, no one should rely on disclaimers as a way of insulating the Green Bank from the comments and opinions that are contributed to forums or communicated in emails. Instead, discussions must be limited to matters of fact and expressions of opinion should be avoided while using company systems or a company-provided account. Communications must not reveal information about

company processes, techniques, trade secrets, or confidential information and must not otherwise violate this or other company policies. Any email messages sent with confidential or nonpublic information must be encrypted.

Employees should not send file attachments by email in situations where there is any potential for the compromise of company secrets or in relation to litigation. Be aware, files from many word processing packages, including Microsoft Word, retain information related to previous versions of the document that can later be retrieved.

Email received

Employees should only open email received from trusted sources. To prevent business email compromise, employees must not open any attachments, click on any links or scan QR codes within email messages received from unknown sources.

Electronic calendars and voicemail

It is Green Bank policy that all employees keep their electronic calendars up to date (using Microsoft Outlook) and that calendars can be read by supervisors. When a meeting or event needs to be kept confidential, it should be marked as 'private' with the appropriate program functionality.

It is Green Bank policy that all employees with email and/or voicemail keep their "out of office assistant" or pre-recorded greetings up to date. In particular, during periods of absence from the office, these greetings should provide the individual with information indicating when the employee will receive a message or information about an alternative contact.

Illegal & Prohibited Activities

Use of your computer for an illegal purpose is prohibited. Illegal activities include violations of local, state and/or federal laws and regulations. Connecticut General Statutes, section 53a-251 establishes the crime of "Computer Crime." A person can be charged with a computer crime for such things as:

- Unauthorized access to a computer system.
- Theft of computer services.
- Interruption of computer services.
- Misuse of computer services.
- Destruction of computer equipment.

A computer crime violation can range from a Class B Felony (1 to 20 years in prison and up to $20,000 fine) to a Class B Misdemeanor (up to 6 months in prison and up to $1,000 fine) depending on the amount of money or damage involved.

The Green Bank strives to maintain a workplace free of harassment and sensitive to the diversity of its employees. Therefore, the Green Bank prohibits the use of any of its systems, including the computers and the e-mail system in ways that are disruptive, offensive to others, or harmful to morale. For example, the display or transmission of sexually explicit images, messages, and cartoons is not allowed. Other such misuse includes, but is not limited to, ethnic slurs, racial comments, off-color jokes, or anything that may be construed as harassment or showing disrespect for others.

It is recognized that employees do not have complete control over all incoming e-mail that is sent to the Green Bank. However, it is the responsibility of every employee to monitor incoming e-mail and request cessation of inappropriate, voluminous, unprofessional, or disruptive e-mail.

Software

It is Green Bank policy that only licensed software that is legally owned by the company may be used. All use of unlicensed software is expressly forbidden, unless ~~written~~ pre-approval by ~~IT and management~~ the Head of Operations. However, you are not allowed to install any software on any company hardware. All software must be approved and installed in coordination with the Head~~Managing Director~~ of Operations. As always, proper documentation of licensing is required.

In order to implement this policy, the Green Bank maintains a central register containing physical licenses for the software install on its computers. Where no physical manifestation of a license exists, a written record of the license purchase is kept with a reference to the relevant invoice. It is the responsibility of the IT vendor and Operations team to maintain this license repository.

Free or shareware programs should not be installed on company computers due to the risk of virus infection and other side effects without approval from IT. Where installed, they are only exempt from the central license recording provided the software clearly identifies itself as free.

Green Bank Computer Software Overview—Microsoft 365

The Green Bank uses Microsoft 365, a cloud-based subscription service that includes various office applications, cloud storage, and security systems, all designed to work together to facilitate productivity, collaboration, and communication in a business environment.

The standard applications that Green Bank staff uses for basic office tasks are all from the Microsoft 365 suite of services: Outlook (email), Word (word processing), Excel (spreadsheets), and PowerPoint (presentations).

~~In addition, we have also implemented Teams and OneDrive, and will soon be rolling SharePoint out to the organization as a replacement for the P Drive. Since these applications may be less familiar to staff, below is an overview of what each application does and when and how it should be used.~~

Teams

An application that allows internal and external users to collaborate on projects using documents, calendars, chat, and other features. Teams also functions as our phone system and internal chat application and employees should remain logged into and available via Teams during regular business hours.

Benefits of using Teams:

- Better security and compliance than our previous document-sharing software
- Accessibility (access information across approved devices without the need of a VPN) and availability (anytime, anywhere access to information)
- Version control and ease of connection with other Office 365 applications

What is the function of Teams within our working environment?

Create a Team when you want to connect internal and/or external individuals around a specific project. The Teams application functions as our phone system and our internal chat service.

OneDrive

An application that allows users to store and backup their personal business files, available on the web and via a desktop app. OneDrive Includes cloud storage that you can get to from anywhere to help you stay organized and access your important documents easily.

Benefits of using OneDrive:

- Better security and compliance
- Accessibility (access information across approved devices without the need of a VPN) and availability (anytime, anywhere access to information)
- Helpful features, such as version control and ease of connection with other Office 365 applications

OneDrive is a place to store your personal business documents (paystubs, expense reports, reviews, etc.) since no one can access any documents there unless you give them permission.

OneDrive should also be used to draft documents and collaborate on them with your colleagues. Once the document you are working on is final, it should be moved to an appropriate folder ~~in the P Drive~~on SharePoint.

SharePoint

A secure place to store, organize, share, and access information from any device. It allows users to create forms, processes, and even websites. It is the document filing system behind Teams—when you create a Team you create a SharePoint site unique to that Team.

- Easier document access and FOIA compliance with enhanced search via metadata tagging
- Accessibility (access information across approved devices without the need of a VPN) and availability (anytime, anywhere access to information)
- Version control and ease of connection with other Office 365 applications
- Significant financial savings

SharePoint is ~~currently the application behind the Green Bank Intranet and our Forms page. Moving forward, SharePoint will be replacing the P Drive as~~ the official storage location for all Green Bank documentation.

Other Green Bank Data Management Platforms

In addition, there are other software solutions that the Green Bank has implemented to help us manage databases and support our programs. These include PowerClerk, NGEN, Intacct, and Salesforce. More detail around each is available below.

PowerClerk

PowerClerk is the database for the RSIP team. Contractors, System Owners, Inspectors, and Green Bank staff collaborate in PowerClerk to submit paperwork, calculate incentives, estimate system production, and track most aspects of residential solar PV projects that receive an RSIP incentive.

NGEN

NGEN stands for National Green Energy Network and is a custom-designed software program that manages workflows for our residential Smart-E Loan program.

NGEN is a workflow management tool where all Smart-E contractor, lender, and project specific data reside. Contractors provide project level data, where Green Bank staff review, and approve each project to be financed. Staff use the NGEN platform to communicate to both lenders and contractors regarding approval for loan closings, and distribution of loan funds to the contractor. Lenders provide overall portfolio data to help staff manage the loan loss reserve and overall portfolio strength.

Sage Intacct

Sage Intacct is a cloud-based financial management system.

The Accounting team uses Sage Intacct to manage all Accounts Payable, Accounts Receivable and Employee Expense processing, as well as tracking of cash, PSA, investment, and loan balances. Sage Intacct is used to perform all necessary financial reporting. Green Bank senior management uses Sage Intacct to manage budget to actual spending and to review financial results.

Salesforce

Salesforce is a customer relationship management (CRM) platform. Based in the cloud, Salesforce allows users to configure their own applications to support sales, service, and marketing initiatives.

The Green Bank uses a custom-designed Salesforce platform for many purposes, including:

- Organization/Company information & Contact management
- C-PACE Lead tracking, organization & reporting
- Campaign monitoring
- Marketing communications
- Complete process management for C-PACE, including automations and workflows
- Project & financial data collection and organization for C-PACE and all commercial programs
- Lien filing tracking for C-PACE projects
- C-PACE billing contact information
- C-PACE Disbursement approvals through DocuSign App
- All C-PACE, Green Bank Solar PPA & MFH KPI data collection & reporting, including progress to targets
- External Salesforce Experience for C-PACE Contractors to submit data & documentation for technical underwriting & commissioning steps within the C-PACE process

Vendor Management Policy

The Green Bank designs its processes and procedures for its IT infrastructure and application processing system to meet its objectives and reporting requirements. Those objectives are based on the commitments that the Green Bank makes to user entities, the laws and regulations that govern the provision of its services, and the financial, operational, and compliance requirements that the Green Bank has established.

Agreements with vendors include clearly defined terms, conditions, and responsibilities between the Green Bank and the vendor and are required to be executed prior to the commencement of a business relationship. See the Green Bank's Information Security Policy for details on vendor management procedures. ~~Additional commitments are standardized and include, but are not limited to, the following:~~

Commented [JB2]: To include link to approved policy

~~• Criteria designed to permit users to access only the information they need based on their role~~
~~• Use of encryption technologies to protect confidential data~~
~~• Use of strong passwords and unique user IDs~~
~~• Implementation of a firewall and antivirus monitoring software~~
~~• Continuous monitoring of system performance~~
~~• Secure and timely backup and retention of data~~

~~SOC2 certification is highly preferred for any data/IT vendor. Designated Green Bank personnel will perform a review of the identified subservice organization's SOC report when they become available to ensure that key controls are designed appropriately and operating effectively and that they coordinate with the controls implemented at the Green Bank. If there is a vendor we want to work with and they are not SOC2 certified, we will work with our managed IT services partner to assess the risk inherent in a possible working relationship.~~

Hardware
Employees issued portable (laptop, tablet) computers must take reasonable precautions. When out of the office the computer should always be under direct control of the employee or out of sight in a secure location. The Green Bank may take other security measures including, but not limited to, computer tracking hardware/software, security cables, and/or hard drive encryption.

- Personal use of the company phone system should be kept to a minimum.
- AV equipment is available in all Conference rooms and is reserved using the calendar resource on Teams or in Outlook, selecting the room as a resource.
- All laptop users must carry their device in an adequately padded laptop case. Laptop sleeves, tote bags and any other un-cushioned bags are unacceptable.
- Printers must be handled with care. If a jam or other issue occurs and you cannot quickly fix the issue, the office manager or IT staff should be contacted to resolve the issue.

Standard Configuration
Standard hardware and software configurations are used wherever possible to provide the best levels of reliability for the company network and computers. Other benefits of the standard configuration include the rapid replacement of faulty equipment with spare parts, the tracking of software licenses (as described in the preceding section) and the ability to plan for the implementation of new projects.

The configuration of company computers should not be changed in any way without the prior agreement of Green Bank management. In particular, new hardware devices, new software and upgrades to existing software should only be installed under the guidance of the Green Bank's IT staff.

Data Security
All employees and staff (consultants, third-party contractors, and administrators) are assigned ~~a network~~ usernames and passwords to systems required to perform job functions when they join the company. ~~The network will force employees and staff to change their password at regular intervals, the interval being determined by the network administrator. The network~~ System administrators will ~~also~~ impose ~~other~~ restrictions, such as password length and complexity requirements as well as multifactor authentication where possible.

Employees must select ~~network~~ passwords that cannot be easily guessed or that appear in a standard dictionary. If it is necessary to create a written record of a password, that record should

Formatted: Line spacing: single, No bullets or numbering

never be stored near the employee's desk and never associated with the employee's username. In general, passwords should be memorized and not recorded in writing.

Employees must password-protect all smartphones, tablets and other mobile devices that are paid for by the Green Bank or ~~contain sensitive or confidential business information~~are used to access the Green Bank's systems and information.

See the Information Security Policy for detailed information about security control procedures to safeguard the Green Bank's systems, data and assets.

Privacy
The Green Bank respects your desire to work without the company being overbearing with respect to monitoring and control. However, detailed electronic records about your use of the PC, the network, email, and Internet are created, but not routinely reviewed by the company.

While the company does routinely gather logs for most electronic activities, they will typically be used for the following purposes:

- Cost analysis
- Resource allocation
- Optimum technical management of information resources
- Production analysis
- Detecting patterns of use that indicate users may be violating company policies or engaging in illegal activity

The Green Bank reserves the right, at its discretion, to review any electronic files, logs, and messages to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy and other company policies. This includes the use of spot checks on Internet (Web) use, network files and email without prior notification or user interaction.

Software tools to identify possible breaches of this policy (e.g., highlighting access to websites with unacceptable content or emails containing abusive language) may be used. The results will be reported to the company management and thoroughly investigated where appropriate.

It should not be assumed that internal or external communications are totally private. Accordingly, particularly sensitive information should be transmitted by other means. Therefore, do not use the company network or mobile devices paid for by the Green Bank for personal items that you would not want made public.

Encryption
Only encryption software supplied by the Green Bank for purposes of safeguarding sensitive or confidential business information may be used. People who use encryption files stored on a company computer must provide their manager with a sealed hard copy record (to be retained in a secure location) of all the passwords and/or encryption keys necessary to access the files.

Power-on passwords should not generally be used but if they are, they are required to be approved by IT.

Please note: this means that employees must inform their supervisor of any passwords used to protect individual documents.

File Storage

The Green Bank creates backups of all files stored in Microsoft 365, including in email, SharePoint, OneDrive and Teams. ~~images of all email, server, and network file stores~~. These ~~images~~ backups are stored in a secure location and can be used in the event of:

- Accidental deletion of important material
- A "disaster" necessitating complete recovery of one or more of the company's systems

Data and other files created during the course of an employee's work should, therefore, be stored ~~on the network~~in appropriate locations in Microsoft 365.

Personal Use

Computers and associated equipment are provided by the Green Bank for employee's and staff's business use. The activities on information technology platforms provided by or paid for the Green Bank, including computers, systems, applications, networks, internet connections, smartphones, tablets, and any mobile devices, may be monitored with or without your knowledge. You should have no expectation of privacy regarding the contents contained within such technology or device.

Only limited, occasional and incidental use for personal, non-business purposes is permissible at the discretion of the President. However, please be mindful of prohibited activities as described above in General Guidelines (i.e., shopping, music streaming, etc.) Limited, occasional, or incidental use is defined as use for less than 15 minutes during a workday.

Use of social networking sites (e.g., Facebook, Twitter, LinkedIn) at any time using company provided computers is prohibited, unless it is for company purposes and/or business. While at work, the impact to company resources can impact business operations, but also opens the device to possible security issues.

Personal laptops, cell phones and other internet-enabled items are permitted to be used; however reasonable restrictions of use may be exercised at HR/management discretion. The Green Bank does not provide internet access for public/private use, except on an approved device/user basis. Please advise IT for further detailed instructions before attempting to connect any device to the Green Bank network.

Streaming media (internet Radio, YouTube, Hulu, Pandora, Spotify, etc.) uses significant resources and is prohibited for personal use. Please consider the impact of its use for business purposes only for all devices, including cell phones.

Company locations may provide a freely accessible public Wi-Fi connection that may be used by employees and staff, but the Green Bank absolves itself of any and all damage, liability, etc. that arises from the use of third-party networks. It is the policy of the Green Bank that if an employee chooses to use these third-party connections that they do so on their break, lunch, or after-hours and do not pursue personal activities during business hours.

Contract and freelance staff

The Green Bank will provide agency/temporary, contract/freelance staff with access to computers and the company computer systems for the sole purpose of fulfilling their contractual role with the Green Bank. No personal use by these staff of computer and communication facilities provided by the Green Bank is permitted at any time.

~~Viruses/Spyware~~Security and privacy incidents

Employees should report potential and actual suspicious activity, security incidents and unauthorized disclosure of personal information immediately to the Incident Response Team by sending an email to reportincident@ctgreenbank.com. Employees should provide details that apply to the situation they observed including:

- Date and time of the observed incident
- Location the incident took place
- People, equipment, systems, or data involved
- Describe the incident including events leading up to incident or after the incident
- Identify any other witnesses that may be able to help

It is important that employees never delay in reporting potential or actual security incidents or unauthorized disclosure of personal information. Employees should never hide or tamper with information related to a potential or actual incident.

~~All computer viruses/spyware must be reported immediately to IT. IT~~ Upon receiving notification, the Incident Response Team will work with the assigned system owner/administrator, including the IT vendor as needed, to detect, contain, respond and recover from reported incidents per the Incident Response Plan. ~~is responsible for verifying the updating of virus/spyware detection software from time to time and providing detailed guidelines in the event of a major problem. IT will also investigate any infection and~~ During this process, it is crucial that the Incident Response Team, system owners/administrators, and the IT vendor ~~must~~ receive the full cooperation of all staff in attempting to ~~to identify the source~~perform incident response procedures and minimize harm to the Green Bank. Any attempt to introduce viruses/spyware/malware to the network or systems through malice or negligence will be thoroughly investigated and will be dealt with according to HR guidelines and procedures.

Mobile ~~Device~~ Application Management

Green Bank does not issue mobile telephone devices to employees but may provide tablets to employees or members of the Board of Directors when a business need is present, with the approval of the employee's supervisor and the President and CEO.

Employees are permitted to access Green Bank data (Office 365 products, including Outlook email and Teams phone/chat), using their personal mobile telephone or tablet, or their Green Bank-issued tablet, only if they install the required ~~"Company Portal"~~ mobile application ("app"). The employee should notify Operations and IT of their intention to enroll, then will be prompted to download the app on their phone and/or tablet. Company data is accessed when an employee logs into a site with their Green Bank-issued credentials.

~~Company portal~~The required mobile application is a device management tool. It **does not** allow IT to:

- See an employee's browsing history on their personal device;
- See their personal emails, documents, contacts, or calendar;
- Access their passwords, view, edit, or delete their photos; or,
- See the location of their personal device.

The required mobile application ~~Company portal~~ **does** allow IT to:

- View the model, serial number, and operating system of the device;
- Identify the device by name;
- ~~Reset the lost or stolen device to factory settings;~~
- View information collected by corporate apps and networks; and,
- For corporate devices (i.e., those issued by the Green Bank), see the full phone number associated with the device, see all apps installed, and see its location.

Upon an employee's departure or termination from the Green Bank, IT will remotely eliminate (or "wipe") only data associated with the apps used by the employee for Green Bank business

(e.g., Microsoft Teams, Outlook, Office, OneDrive, or SharePoint) on their mobile device(s). No personal data will be impacted by this action.

It is the employee's responsibility to take care of their device(s) and ensure their safety. If a current employee reports their mobile device(s) lost or stolen, they should notify Operations and the IT vendor immediately. IT will remotely eliminate data associated with the pertinent apps but can only reset the full device to its factory settings with the written permission of the employee.

The Green Bank has a zero-tolerance policy regarding using a cell phone and other mobile devices while driving. For the safety of our employees and others it is imperative that you pull over and stop at a safe location to dial, receive, text or converse on the cell phone in any way. Please consider the use of hands-free devices as allowed by Connecticut State Law.

Mobile devices equipped with cameras require special attention. No photography should occur where confidential information exists, nor where client information is stored. Areas where personal privacy exists (bathrooms, etc.) should be avoided with such devices entirely. Under no circumstances should photography occur at a client location without their permission.

Personal access may be reimbursed by the Green Bank, with the employee's supervisor's approval, if the employee is required to use their personal device outside of normal business hours. Reimbursements will only be made for relevant business-related expenses and not for coverage of any personal applications associated with their mobile plan (e.g., streaming or music subscriptions, etc.). Exceptions can be made by the supervisor based on business need.

Company Data

The Information Technology department is Assigned system owners/administrators and the Operations department are responsible for protecting company data. This includes all data in systems and on the servers, as well as on other devices such as laptops, desktops, mobile devices, and multifunction printers. The IT department backs up all data on the servers on a daily, weekly, and monthly schedule and retains this data under the company-approved Backup Policy.See the Information Security Policy for details on safeguards in place to protect company data, assets and systems.

The following are not permitted:

- Backing up company data on your own.
- Having company data on your personal equipment, this includes the following:
  - Personal PCs laptops or desktops, tablets, smartphones, or other mobile devices.
  - Personal USB devices, such as memory sticks, MP3 players, hard drives, or other recording devices.
- Sending company data via e-mail to your or another Green Bank employee's personal email account.
- Accessing another employee's hardware, computer files or email without prior permission from employee or appropriate manager.
- Sharing your logon password with anyone except the IT staff.
  - The system will ask to reset your password every 90 days.

If you telecommute, all work must be done on company equipment. If you are not using a company-owned laptop, a loaner PC can be arranged through the office manager or IT Operations department department with proper advanced notice to accommodate your needs. No personal devices may be attached to company hardware or used to access company systems and data without prior approval by the IT Operations department (i.e., printers, hard drives, etc.).

It is permissible to transfer items such as presentations and documents to a recording device for the sole purpose of collaboration with approved clients or customers pertaining to company business.

Access to the Internet at the Green Bank is a resource and use thereof is subject to the same rules as other Green Bank resources. It is the responsibility of the user to make sure that all use of the Internet is authorized, appropriate and to the benefit of the Green Bank. Each individual with access to the Internet is responsible for controlling its use. The use of the Internet is a privilege, not a right, which can be revoked at any time.

Social Media
These guidelines apply to Green Bank employees, temporary employees and contractors who create or contribute to blogs, wikis, social networks, virtual worlds, or any other kind of social media for both professional and personal use.

Overview
Social networks are fundamentally changing the way people communicate, conduct research, and make purchasing decisions. As an organization, the Green Bank is engaged in these communities as they are appropriate and relevant to our clients and the Marketing department has developed a strategy for our Social Media Platform. We encourage you to learn how you can use social media to help us share the exciting things we are doing with our clients, uncover new opportunities and strengthen the perception of the Green Bank's staff as innovative professionals—people who work for a company that our clients trust and want to do business with.

Marketing does not exist in a vacuum within the Marketing department; every interaction our clients, prospective clients and partners have with us can strengthen or harm our brand. Therefore, social media should not be thought of just as a marketing tool. While it can be a vehicle for organizations to publish content, it can also be a way for the people who make up those organizations to build and maintain relationships with clients and business partners.

You might be thinking "I already know how to use social media. What else do I need to know?" As the lines between personal and business communications become increasingly blurred, there are a few important points we would like you to consider when using social media in the capacity of your job.

1. You don't have to participate if you don't want to.

Unless you are in marketing, using social media is not likely to be an official part of your job role. We respect that some people prefer not to participate in social networking or are unsure if they want to mix personal and professional networks. Don't worry, there's no pressure to participate.

2. Be honest and transparent about your role.

If you publish something or respond to something about the Green Bank, make sure to include your real name and it is understood that you are a Green Bank employee so there is no conflict of interest. There are several easy ways to do this, such as listing the Green Bank as your place of employment on your profile or starting your comment with something like" "Disclaimer: I work for the Green Bank", but regardless of your method, your audience will appreciate your transparency.

3. Know what the official lines of communication are and when to defer to them.

There is a significant difference between speaking *about* the Green Bank and speaking *on behalf* of the Green Bank. The Green Bank has official means to publish information when it needs to and only a few people are authorized to do so via social media, the press, or any other venue. On your own blogs or social profiles, you can use simple statements such as "The postings on this site are my own and don't necessarily represent the Green Bank's positions, strategies or opinions" to make it clear you are not speaking on behalf of the Green Bank.

If you are not authorized to speak on behalf of the Green Bank and receive requests for official comments or are unsure if you should respond to an inquiry, defer to the Marketing department.

Social media can be a forum for customers to share negative comments about an organization. The Green Bank monitors our social profiles daily and has official means of diffusing and responding to these situations. Our policy is to respond promptly and openly and to take the conversations offline. If you see a negative comment or a situation that concerns you, do not respond directly, but report it to your supervisor and/or Marketing and it will be addressed quickly and professionally.

4. Remember our core values and follow our general code of conduct.

You should use your best judgment and consider the Green Bank's values of integrity, accountability, and professionalism as a guide for your conduct in online communities, just as they are a guide for other professional behavior. You are personally responsible for the content you post on any social network. These forums are public, are often searched and indexed, and should be treated as though they will be available for public viewing forever. If you aren't sure whether certain content should be published or discussed, ask before you post.

Know and follow our Code of Conduct and never share any confidential or proprietary information belonging to the Green Bank or any other organization. Never comment on anything related to legal matters, litigation, or any parties the Green Bank may be in litigation with. Postings must respect copyright, privacy, fair use, financial disclosure, and other applicable laws. Only Marketing may post or authorize the posting of pictures, videos, and other media produced on the business premises or outside events. The Green Bank reserves the right to request that certain subjects be avoided, withdraw certain posts, and remove inappropriate comments. If such employee denies or does not comply, proper legal action will be taken. When in doubt, feel free to run by Marketing or Human Resources.

5. Think before you post.

Use common sense when it comes to verbiage and tone in written online content. While social media is, in some cases, less formal than traditional business communications, the Green Bank uses social media as a professional extension of our business. Do not use ethnic slurs, insults, or otherwise inappropriate and unprofessional language that would not be acceptable in the workplace. Respect the privacy of others and avoid potentially inflammatory topics.

Above all else, seek to add value in your participation. Our clients are looking for your information, insight, and expert perspective. Bashing competitors and posting negative comments about work, our clients, or our partners violates our Code of Conduct and adds nothing positive to an online dialogue. Think before you post and ask yourself if you are making a situation better or worse by doing so. Answering questions, sharing resources, and talking about your experiences are a great way to add value.

6. Online activities should not interfere with your job.

Social media, like, the Internet, can quickly change from a worthwhile tool to a distraction. Make sure your online activities do not interfere with your job or your commitments to our clients. In addition, social media sites may not be accessed on company hardware for personal reasons.

All employees must review these policies and sign the Information Technologies Policies acknowledgement form found in the Appendix and return it to Human Resources.

Solicitation and Distribution

All Green Bank employees are entitled to the opportunity to perform their work without being bothered or disturbed. Accordingly, we have adopted the following solicitation and distribution rule.

Non-Employees
Anyone who is not an employee of the Green Bank is prohibited from soliciting or distributing literature on Green Bank premises at any time.

Employees
The Green Bank's Solicitation and Distribution policy as it relates to current employees is as follows:

- Employees may not engage in solicitation or distribution of literature during working time. "Working time" means actual working time during the workday and includes both the working times of an employee doing the soliciting or of an employee being solicited. Working time does not include lunch periods, work breaks, or any other period in which employees are not on duty.
- Employees may not distribute literature concerning matters other than those directly related to Green Bank business in work areas at any time.
- Employees may not engage in verbal solicitation or distribution of literature at any time in those areas normally frequented by clients carrying on Green Bank business.

Bulletin Boards

Bulletin boards are important as communications tools to alert you to Green Bank programs and activities. The posting of written solicitations of any kind on bulletin boards is restricted. Only notices relating to Green Bank-sponsored activities may be posted on bulletin boards. These bulletin boards display important information, and employees should consult them frequently for:

- Employee announcements
- Internal memoranda
- Job openings
- Organization announcement.
- Workplace Violence Policy Memorandum

VIOLENCE IN THE WORKPLACE PREVENTION POLICY SUMMARY

Below is the Green Bank's policy concerning workplace violence and prohibiting weapons and dangerous instruments in the workplace.

The policy is consistent with what has been called a "Zero Tolerance" approach. Violence or the threat of violence by or against any employee of the State of Connecticut, including the Green Bank, is unacceptable and will subject the perpetrator to serious disciplinary action and possible criminal charges.

The Green Bank is committed to providing its employees a safe and healthy work environment, free from intimidation, harassment, threats, and/or violent acts.

The worksite is any location, either permanent or temporary, where an employee performs any work-related duty. This includes but is not limited to the building and the surrounding perimeter, including the parking lot. It includes all state-owned and leased space, including vehicles and any location where state business is conducted.

According to the National Institute for Occupational Safety and Health (NIOSH), workplace violence is defined as:

"any physical assault, threatening behavior or verbal abuse occurring in the work setting. It includes, but is not limited to beatings, stabbings, suicides, shootings, rapes, near suicides, psychological traumas such as threats, obscene phone calls, an intimidating presence, and harassment of any nature such as being followed, sworn at, or shouted at."

There is no such thing as a "joke" when dealing with this subject. It is not funny when employees speak about "going postal", "getting" another employee or anything remotely similar.

Do not ignore violent, threatening, harassing, intimidating, or other disruptive behavior. If you observe or experience such behavior by anyone on Authority premises, whether they are a Green Bank employee or not, report it immediately to a supervisor or manager.

The cooperation of all Green Bank staff is needed to implement this policy effectively and maintain a safe working environment.

VIOLENCE IN THE WORKPLACE PREVENTION POLICY (Continued)

The State of Connecticut has adopted a statewide zero tolerance policy for workplace violence. The Connecticut Green Bank fully supports this policy and recognizes the right of its employees to work in a safe and secure environment that is characterized by respect and professionalism.

Prohibited Conduct

Except as may be required as a condition of employment:

No employee shall bring into any state worksite any weapon or dangerous instrument as defined herein.

No employee shall use, attempt to use, or threaten to use any such weapon or dangerous instrument in a state worksite.

No employee shall cause or threaten to cause death or physical injury to any individual in a state worksite.

In addition, the Connecticut Green Bank prohibits all conduct, either verbal or physical, that is abusive, threatening, intimidating, or demeaning.

Definitions

"Weapon" means any firearm, including a BB gun, whether loaded or unloaded, any knife (excluding a small pen or pocketknife), including a switchblade or other knife having an automatic spring release device, a stiletto, any police baton or nightstick, or any martial arts weapon or electronic defense weapon.

"Dangerous instrument" means any instrument, article, or substance that, under the circumstances, is capable of causing death or serious physical injury.

Confiscation of Weapons and Dangerous Instruments

Any weapon or dangerous instrument at the worksite will be confiscated and there is no reasonable expectation of privacy with respect to such items in the workplace.

Reporting Procedures

Emergency Situations: Any employee who believes that there is a serious threat to their safety or the safety of others that requires immediate attention should contact **911**. The employee must also contact their **immediate supervisor** or **Human Resources** at (860) 258-7861 or the Managing Director of Operations at 860-257-2897.

Please note that when 911 is dialed from a hard line, the local police authority will respond. When dialing from a cell phone, 911 will connect you directly to the nearest State Police Troop.

Non-Emergency Situations: any employee who feels subjected to or witnesses violent, threatening, harassing, or intimidating behavior in the workplace should immediately report the incident or statement to their supervisor or manager or Human Resources.

Supervisors/Managers Responsibilities: Any manager or supervisor who receives a report of violent, threatening, harassing, or intimidating behavior shall immediately contact the Human Resources Office so that office may evaluate, investigate, and take appropriate action.

Investigation and Corrective Action

The Green Bank will promptly investigate all reports or alleged incidents of violent, threatening, harassing, or intimidating behavior.

All employees are expected to cooperate fully in all such investigations.

Any employee suspected of violating this policy may be placed immediately on administrative leave pending the results of the investigation.

If the claims of violent, threatening, harassing, or intimidating conduct are substantiated, or if it is found that the employee has otherwise violated this policy, the employee will be dealt with through the appropriate disciplinary process, and may be subject to discipline up to and including dismissal from the Green Bank.

Where the situation warrants, the Green Bank will request that the appropriate law enforcement agencies become involved in the investigation of the matter, and the Green Bank may seek prosecution of conduct that violates the law.

Enforcement of the Policy

This policy will be prominently posted for all agency employees.

President & CEO

Disciplinary Procedure

The Green Bank believes each employee should be treated and respected as an individual. Therefore, employee misconduct is approached in a case-by-case manner. Some infractions are more serious than others are and an employee's length of service, work record, and prior conduct are all important in determining the proper disciplinary action. It is our general practice to use progressive disciplinary counseling procedures between the employee and their immediate supervisor, in which the supervisor will explain the allegations and allow the employee to explain their position. In all phases of the disciplinary procedure, the Green Bank will make reasonable efforts to give the employee the opportunity to make their position clear, orally or in writing. Some serious incidents of misconduct may require immediate discharge from employment, but whenever possible, misconduct will be approached with counseling before termination of employment is considered. The primary purpose of discipline is remedial, not punitive. When possible and appropriate the steps of progressive discipline will be as follows:

1. A verbal (oral) warning giving clear guidelines for corrective action and potential consequences.
2. A written warning with the infraction and required corrective action specified.
3. A written reprimand is issued when the employee has been warned and the problem behavior has not been corrected.
4. A suspension without pay serves as the last resort prior to discharge.
5. A demotion results when an employee is willing but unable to perform assigned duties.
6. A termination of employment usually follows prior disciplinary steps or for a serious rule violation.

When disciplinary action is required upon the recommendation of the Supervisor, the President and CEO and/or their designee may elect a written reprimand, suspension without pay demotion, disciplinary probation, or dismissal. The President and CEO and/or their designee may take any such disciplinary action after the evaluation process determines that an employee's performance and/or conduct is unacceptable, taking any mitigating circumstances into account. A record of the written reprimand or documentation of other disciplinary action will be made a permanent part of the employee's personnel file.

Management reserves the right to enter into any level of disciplinary action or termination based upon the severity of the offense requiring discipline and the employee's past work record. This policy in no way alters the at-will employment policy; the employee or the Green Bank may terminate the employment relationship at any time and for any reason.

Employment Termination

Termination of employment is an inevitable part of personnel activity within any organization, and many of the reasons for termination are routine. Below are examples of some of the most common circumstances under which employment is terminated:

Resignation
Employment termination initiated by an employee who chooses to leave the Green Bank voluntarily.

Discharge
Employment termination initiated by the Green Bank.

Layoff
Involuntary employment termination initiated by the Green Bank for non-disciplinary reasons.

Retirement
Voluntary retirement from active employment status initiated by the employee.

Exit Interview
The Green Bank will generally schedule exit interviews at the time of employment termination. The exit interview will afford an opportunity to discuss such issues as employee benefits, conversion privileges, repayment of outstanding debts to the Green Bank, return of CI-owned property, and assuring that necessary assignments are completed. Suggestions, complaints, and questions can also be voiced.

Employee benefits will be affected by employment termination in the following manner. All accrued, vested benefits that are due and payable at termination will be paid. Some benefits may be continued at the employee's expense if the employee so chooses. The employee will be notified in writing of the benefits that may be continued and of the terms, conditions, and limitations of such continuance

Grievance Procedure

Supervisors are responsible for being accessible and for regularly discussing working conditions, job performance, or any other concern an employee has about their job at the Green Bank making reasonable efforts to address problems and concerns. Our success depends upon maintaining clear and open communication with employees. It is of utmost importance to respond to complaints, problems, or anything employees deem unfair or unacceptable. Each employee should feel free to discuss any complaint or problem with their immediate supervisor. This initial step in the grievance procedure is informal to encourage a quick resolution. No employee will be penalized or discriminated against for bringing up a problem or registering a grievance regardless of the nature of the complaint.

Grievances Not Involving Discrimination or Sexual Harassment
If an employee has a grievance that remains unresolved in informal discussions with their supervisor, they should make a scheduled, recorded appointment with their supervisor to discuss the problem. The employee and supervisor should keep a written record of this discussion.

If a settlement satisfactory to both parties cannot be reached, the employee and their supervisor should submit the grievance in writing to the President and CEO and/or their designee, attaching their written records of the meeting. The President and CEO and/or their designee will schedule a meeting with the employee and the supervisor within five (5) working days of receipt of the grievance. A written record of this meeting will also be kept, and the President and CEO and/or their designee will render a decision within three (3) working days after the meeting.

In the event the employee is not satisfied with the decision of the President and CEO and/or their designee, they may request a hearing before the Board of Director's Budget and Operations Committee. The decision of the Budget, Operations, and Compensation Committee shall be final.

Grievances Involving Discrimination or Sexual Harassment
Any employee who feels they would like counseling about possible violations of the Green Bank's affirmative action or anti-harassment policies, or any state or federal statutes related to Equal Employment Opportunity (EEO), Affirmative Action (AA), or Sexual Harassment should contact Human Resources. This counseling will be kept confidential and no related information

will be released except upon signed consent of the employee or as necessary for the Green Bank to comply or fulfill its obligations under federal or state law. Human Resources will provide information on state, federal agencies and Green Bank resources available to employees who wish to pursue a grievance regarding discrimination.

If a grievance involves sexual harassment by the employee's supervisor, or if there are other circumstances that make it impossible for the employee to initially address a grievance directly to the supervisor, they may schedule the initial meeting with the President and CEO and/or their designee. If the employee's supervisor is the President and CEO and/or their designee, the grievance may be directed to the Budget and Operations Committee.

Grievance Procedure Contacts

Separate and independent from the above process, the complainant may file written complaints of discrimination with:

The Connecticut Commission on Human Rights and Opportunities (CHRO)
21 Grand St, Hartford, CT 06106
Phone: (860) 541-3400

The Equal Employment Opportunity Commission (EEOC)
150 Causeway St, Boston, MA. 02114
Phone (617) 565-3214

Department of Justice (DOJ)
Office on the Americans with Disabilities Act
Civil Rights Division, P.O. Box 66118, Washington, D.C. 20507
Phone (202) 514-0301.

Employees may also file complaints with any other agencies, state, federal or local, including the United States Department of Labor, Wage and Hour Division, that enforce laws concerning discrimination in employment. Employees should be aware that there are statutes of limitations that require complaints be filed by a certain time period or the employee may forfeit their rights. Employees may inquire further with the respective agency.

No individual who files a complaint, or who cooperates or testifies in the investigation of a complaint, shall be unlawfully retaliated against for the exercising of their legal rights.

Whistleblower Policy

Any person having knowledge of corruption, unethical practices, violation of state laws or regulations, mismanagement, gross waste of funds, abuse of authority, or danger to the public safety occurring within the Green Bank or in a related contract with the Green Bank may disclose such matter to any member of the Audit, Compliance and Governance Committee of the Green Bank or the state Auditors of Public Accounts. A person disclosing such information is known in lay terms as a "whistleblower." A whistleblower should feel free to report such information without fear of retaliation.

No Green Bank officer or employee, may take or threaten to take any personnel action against a whistleblower who is an employee of the Green Bank in retaliation for disclosing such information. Whistleblower's protection applies to any Green Bank employee who discloses such information:

(1) to any employee of the Auditors or of the Attorney General.
(2) to any member of the Audit, Compliance and Governance committee of the Green Bank.
(3) to an employee of the state or quasi-public agency that employs the person who retaliated or threatened retaliation.
(4) to an employee of a state agency pursuant to a mandated reporter statute; or,
(5) in the case of a large state contractor, to an employee of the contracting state agency concerning information about a large state contract.

A Green Bank employee who believes they are the subject of retaliation for "whistleblowing" may file a "whistleblower retaliation complaint" with the Chief Human Rights Referee at the CHRO's Office of Public Hearings not later than thirty (30) days after the employee learns of the specific incident giving rise to the claim (i.e., the personnel action threatened or taken against him/her). An employee who believes that they have been retaliated against should contact a private attorney to discuss their rights. The Attorney General cannot provide legal advice or counsel.

The Green Bank's guidelines for making whistleblower complaints are set forth below.

- File a written complaint or verbal complaint with the President and CEO and/or the Ethics Officer, and or the Green Bank's Audit, Compliance, and Governance Committee. Employees may also choose to file a written complaint or make a telephone complaint with the Auditors of Public Accounts. All complaints should be filed in writing with the Auditors of Public Accounts, 210 Capitol Avenue, Hartford, CT 06106, or by telephone: Toll Free within Connecticut: (800) 797-1702 or Locally: (860) 240-5305. If the employee wishes to remain anonymous, they may.
- Whistleblower complaints will be referred to the Green Bank's Audit, Compliance, and Governance Committee for review. That committee will serve as the primary contact between the Green Bank and the Auditors of Public Accounts.

Employees can visit Auditors of Public Accounts website for more information about filing a complaint. In addition, employees may visit the Commission on Human Rights and Opportunities website for information regarding the processes and procedures in the administration of whistleblower retaliation complaints.

THE CONNECTICUT GREEN BANK ETHICAL CONDUCT POLICY

I. Introduction

Ethical conduct is a core value of The Connecticut Green Bank ("Green Bank") and all employees and officials of the Green Bank are expected to maintain the highest professional standards in the conduct of their duties. In particular, each person is responsible for, and should become familiar with, the Code of Ethics for Public Officials. A copy of the "Guide to the Code of Ethics for Public Officials" is attached here. You may also access both the Code and the guide on the Office of State Ethics website at www.ct.gov/ethics by clicking on "Public Information".

II. Code of Ethics Compliance

Principle provisions of the Code of Ethics for Public Officials include:

- **GIFTS -** In general, state employees are prohibited from accepting gifts from anyone doing business with, seeking to do business with, or directly regulated by the state employee's agency or department or from persons known to be a registered lobbyist or lobbyist's representative. There are also restrictions on gifts between state employees in certain circumstances. (See the "Guide to the Code of Ethics for Public Officials" and Statutory References below, Sections 1-79(e) and 1-84(m).)
- **FINANCIAL BENEFIT -** A state employee is prohibited from using their office or non-public information obtained in state service for the financial benefit of the individual, certain family members, or that of an associated business.
- **OUTSIDE EMPLOYMENT -** A state employee may not accept outside employment which will impair their independence of judgment as to official state duties or which would induce the disclosure of confidential information. Generally, outside employment is barred if the private employer can benefit from the state employee's official actions.
- **FINANCIAL DISCLOSURE -** Certain state employees are required to file a financial disclosure statement with the State Ethics Commission. This statement will be considered public information.
- **RECUSAL OR REPORTING IN CASE OF POTENTIAL CONFLICTS –** The Code of Ethics requires that public officials and state employees avoid potential conflicts of interest. If a public official or state employee would be required to take official action that would affect a financial interest of such public official or state employee, certain family members or a business with which they are associated, they must excuse themselves from the matter or prepare and file a sworn written statement explaining why continued involvement in the matter would be on an objective basis and in the public interest despite the potential conflict. (See Statutory References below, Section 1-86(a).)

III. Additional Green Bank Policies

The Green Bank expects that, in addition to complying with all provisions of the Code of Ethics for Public officials, employees and officials will:

- Protect the confidential information to which the Green Bank has access.
- Avoid actual or potential conflicts of interest.
- Neither interfere with nor solicit contracts on behalf of any person.

- Avoid, in the case of employees, outside employment which may compromise or interfere with the ability to perform duties for the Green Bank; and
- For those employees subject to the requirements of C.G.S. 1-83(a), submit the Statement of Financial Interests disclosure documents to the Office of State Ethics in a timely manner.

For the same reasons, and in order to maintain public confidence and avoid even an appearance of impropriety

- Green Bank employees and members of their immediate families are prohibited from investing in companies that receive financial assistance from the Green Bank; and
- If an application for financial assistance from the Green Bank is received from a business with which a Green Bank employee is associated, or in which such employee or an immediate family member has a direct financial interest, such employee, whether or not they expect to be involved in the processing or consideration of such application, shall notify the President of such business association or financial interest and such employee shall be sequestered from all information, discussions, actions and other activities related to such application. For this purpose, a business with which such employee is associated has the same meaning assigned in Section 1-79 of the Code of Ethics to the phrase "business with which he is associated". (See Statutory References below, Section 1-79(b).)

For these purposes, the Green Bank may post a "restricted list" of companies in which employees may not invest and may require employees to disclose outside business interests. The rules of conduct in these matters may also be covered in more detail in the Green Bank's Handbook.

IV. Post-State Employment Restrictions

Employees leaving the Connecticut Green Bank are required to comply with the Code of Ethics provisions pertaining to post-state employment, which are commonly known as the "revolving door" provisions. For example, there are restrictions on accepting employment with a party to certain contracts (which would include contracts relating to investments or other financial assistance) if the employee or official were involved in the negotiation or award of the contract, and restrictions on representing other parties before the Green Bank during the one-year period following departure from state service. Employees should familiarize themselves with the statutes pertaining to post-state employment. They can be found at C.G.S. Section 1-84a and 1-84b. (See Statutory References below.) You may access these statutes on the Office of State Ethics website at www.ct.gov/ethics by clicking on "Statutes and Regulations". A summary of these requirements is included in the "Guide to the Code of Ethics for Public Officials and State Employees" attached to this ethics policy.

Before an employee leaves the employment of The Connecticut Green Bank, an exit interview will be conducted by our Ethics Liaison Officer. The purpose of this exit interview will be to individually review potential issues relating to post-Connecticut Green Bank employment.

V. Other Matters

The Board of the Connecticut Green Bank continues to have well-justified faith in the integrity and ethical conduct of employees and officials of the Connecticut Green Bank. It is understood however, that breaches of this ethics policy may require disciplinary action, including but not

limited to dismissal from the Green Bank, in addition to sanctions provided by state law. Such sanctions are to be applied as appropriate with the approval of the Connecticut Green Bank Board of Directors.

It is the responsibility of each employee and official to inquire of the Ethics Liaison Officer or the Office of State Ethics at 860.566.4472 should any question arise concerning their conduct.

VI. Statutory References

Sec. 1-79. Definitions. The following terms, when used in this part, shall have the following meanings unless the context otherwise requires:

(b) "Business with which he is associated" means any sole proprietorship, partnership, firm, corporation, trust or other entity through which business for profit or not for profit is conducted in which the public official or state employee or member of his immediate family is a director, officer, owner, limited or general partner, beneficiary of a trust or holder of stock constituting five per cent or more of the total outstanding stock of any class, provided, a public official or state employee, or member of his immediate family, shall not be deemed to be associated with a not for profit entity solely by virtue of the fact that the public official or state employee or member of his immediate family is an unpaid director or officer of the not for profit entity. "Officer" refers only to the president, executive or senior vice president or treasurer of such business.

(e) "Gift" means anything of value, which is directly and personally received, unless consideration of equal or greater value is given in return. "Gift" shall not include:

(1) A political contribution otherwise reported as required by law or a donation or payment as described in subdivision (9) or (10) of subsection (b) of section 9-601a;

(2) Services provided by persons volunteering their time, if provided to aid or promote the success or defeat of any political party, any candidate or candidates for public office or the position of convention delegate or town committee member or any referendum question;

(3) A commercially reasonable loan made on terms not more favorable than loans made in the ordinary course of business;

(4) A gift received from (A) an individual's spouse, fiancé or fiancée, (B) the parent, brother or sister of such spouse or such individual, or (C) the child of such individual or the spouse of such child;

(5) Goods or services (A) which are provided to a state agency or quasi-public agency (i) for use on state or quasi-public agency property, or (ii) that support an event, and (B) which facilitate state or quasi-public agency action or functions. As used in this subdivision, "state property" means (i) property owned by the state or a quasi-public agency, or (ii) property leased to a state agency or quasi-public agency;

(6) A certificate, plaque or other ceremonial award costing less than one hundred dollars;

(7) A rebate, discount or promotional item available to the general public;

(8) Printed or recorded informational material germane to state action or functions;

(9) Food or beverage or both, costing less than fifty dollars in the aggregate per recipient in a

calendar year, and consumed on an occasion or occasions at which the person paying, directly or indirectly, for the food or beverage, or his representative, is in attendance;

(10) Food or beverage or both, costing less than fifty dollars per person and consumed at a publicly noticed legislative reception to which all members of the General Assembly are invited and which is hosted not more than once in any calendar year by a lobbyist or business organization. For the purposes of such limit, (A) a reception hosted by a lobbyist who is an individual shall be deemed to have also been hosted by the business organization which he owns or is employed by, and (B) a reception hosted by a business organization shall be deemed to have also been hosted by all owners and employees of the business organization who are lobbyists. In making the calculation for the purposes of such fifty-dollar limit, the donor shall divide the amount spent on food and beverage by the number of persons whom the donor reasonably expects to attend the reception;

(11) Food or beverage or both, costing less than fifty dollars per person and consumed at a publicly noticed reception to which all members of the General Assembly from a region of the state are invited and which is hosted not more than once in any calendar year by a lobbyist or business organization. For the purposes of such limit, (A) a reception hosted by a lobbyist who is an individual shall be deemed to have also been hosted by the business organization which he owns or is employed by, and (B) a reception hosted by a business organization shall be deemed to have also been hosted by all owners and employees of the business organization who are lobbyists. In making the calculation for the purposes of such fifty-dollar limit, the donor shall divide the amount spent on food and beverage by the number of persons whom the donor reasonably expects to attend the reception. As used in this subdivision, "region of the state" means the established geographic service area of the organization hosting the reception;

(12) A gift, including but not limited to, food or beverage or both, provided by an individual for the celebration of a major life event **[Not an available exception; see Section 1-84(m) below]**;

(13) Gifts costing less than one hundred dollars in the aggregate or food or beverage provided at a hospitality suite at a meeting or conference of an interstate legislative association, by a person who is not a registrant or is not doing business with the state of Connecticut;

(14) Admission to a charitable or civic event, including food and beverage provided at such event, but excluding lodging or travel expenses, at which a public official or state employee participates in his official capacity, provided such admission is provided by the primary sponsoring entity;

(15) Anything of value provided by an employer of (A) a public official, (B) a state employee, or (C) a spouse of a public official or state employee, to such official, employee or spouse, provided such benefits are customarily and ordinarily provided to others in similar circumstances;

(16) Anything having a value of not more than ten dollars, provided the aggregate value of all things provided by a donor to a recipient under this subdivision in any calendar year shall not exceed fifty dollars; or

(17) Training that is provided by a vendor for a product purchased by a state or quasi-public agency which is offered to all customers of such vendor.

Section 1-84 Prohibited Activities

(m) No public official or state employee shall knowingly accept, directly or indirectly, any gift, as defined in subsection (e) of section 1-79, from any person the official or employee knows or has reason to know: (1) Is doing business with or seeking to do business with the department or agency in which the official or employee is employed; (2) is engaged in activities which are directly regulated by such department or agency; or (3) is prequalified under section 4a-100. No person shall knowingly give, directly or indirectly, any gift or gifts in violation of this provision. For the purposes of this subsection, the exclusion to the term "gift" in subdivision (12) of subsection (e) of section 1-79 for a gift for the celebration of a major life event shall not apply. Any person prohibited from making a gift under this subsection shall report to the State Ethics Commission any solicitation of a gift from such person by a state employee or public official.

Section 1-84a. Disclosure or use of confidential information by former official or employee

No former executive or legislative branch or quasi-public agency public official or state employee shall disclose or use confidential information acquired in the course of and by reason of his official duties, for financial gain for himself or another person.

Sec. 1-84b. Certain activities restricted after leaving public office or employment

(a) No former executive branch or quasi-public agency public official or state employee shall represent anyone other than the state, concerning any particular matter (1) in which he participated personally and substantially while in state service, and (2) in which the state has a substantial interest.

(b) No former executive branch or quasi-public agency public official or state employee shall, for one year after leaving state service, represent anyone, other than the state, for compensation before the department, agency, board, commission, council or office in which he served at the time of his termination of service, concerning any matter in which the state has a substantial interest. The provisions of this subsection shall not apply to an attorney who is a former employee of the Division of Criminal Justice, with respect to any representation in a matter under the jurisdiction of a court.

(f) No former public official or state employee (1) who participated substantially in the negotiation or award of (A) a state contract valued at an amount of fifty thousand dollars or more, or (B) a written agreement for the approval of a payroll deduction slot described in section 3-123g, or (2) who supervised the negotiation or award of such a contract or agreement, shall accept employment with a party to the contract or agreement other than the state for a period of one year after his resignation from his state office or position if his resignation occurs less than one year after the contract or agreement is signed.

(g) No member or director of a quasi-public agency who participates substantially in the negotiation or award of a contract valued at an amount of fifty thousand dollars or more, or who supervised the negotiation or award of such a contract, shall seek, accept, or hold employment with a party to the contract for a period of one year after the signing of the contract.

SECTION 8: HEALTH AND SAFETY

Health and Safety

Each employee is expected to share our commitment to a safe workplace. This obligation means that safe working habits and principles must be followed. All employees are expected to exercise common sense and good housekeeping practices. For the sake of all our employees and clients, safety concerns must be taken seriously. Every employee is expected to take a proactive role in providing a safe workplace. Horseplay or other unsafe activity is prohibited. Every employee must report any injury, no matter how slight, immediately to their supervisor. Such reports are necessary to initiate any necessary emergency procedures, to comply with workers compensation laws, and to initiate insurance and workers compensation benefits procedures.

First-aid kits containing items needed for most minor first-aid situations are maintained throughout the building. All employees should make a note of their locations. Each employee is expected to exercise safe working habits and reasonable caution in all work activities. Any unsafe condition must be reported immediately to the appropriate supervisor. Employees who violate safety standards, who cause hazardous or dangerous situations, or who fail to report, or where appropriate, remedy such situations, may be subject to disciplinary action.

Policy On Life-Threatening and Communicable Diseases

This policy provides guidance for dealing with work situations involving employees, who have life threatening and communicable diseases, including but not limited to:

- Acquired Immune Deficiency Syndrome (AIDS).
- Human Immunodeficiency Virus (HIV) infection.
- HIV related illness as defined by the Connecticut General Statutes Section l9a58 1; or
- Any other life threatening and communicable disease.

Non-Discrimination
The Green Bank does not unlawfully discriminate against qualified individuals with life-threatening and communicable diseases in any terms or conditions of employment.

It is our policy that individuals with life-threatening and communicable diseases will be treated with the same compassion and consideration given to any employee with a health problem. No person will be treated differently in the workplace as a result of having or being perceived as having such a disease.

No H.I.V. Or Aids Testing
Present or prospective employees will not be required to submit to an AIDS or HIV-related test as a condition of hiring or continued employment.

Ability To Work
The Green Bank recognizes that employees with life-threatening and communicable diseases may require a reasonable accommodation to perform their job duties. It is the Green Bank's policy to accommodate these employees by allowing them to work as long as they are able to perform their essential job functions, with or without reasonable accommodation, provided that medical evidence indicates that their conditions do not pose a direct threat to themselves or others.

Employee Health and Safety

The Green Bank also recognizes its obligation to provide a safe and healthy work environment for all employees. Therefore, the Green Bank may obtain appropriate medical direction, when necessary, to ensure that an employee's condition does not pose a significant risk of substantial harm to him/herself or to other employees or customers of the Agency.

Confidentiality

All employee records or information regarding life-threatening and communicable diseases will be confidentially maintained in the Human Resources Office in a secure area, apart from the employee's personnel file.

Drug and Alcohol Policy

The Green Bank is committed to maintaining a substance-free, healthful, and safe work environment. To promote this goal employees are required to report to work in appropriate mental and physical condition to perform their jobs in a satisfactory manner. Employees are forbidden to use, possess, consume, manufacture, distribute, purchase, sell, or be under the influence of alcohol, illegal drugs, or controlled substances during working hours, whether on the premises, or representing or conducting the business of the Green Bank elsewhere. Reporting to work under the influence of alcohol or illegal drugs or being in possession of alcoholic beverages or illegal drugs on the Green Bank's premises will not be tolerated. Such conduct is also prohibited during non-working time to the extent that, in the Green Bank's opinion, it impairs an employee's ability to perform on the job or threatens the reputation or integrity of the Green Bank.

The legal use of physician-prescribed, or legal over-the-counter drugs is permitted on the job if it does not impair an employee's ability to perform the essential functions of the job effectively and in a safe manner that does not endanger other employees or clients. Any employee taking any legal or prescribed drugs known to have possible side effects that affect or impair judgment, coordination, or other senses, or that might adversely affect the employee's ability to perform normal work in a safe and productive manner, must notify their supervisor or other manager before commencing work. Information provided by the employee concerning the use of medication will be treated in a confidential manner. If the Green Bank has reasonable cause to believe an employee is adversely affected by the use of a drug or medication such that a threat is posed to the safety of the employee, other persons, or to property, the employee may be denied permission to continue working pending further investigation. The investigation will be conducted expeditiously, with the resulting information treated confidentially to the extent possible.

An employee whose job performance has deteriorated through the use of alcohol and/or drugs to the extent that termination of employment is being considered may opt to enter an approved treatment facility of their choice. Upon successful completion of treatment, the employee may be permitted to resume normal employment.

Employees must give notification in writing to Human Resources within five (5) calendar days of any drug conviction for violation of a criminal drug statute if the violation occurred in the workplace. Employees who have substance abuse problems are encouraged to participate in a rehabilitation program prior to any disciplinary action. If an employee chooses not to undergo rehabilitation, the Green Bank will take disciplinary action consistent with state law and regulation within 30 calendar days of receiving notice of the conviction. A conviction means a finding of guilt including a plea of nolo contendere, or the imposition of a sentence by a judge or jury in any federal or state court.

Violations of any part of this policy may lead to disciplinary action, up to and including immediate termination of employment. Such violations may also have legal consequences.

Smoking Policy

The health and well-being of staff and visitors to the Green Bank are primary concerns of management. The Environmental Protection Agency has released a report officially concluding that secondhand smoke is a Class A human carcinogen. It is also known that secondhand smoke causes respiratory illness and is suspected to be even more dangerous in its link with heart problems.

In order to protect the health of those who use our building, smoking or other use of tobacco products is prohibited in any offices or work areas within the Green Bank. Smoking is permitted only out-of-doors.

Emergency Procedures

Emergencies can occur at any time, and we need to be prepared to handle such situations to minimize injury and damage. The following information is designed to assist you in preparing for and handling an emergency.

Emergency Phone Numbers

Hartford Police	**911** or **860-757-4000** (Routine calls)
Hartford Fire	**911** or **860-757-4500** (Routine calls)
Stamford Police	**911** or 203-977-4444
Stamford Fire/Ambulance	**911**
Health Emergencies	**911** (this alerts CT Green Bank first responders to a Teams call being made to 911)

Medical Emergency Procedures for Staff

When dialing 911, Green Bank first responders are alerted that you have placed a call to 911. A paging system is no longer available since moving phones to Teams. TEAMS First Responders Notification Group is FirstReponders@Ctgreenbank.com.

If the person is unconscious, not responsive, seriously injured or in apparent serious distress, immediately dial 911.
(This will always be a personal judgment call and do not worry about calling unnecessarily.)
Please use the **Teams phone (not cell)** if possible as this triggers an in-house and police alert, and also sends message to the Green Bank's first responders.

First Responders Team Actions

Always know that if YOU are in distress and call 911 the first responders are also notified that you are calling 911. Do not hesitate to use this in an emergency.

1. Response Team Members will go directly to code red location immediately. Follow trained response.
2. In route to location, pick-up **AED unit --portable First Aid Kit** --notebook and Emergency Bag.
   Hartford Office Location: Wall mount outside of Greta Thunberg Huddle Room before

hallway to Café.
Stamford Office Location: Wall mount in kitchen.

3. If 911 has not yet been called, Green Bank trained staff will decide whether or not to call **911** directly or ask someone to do so and report the nature of the emergency and location. (Best to call in the presence of the victim if at all possible so information can be relayed to EMTs.)

One or two Response Team members will assess the situation and take the lead in providing necessary response. Remaining team members will provide the following:

1. Set-up AED for use, if needed.
2. Prepare for CPR relief, if needed. 3 to 5 minutes is desired.
3. Provide Privacy/Crowd Control, request non-response team personnel to evacuate the area until all is clear.
4. Meet and direct medical personnel to emergency location.
5. Once the Emergency Medical Team (EMT) has arrived the duties and responsibilities are transferred to them. They may take AED with them.
6. Provide necessary information and any other support needed by the EMT.
7. Contact necessary family member(s) of victim. (List at AED location)
8. See that victim is accompanied to ER when applicable.
9. Provide follow-up report to Human Resources Designee.

Medical Emergency Procedure for all Personnel
Response team members will go directly to red code location and follow trained response instructions. If possible while in route to location, pick-up AED unit and portable First Aid Kit located inside the AED unit box mounted on the main hallway wall outside of the Greta Thunberg Room in Hartford, or kitchen in Stamford.

1. Response team evaluates situation and does one or all of the following:
    a. Call 911
    b. Team will activate procedure for 911.
2. Keep lines open for further communication.

A list of all family emergency numbers for staff is available and found inside of each office's defibrillator cabinet.

Fire

In order to minimize property damage and possible loss of life, familiarize yourself with the building's fire prevention system. Know the location of fire alarm pull stations and fire extinguishers and familiarize yourself with the instructions on the extinguishers. Signs are posted throughout both offices for exits and outside meeting locations where staff need to gather.

WHEN THE FIRE ALARM IS HEARD:

- EVERYONE SHOULD IMMEDIATELY STOP WHAT THEY ARE DOING.
- EVACUATE THE BUILDING IN A CALM, ORDERLY MANNER TO A CENTRAL LOCATION AT LEAST 300 FEET FROM THE BUILDING.
- Do Not Stop to Gather Belongings.
- Follow Emergency Exit Signs to Exit Building.
- Sweepers will sweep the office in their assigned areas, including common areas and bathrooms. Check offices and cubicles as you leave your area.
- Sign-in iPad should be picked up and taken to company gathering place.
- ALL DEPARTMENTS AND TENANTS:
  Hartford Office—gather in the Capewell Lofts parking lot area directly opposite the Green Bank reserved parking spaces.
  Stamford Office—gather along canal closer to parking garage.
- IF FRONT EXIT IS BLOCKED AND YOU MUST EXIT FROM THE REAR OF THE BUILDING, TRAVEL AROUND THE BUILDING AND HEAD TO THAT AREA. PLEASE REMAIN IN A GROUP. FIRE MARSHALL NEEDS HEAD COUNT IMMEDIATELY.
- DEPARTMENT SUPERVISORS TAKE A HEAD COUNT WHEN ALL CLEAR SIGNAL RECEIVED FROM FIRE MARSHALL SUPERVISORS WILL GIVE INSTRUCTIONS TO REENTER BUILDING.

Note: When moving into exit areas in an emergency situation, before going through the door, put your hand against it to feel for heat—there could be a fire on the other side. If the door feels cool proceed with caution. If the door feels hot, use an alternate escape route.

Fire Procedures

If you should spot a fire, follow these suggested guidelines:

1. If the fire is minor (wastebasket, ashtray, etc.) extinguish if possible. However, do not take risks! Your personal safety comes first!
2. If the fire cannot be immediately brought under control without personal risk, isolate or contain if possible by closing the door to the fire area.
3. Call the Fire Department at **911**
   a. Give building name: Connecticut Green Bank at Atlantic Works, or 700 Canal Street, 5th Floor.
   b. Give building address and intersection: **75 Charter Oak Avenue, Suite 1-103, Hartford, or 700 Canal Street, 5th Floor, Stamford**
   c. Give the Green Bank's main telephone number **(860) 563-0015.**
   d. Give location and extent of fire.
4. Pull the fire alarm pull station so that evacuation can begin.
5. If trapped by flame or heat:
   a. If possible, telephone the Fire department and request immediate assistance.
   b. Close doors separating you from the source of heat or flame.
   c. Break glass window if necessary in order to escape.

d. Remember that both **heat and smoke rise**—air near the floor will be cleaner and cooler. Crouch down or crawl to exits.

Fire Drills
Fire drills are conducted once a year according to town codes. The Fire department and property owners will be directly involved so that they can test the fire alarm system and see if fire evacuation procedures are being followed.
Supervisors will be designated as the fire safety captains for their area.

Fire Safety Captains
There is a Fire Safety Captain and will help coordinate evacuation efforts. The captains' responsibilities include:

1. An awareness of employees in their area/office who are present that day so that all are accounted for after evacuating.
2. Knowledge of any employees with handicaps or disabilities which should be considered in an emergency.
3. Awareness of an up-to-date evacuation route from their area or office.
4. Checking of restrooms, conference rooms, smoking rooms or other areas which are not immediately visible to ensure that they are also evacuated.
5. Reporting any problems or special circumstances to Fire Warden.
6. Ensuring that people are exiting from the building in a calm and orderly fashion.

IN THE EVENT OF AN EMERGENCY, THE FIRE SAFETY CAPTAIN WILL IMMEDIATELY NOTIFY THE GREEN BANK'S PRESIDENT AND CEO, VICE PRESIDENT OF OPERATIONS, AND/OR SENIOR MANAGEMENT TEAM.

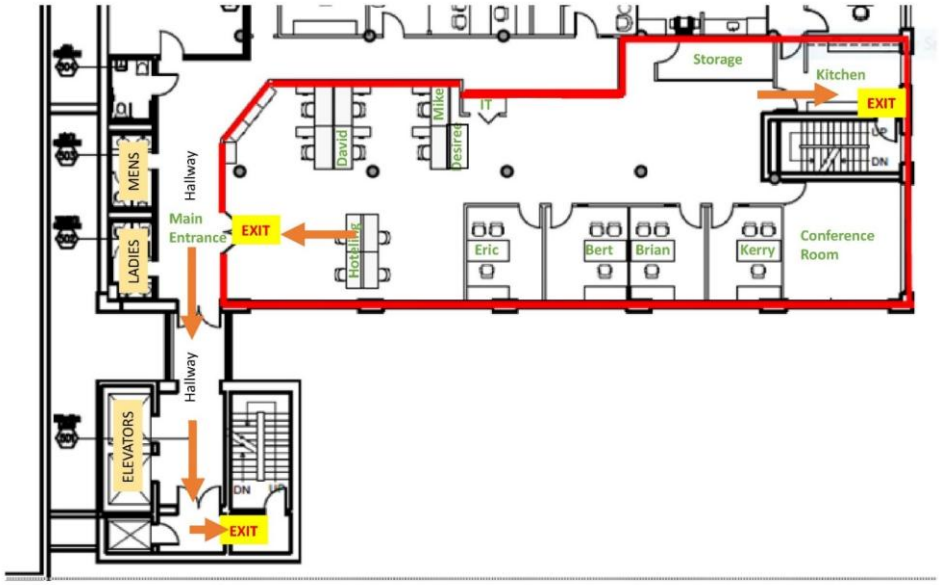
Housekeeping
Please inspect your space regularly and remove any items that could start or contribute to a fire or be a safety hazard. The following guidelines should be adhered to:

1. Do not allow accumulation of trash or waste material that is flammable.
2. Flammable materials or chemicals should not be stored within five feet of exit doors.
3. The wall and ceiling space around emergency and exit light fixtures should be kept clear.
4. The area surrounding electrical equipment should be free of clutter to provide for adequate air circulation.
5. Coffee makers and oven units are potential sources of fire. The last person leaving the building should check to be sure that they are turned off.

Connecticut Green Bank Fire Exits

700 Canal – 5th Floor
Stamford, CT 06902

FIRE EXITS



How To Handle Biological Agent Threats

At times facilities in communities around the country have received anthrax threat letters. Most were empty envelopes; some have contained powdery substances. The purpose of these guidelines is to recommend procedures for handling such incidents.

How to handle a suspicious letter or package marked with threatening message such as "anthrax":

1. Do not shake or empty the contents of any suspicious envelope or package.
2. **PLACE** the envelope or package in a plastic bag or some other type of container to prevent leakage of contents. Plastic bags and/or containers are available in the kitchen.
3. If you do not have a container, then **COVER** the envelope or package with anything (e.g., clothing, paper, trashcan, etc.) and do not remove this cover.
4. **LEAVE** the room and **CLOSE** the door, or section off the area to prevent others from entering. Keep others away.
5. **WASH** your hands with soap and water to prevent spreading any powder to your face.
6. If item has leaked: **DO NOT** try to **CLEAN Up** the powder. **REMOVE** contaminated clothing as soon as possible and place in a plastic bag, or some other container that can be sealed. This clothing bag should be given to the emergency responders for proper handling. Plastic bags and/or containers are available in the kitchen. SHOWER with soap and water as soon as possible. DO NOT USE BLEACH OR OTHER DISINFECTANT ON YOUR SKIN.
7. Contact **Human Resources.** They will take the necessary steps to report the incident to the proper authorities.
8. **LIST** all persons who were in the room or area when this suspicious letter or package was recognized. This list will be given to both the local public health authorities and law enforcement officials for follow-up investigations and advice.

Bomb Threats

In the event of a bomb threat, evacuating people from the potential danger area is the highest priority. In the event of the receipt of a bomb threat, try to remember as many of the following details as possible:

1. Time call received
2. Time call terminated
3. Exact words of caller
4. Time to explode
5. Location of bomb (if given)
6. Description/type of bomb (if given)
7. Why was it placed?
8. Description of voice (male, female, deep, high, accents, etc.)
9. Background sounds (traffic, machinery, music, voices, etc.)

Then immediately call: 911 for the Police and Fire Department.

Immediately call **Administrative Services ext. 391 IT ext. 365**. Explosives can be concealed in any type of container and in any location. Any suspicious item must not be touched and should be considered dangerous. Alert police of anything out of the ordinary, and do not turn on or adjust anything electrical in nature (i.e. - thermostats, light switches, radios, etc.)

It is policy that everyone evacuates the building immediately!

COVID-19 Response

The Green Bank recognizes its role in protecting its employees and in limiting the transmission of COVID 19. The organization has a taskforce that coordinates the organization's response. The Green Bank will adhere to appropriate regulations and orders and will work with employees to make sure that our work continues. The organization will implement the state's guidelines and reserves the right to limit the number of staff in the office at a particular time, require personal protective equipment be worn, require disclosure of exposure, require testing and/or vaccination, and other measures to be defined. Exceptions to policy must be approved by the Vice President of Operations and the President and CEO.

COVID-19 (and other pandemic) Guidelines

- Masking—dependent upon the prevalence of the coronavirus in our community as well as local and state mandates, we may recommend or require that employees mask while present in our offices. Employees are always welcome to mask while indoors as they feel comfortable.
- When possible, social distance and keep away from your colleagues if at all possible.
- Employees with offices do not have to mask while in their own space. However, we don't have enough information to determine if the walls of the cubes are effective partitions. Employee masking at workspaces is a personal decision, based on personal judgement and comfort level.
- Visitors may be banned from entering our premises unless their physical presence is required by business needs. Please be cautious about hosting visitors in our offices and note that all visitors must be masked while in our offices.

In Case of Emergency: Questions and Answers for Employees

What happens if I can't reenter the building?

The Emergency Operations Team, including the President when available, will assess the immediate damage and will inform the President or designee of what to expect. You may be asked to assemble at a nearby building for further instruction.

How will I know when and where to go back to work?

The Green Bank has designated a Team Leader for implementing its Business ~~Continuation~~ Continuity and Disaster Recovery Plan. This team leader will contact you at home and let you know when and where to return for work. If the business disruption is a serious one, it may take up to 30 days for all staff to return. A small number of employees who handle critical business functions may be asked to report to work immediately in a different office location.

What should I do if a reporter approaches me?

If a member of the press approaches you, please refrain from commenting about the incident or your personal reaction to what has occurred. It is natural that any business – disrupting incident may result in press coverage, and the Marketing Staff is the designated Green Bank representative to keep the news media informed and answer questions. Please refer any such inquiries to that designee.

75 Charter Oak Avenue, Suite 1 - 103, Hartford, CT 06106
T 860.563.0015
ctgreenbank.com

CONNECTICUT GREEN BANK

Memo

To: Audit, Compliance, & Governance Committee

From: Eric Shrago (Executive Vice President of Operations) & Joe Buonannata (Associate Director of Operations)

Date: January 6, 2026

Re: Proposed IT Policies and Employee Handbook Updates

As a result of recent audits, security assessments, and other benchmarking efforts, Green Bank Staff are looking to update and create new policies that are intended to safeguard our organization's technology infrastructure and data. Working with our outsourced information technology ("IT") firm and our IT risk consultant, we identified four areas where we need to update existing policies/plans or create new ones.

We are proposing the following, which are attached to this memorandum:

- **Information Security Policy** (new) - This policy defines how Connecticut Green Bank will protect information and assets through the implementation of security measures as aligned with the National Institute of Standards and Technology ("NIST") Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations[1]. The topics within this policy are developed to consistently implement standards and set expectations with the workforce to minimize risk and safeguard the confidentiality, integrity and availability of information.

- **Privacy Policy** (new) - This policy defines how Connecticut Green Bank will collect, use, disclose, retain and protect personal information. The topics within this policy are developed to consistently implement standards and set expectations with the workforce to minimize risk and safeguard the confidentiality of personal information.

- **Incident Response Plan** (new) - This plan provides a standardized response process for cybersecurity incidents and describes the process and completion through the incident response phases as defined in NIST Special Publication 800-61 including preparation, detection and analysis, containment, eradication and recovery, and post-incident activities. This plan outlines the people, processes and technologies needed to address incidents affecting Connecticut Green Bank's systems, data and networks to minimize harm, while supporting the restoration of business operations.

[1] https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

- **Business Continuity and Disaster Recovery Plan** (revised) - This plan prepares the Green Bank for unexpected disruptions and outages due to events beyond our control and to recover critical business systems and services as quickly as possible. This document is intended to guide our organization in effectively communicating, assigning responsibilities, activating recovery procedures and staying resilient if a disruption occurs.

In addition, we're proposing edits to the **Employee Handbook (see attached)** to reference these policies, enhance IT security, and update related text. The edits are in redline between pages 58-70 in the attached draft handbook and include:

- Requiring that any email messages sent with confidential or nonpublic information be encrypted (page 62)
- Stating that employees should not open emails or click on attachments from unknown sources (page 62)
- Referencing the creation of the newly created reportincident@ctgreenbank.com email address for employees to immediately report potential and actual suspicious activity, incidents and unauthorized disclosure of personal information to the internal Incident Response Team (page 68)
- Editing the "mobile application management policy," previously referred to as the "mobile device management policy," to clarify that IT cannot remotely eliminate data associated with pertinent apps (pages 69-70)

Pending recommendation of approval from the ACG Committee to the Board of Directors, and subsequent Board approval, Green Bank staff and our IT services and risk partners will conduct tests of these policies and training for staff. Should any adjustments be needed as identified from the tests or training, we will bring those edits back to the ACG Committee for the April 2026 meeting.

RESOLUTION:

WHEREAS, pursuant to Section 5.2.1 of the Connecticut Green Bank (Green Bank) Bylaws, the Audit, Compliance, and Governance (ACG) Committee is charged with the review and approval of, and in its discretion recommendations to the Board of Directors (Board) regarding, all governance and administrative matters affecting the Green Bank, including but not limited to organizational policies and the Green Bank Employee Handbook;

NOW, therefore be it:

RESOLVED, that the ACG Committee hereby recommends that the Board of the Green Bank approve of the implementation of new information technology policies and of the revisions to the Green Bank Employee Handbook presented on January 13, 2026 and as described in the memorandum to the ACG Committee dated January 6, 2025.

Incident Response Plan

Effective Date		**Review Frequency**	Annually or at a major change in business function or system
Approval Date		**Approved By**	
Reviewed Date	12/19/2025	**Reviewed By**	Head of Operations

Version History

Version	Date	Prepared By	Approved By	Summary of Modifications
1.0	12/19/2025	Operations Teram		First Draft

Table of Contents

Purpose

The purpose of this Incident Response Plan ("IRP") is to provide a standardized response process for cybersecurity incidents and describes the process and completion through the incident response phases as defined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61 including preparation, detection and analysis, containment, eradication and recovery, and post-incident activities. This plan outlines the people, processes and technologies needed to address incidents affecting Connecticut Green Bank's systems, data and networks to minimize harm, while supporting the restoration of business operations.

Scope

The scope includes all information systems, applications, cloud environments, networks and data owned or managed by the Green Bank. This policy applies to all employees and relevant external parties and vendors/consultants.

Objectives

- Prepare to protect against threats
- Reduce the impact of incidents
- Improve incident response

Definitions

The National Institute of Standards and Technology ("NIST") provides the following definitions.

Event: is any observable occurrence that involves computing assets, including physical and virtual platforms, networks, services, and cloud environments.

Adverse events: are any events associated with a negative consequence regardless of cause, including natural disasters, power failures, or cybersecurity attacks.

Cybersecurity incident: an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Breach: The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially

accesses personally identifiable information ("PII"); or an authorized user accesses personally identifiable information for another than authorized purpose.

Adversary: Person, group, organization, or government that conducts or has the intent to conduct detrimental activities. An entity that is not authorized to access or modify information, or who works to defeat any protections afforded the information.

Incident Response Team Roles and Responsibilities

The following table describes Connecticut Green Bank's assigned roles and responsibilities as they relate to incident response. The goal is to eliminate confusion, speed up recovery efforts and maintain accountability.

The Green Bank has routine meetings with its third-party IT vendor and will use those opportunities to discuss all incidents that occur. Incidents with greater severity will be discussed with the IT vendor outside of that regular meeting cadence.

Role	Responsibilities
Incident Response Lead	This is assigned to the Head of Operations. They are responsible for: • Overseeing the development and maintenance of the Incident Response Plan • Leading Incident Response Plan tests and training efforts • Performing the initial assessment of a potential or actual incident • Authorizing the actions needed to minimize harm to the Green Bank during an incident including confiscating, disconnecting or shutting down technology assets and systems • Communicating to appropriate departments • Mobilizing the Crisis Management Team • Overseeing plan activation of Incident Response and Business Continuity and Disaster Recovery ("BCDR") efforts • Directing business operations and approving priority of mission critical applications during an incident • Updating Senior Staff, the Board of Directors and the Crisis Management Team as necessary • Creating customer communications • Transitioning to normal business operations after recovery
Incident Handlers	This team is comprised of the Associate Director of Operations and the Office Manager. They report to the Incident Response Lead. They are responsible for: • Developing and maintaining the Incident Response Plan • Engaging vendors to verify an incident has occurred, collect and analyze data and evidence • Prioritizing incident response activities • Working with vendors to limit damage, find root causes, and restore operations

	• Working with technology vendors to develop recovery and contingency plans for specific scenarios • Under the Incident Response Lead's direction, performing the initial assessment of the disruption or incident and mobilizing appropriate vendors • Maintaining documentation and performing status updates during an active incident • Participating in Incident Response Plan testing and training activities
Crisis Management Team	This team is comprised of Green Bank Officers, Head of Operations, Director of Accounting & Reporting, Director of Marketing & Communications, Associate Director of Operations. They are responsible for: • Approving and delivering media and public communications • Handling regulators and stakeholders • Contacting the insurance company • Addressing immediate financial needs of the incident, including recovery efforts and related procurement • Assessing financial implications of the incident including lost documents, assets, revenue, etc. • Identifying and addressing legal implications as a result of the incident • Participating in Incident Response Plan testing and training activities
Green Bank Senior Staff	Provide feedback on Incident Response Plan development and updates prior to the Board of Directors approval, support Incident Response Plan efforts and provide approval on related procurement. Stay informed on status updates and incident related communication. Provide direction on mission critical business operations during a disruption or disaster.
Board of Directors	Approve this Incident Response Plan and related policies and procedures, oversee and support the Incident Response program, document agendas, minutes and signatures showing oversight.
Managers	Ensure compliance with security and privacy policies and procedures, BCDR and Incident Response Plans in their teams, identify and report risks, potential or actual incidents, disruptions or disasters promptly to the Incident Response Lead, and perform approved notifications and communications to their teams and customers as required.
Human Resources	Stay informed on status updates and incident related communication. Contact employee emergency contacts as necessary. Oversee and provide guidance on progressive discipline measures in the case an incident or disruption was caused by employee error, negligence or ill intent. Ensure risk reducing practices such as pre-employment screening and standard onboarding, transfer and offboarding changes are performed.
All Staff and Contractors	Follow security and privacy policies and procedures, BCDR and Incident Response Plans, report risks, potential or actual incidents, disruptions or disasters promptly to the Incident Response Lead and their manager, complete required security, privacy and related training.
System Owners/ Administrators	Ensure access is authorized, documented and granted based on the principle of least privilege, required security controls are configured, and system is periodically monitored. Stay up-to-date and address system upgrades, new features and updates that may increase risk. Participate in line of business

	application recovery and testing in the case of a disruption, disaster or incident, validate business data and emergency mode operation procedures.
Third-Party Vendors	Meet contractual security obligations and undergo due diligence audits as applicable. Report malicious activity, potential or actual incidents promptly to the relevant Green Bank program lead (employee), who will then notify the Incident Response Lead. Provide support and recovery activities as needed.

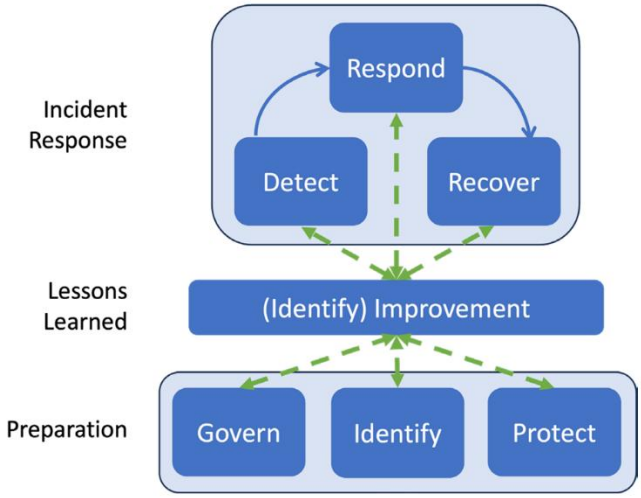
Incident Classification

The following guidelines are used to classify incidents by severity level to support the prioritization of recovery efforts and maintenance or restoration of operations.

Severity Level	Description	Examples	Response Strategy
Low	Little to no impact, localized and quickly contained	Blocked phishing attempts, isolated malware	Implemented technology and security controls detect, block, isolate and address incidents. If needed, related vendors perform incident response procedures. The Incident Response Form and formal or coordinated response activities outlined in this plan will NOT be performed.
Medium	Limited impact, requires coordinated response	Single account compromise	Related vendors perform incident response procedures. The Incident Response Form and formal, coordinated response activities outlined in this plan will NOT be performed. Any identified security controls or procedural updates will be made to reduce the likelihood of recurrence.
High	Significant system or data impact	Ransomware, PII exposure, breach of critical system	Formal and coordinated response activities will be performed as outlined in this plan.
Critical	Major outage, breach or incident with regulatory impact	Data exfiltration, widespread compromise	Formal and coordinated response activities will be performed as outlined in this plan. The Crisis Management Team will be engaged.

Incident Response Lifecycle

The following diagram shows a high-level incident response lifecycle aligned with the six NIST Cybersecurity Framework functions.



Preparation

Govern: The organization's information security policy, including risk management strategy, business continuity and disaster recovery plan and this incident response plan are established and communicated.

Identify: The organization's current cybersecurity risks are identified and understood. During post-incident activities lessons learned are assessed and incorporated into improving preparation and incident response procedures.

Protect: Safeguards are in place to manage the organization's cybersecurity risks.

Incident Response

Detect (and Analyze): Possible cybersecurity attacks and compromises are found and analyzed.

Respond (and Contain): Actions regarding detected cybersecurity incidents are taken.

Recover (and Eradicate): Assets and operations affected by cybersecurity incidents are restored.

Incident Response Phases

Each phase of incident response is essential in preventing incidents, minimizing impact and successful recovery. The phases outlined in this section align with the Cybersecurity and Infrastructure Security Agency's ("CISA") Cybersecurity Incident Response Playbook.

Prepare

The Green Bank will effectively prepare for incidents before they occur to mitigate any impact on the organization. The goal is to ensure resilient systems are in place to maintain critical operations in a compromised state. The following activities are performed to prepare for potential incidents:

Policies and Procedures

- This Incident Response Plan will be maintained to escalate incidents based on severity and minimize harm to the organization.
- A Business Continuity and Disaster Recovery Plan ("BCDR Plan") will be maintained to define recovery strategies for critical business functions and define contingency plans for top threats including potential cybersecurity incidents.
- An Information Security Policy will be maintained to outline the safeguards needed to protect the organization's systems, assets and data.
- A Privacy Policy will be maintained to maintain the confidentiality of nonpublic information.

Instrumentation

The organization has implemented the following tools to monitor and detect incidents:

- Antivirus software on all endpoints
- Endpoint detection and response (EDR) solution
- Intrusion detection and prevention systems (IDPS)
- Authorization, host, application and cloud logs
- Security information and event management (SIEM) systems
- Systems for logging, log retention, and log management

Trained Response Personnel

In order to prepare personnel to respond appropriately to cybersecurity incidents, the following training and exercises are implemented on a periodic basis:

- Annual training for the Incident Response Lead and Incident Handlers so they are equipped with the knowledge needed to respond quickly and effectively to incidents.

- Annual Incident Response Plan and Business Continuity plan testing and exercises where the Incident Response Lead, Incident Handlers and other critical personnel and vendors will participate.

Technical Vendor Planning

The organization will meet with the third-party vendor who oversees the network and Microsoft 365 to plan for incident response, business continuity and disaster recovery. Points of contact will be updated to coordinate related activities.

Testing Procedures

Incident Response Plan testing will be performed annually to ensure communication and preparation are effective and incident response phases are successfully completed. Updates will be made to the Incident Response Plan based on the results of these tests.

Cyber Threat Intelligence

The organization will monitor intelligence feeds and notifications for threat advisories from trusted sources like technology partners and government agencies.

Communications and Logistics

Communication and escalation methods are outlined in the organization's Business Continuity and Disaster Recovery Plan and will be implemented if a major outage or disruption occurs as a result of a cybersecurity incident.

Operational Security

The organization will implement the following processes to decrease the likelihood of incident response activity detection by attackers:

- Segmenting and managing SOC systems separately from the broader enterprise IT systems
- Managing sensors and security devices via out-of-band means
- Notifying users of compromised systems via phone rather than email
- Using hardened workstations to conduct monitoring and response activities

Technical Infrastructure

The following infrastructure is implemented to protect incident response data and reporting:

- Secure storage for incident data and reporting only accessible by the Incident Response Lead, Handlers and authorized personnel and vendors,
- Provide a means for collecting forensic evidence and safely handling malware

- Implement an Incident Response Form and document storage system for high and critical systems to track and capture pertinent details of suspicious activity and adversary information like tactics, techniques and procedures

Detect Activity

The organization will partner with their technology vendor to configure tools to analyze logs and receive alerts for suspicious activity.

Detect and Analyze

Incident response procedures will be implemented to detect and analyze potential and actual incidents. Efforts will be made to preserve evidence. The following activities will be performed during this phase:

Incident Response Team Notification

When an incident is detected the Incident Response Lead and Team must be immediately notified to allow them to begin incident response procedures. Green Bank personnel will be asked to report incidents by emailing reportincident@ctgreenbank.com so they can effectively communicate incidents to the Incident Response Lead and Team in a timely manner. In the case of incidents in Microsoft 365 or the network, the Incident Response Lead and Team will be promptly notified by the IT vendor.

Declare Incident

The Incident Response Lead or Green Bank Senior Staff are authorized to declare an incident. Upon declaring an incident, appropriate vendors, the Incident Response Team and applicable Green Bank personnel or subject matter experts will be contacted to begin investigation. During high and/or critical level incidents the Crisis Management Team may be mobilized, and the cybersecurity insurance company may be contacted depending on the scenario. The Business Continuity and Disaster Recovery Plan will also be activated for high and/or critical level incidents.

Determine Investigation Scope

The Incident Response Team and engaged vendors will conduct an investigation to determine the scope of the incident. They will use available data to identify the type of access, the extent to which assets have been affected, the level of privilege attained by the adversary, and the operational or informational impact. The team will analyze any automated detection or sensors, available system reports, audit trails and speak to related users, contractors and third parties to determine an accurate scope of the incident. They will update the Incident Response Form with this information.

Collect and Preserve Data

In coordination with the engaged vendors, the Incident Response Team will collect and preserve data for incident verification, classification, prioritization, mitigation and reporting. This information will be stored on the organization's SharePoint site, if it is determined to be safe from the scope of the incident. If it is not safe, the Incident Response Team will identify an alternate method of storing this information to safeguard evidence for use in any potential law enforcement investigation.

Perform Technical Analysis

The Incident Response Team will work with engaged vendors to develop a technical and contextual understanding of the incident. They will determine the root cause and document adversary activities to discover the attack chain and enable prioritization of response activities.

Correlate Events and Document Timeline

The Incident Response Team will work with engaged vendors to acquire, store, and analyze logs to correlate adversarial activity. They will create a timeline of all relevant findings to allow the team to account for all adversarial activity. They will update the Incident Response Form with this information.

Identify Anomalous Activity

The Incident Response Team will work with engaged vendors to assess affected systems, networks, assets, cloud environments and data for any activity that might be adversary behavior. This will enable the team to identify deviations form normal business behavior. They will update the Incident Response Form with this information.

Identify Root Cause and Enabling Conditions

The Incident Response Team will work with engaged vendors to identify the root cause of the incident and collect threat information. They will analyze the anomalous activity to continue investigating and to inform response efforts. They will identify the conditions that enabled the adversary to access and operate within the environment, which will be assessed during post-incident activities. They will update the Incident Response Form with this information.

Respond and Contain

To prevent further damage and reduce the impact of the incident, the Incident Response Team will work with engaged vendors to contain the incident. The containment strategy used will depend on the type of scenario and incident taking place. The Incident Response Lead or designee is authorized to approve actions including confiscating, disconnecting or shutting down technology assets and systems as part of the containment and response procedures.

Considerations

The following will be considered when evaluating containment courses of action:

- Any additional adverse impacts to mission operations, availability of services
- The duration of the containment process, resources needed, and effectiveness
- Any impact on the collection, preservation, securing and documentation of evidence

Containment Activities

The Incident Response Team will work with engaged vendors to implement authorized containment activities and short-term mitigations to isolate threat actor activity and prevent additional damage from the activity or them pivoting into other systems. Containment activities may include:

- Isolating impacted systems and network segments from each other and/or from non-impacted systems and networks. The continuation of critical business functions will be assessed and modified during this phase to the best extent possible.
- Capturing forensic images to preserve evidence for legal use (if applicable) and further investigation of the incident.
- Updating firewall filtering.
- Blocking (and logging) of unauthorized accesses; blocking malware sources.
- Closing specific ports and mail services or other relevant services.
- Changing system admin passwords, rotating private keys, and service/application account secrets where compromise is suspected and revocation of privileged access.

The Incident Response Team will update the Incident Response Form with containment activities performed.

Eradicate and Recover

Before moving to the eradication and recover phase, the organization will ensure all means of unauthorized access have been accounted for (including back doors), that adversary activity is sufficiently contained, and all evidence is collected. The objective of this phase is to return to normal business operations by eliminating artifacts of the incident.

Execute Eradication Plan

The Incident Response Team will work with engaged vendors to develop an Eradication Plan before execution. This plan may include the following eradication activities:

- Remediating all infected IT environments (cloud, network, host, hybrid, OT, etc.)
- Reimaging affected systems or rebuilding systems from scratch

- Rebuilding hardware
- Replacing compromised files with clean versions
- Installing patches
- Resetting passwords on compromised accounts
- Monitoring and responding to any signs of adversary response to containment activities
- Allowing adequate time to ensure all systems are clear of all possible threat actor mechanisms

The Incident Response Team will update the Incident Response Form with eradication activities performed. After executing the plan, the organization will continue to detect and analyze activities and monitor for signs of reentry or new access methods.

Recover Systems and Services

The goal of this phase is to recover systems and services to normal business operations. Depending on the scenario, the recovery plan may include:

- Reconnecting rebuilt/new systems to networks
- Tightening perimeter security and access rules
- Testing systems thoroughly
- Monitoring operations for abnormal behaviors

The Incident Response Team will work with engaged vendors and subject matter experts to confirm systems and services are functioning correctly and validate data integrity. The Incident Response Team will update the Incident Response Form with recovery activities performed.

Post-Incident Activities

Breach Notification and Reporting Requirements

The Incident Response Team will assess the incident and determine if any breach notification or incident reporting actions are needed to meet regulatory requirements. If it is determined that unauthorized disclosure of personal information took place, a record will be retained and reported to affected individuals. The Green Bank's Senior Staff will be engaged for direction on conducting and documenting notifications and reports as needed.

Adjust Sensors, Alerts and Log Collection

The Incident Response Team will work with engaged vendors to identify and address any sensors, alerts and log collection activities needed to ensure adequate coverage moving forward. The affected environment will continue to be closely monitored.

Identify Lessons Learned

The Incident Response Team will work with engaged vendors to conduct a lessons learned analysis which includes:

- Ensuring root cause has been eliminated or mitigated
- Identifying infrastructure problems to address or security controls to harden in cloud systems
- Identifying issues related to policies and procedures that need to be addressed
- Reviewing and updating roles, responsibilities and authority to ensure clarity
- Identifying technical or operational training needs
- Improving tools to perform protection, detection, analysis or response actions
- Determining areas of improvement to this Incident Response Plan

Finalize Reports

The Incident Response Team will complete the Incident Response Form and include all updates from this section. The Incident Response Form will be saved in the organization's central SharePoint site with other incident related documentation and will be provided to the Incident Response Lead.

Conduct Post Incident Review Meeting

A Post Incident Review Meeting will be conducted with the Incident Response Lead, Incident Response Team, Crisis Management Team and Green Bank Senior Staff as needed. The Incident Response Form will serve as a guide for this meeting. Lessons learned will be discussed and any follow up actions determined. The incident will be closed when all malicious activity is eradicated, systems are restored and validated, and the Post Incident Review Meeting is conducted. Additional communication to Green Bank personnel, vendors, customers will be determined and performed.

Plan Management

The Connecticut Green Bank will maintain this plan in accordance with other security polices to comply with required frameworks, regulations and company standards. If modifications are made to this plan, they will be documented and approved prior to implementation and communication across the workforce. This plan will be reviewed annually internally at the staff level or as business needs and regulatory requirements evolve and approved by the Head of Operations. Any substantive changes will be presented for Board of Directors' review and approval prior to implementation. This plan will be made available to employees via the standard SharePoint site used to centrally store other company policies and procedures.

Compliance & Monitoring

The Connecticut Green Bank takes violations of security policies and procedures very seriously. Suspected or actual violations will be documented, investigated and tracked per the Progressive Discipline Policy in the Employee Handbook. Non-compliance with this plan may result in disciplinary action, up to and including termination of employment.

Vendors found in violation of contractual obligations or security requirements may be subject to remediation requirements, penalties, or termination of services.

Related Documentation

- Business Continuity and Disaster Recovery Plan
- Information Security Policy
- Critical Systems Inventory
- Critical Assets Inventory
- Security Risk Assessments
- Privacy Policy
- Employee Handbook

References:

National Institute of Standards and Technology ("NIST") Cybersecurity Framework (CSF) 2.0

National Institute of Standards and Technology ("NIST") Special Publication 800 NIST SP 800-61r3: Incident Response Recommendations and Considerations for Cybersecurity Risk Management

Cybersecurity and Infrastructure Security Agency's ("CISA") Cybersecurity Incident Response Playbook

Appendix: Incident Response Form

Reporting Individual	
Name:	**Job Title**:
Email:	**Phone**:
Incident Information	
Date Incident was Detected:	**Time Incident was Detected**:
Location of Incident:	**Type of Incident:**
How was the incident detected?	**Help Desk Ticket Number:**
Incident Description:	
When was it reported?	**How was it reported?**
Describe Initial Notifications: (BCDR/Incident Response Lead, BCDR/Incident Response Team, Crisis Management Team, Green Bank Senior Staff, HR, vendors, law enforcement, etc.)	
Initial Impact Assessment	
Describe Impact on Business:	
Severity: Low / Medium / High / Critical	**Actual Incident declared?** Yes / No
Describe Initial Actions Taken and Initial Communication (If an actual incident was NOT declared include reason and actions to resolve incident):	

Describe Declared Disaster Notifications		
Internal:	**Method:**	**Completed By:**
Vendors:	**Method:**	**Completed By:**
Customers:	**Method:**	**Completed By:**
Law Enforcement:	**Method:**	**Completed By:**
Property Management:	**Method:**	**Completed By:**
Insurance:	**Method:**	**Completed By:**
Other:	**Method:**	**Completed By:**

Damage Assessment
Scope of the incident:
Symptoms of the incident:
Root cause of the incident:
Affected systems:
Affected assets:
Affected accounts:
Affected property:
Affected documents:
Describe digital data compromised:
What regulations apply to the data breached?
Was evidence gathered to support incident findings and mitigation activities?
Financial Considerations:
Legal Considerations:

Actions Taken			
Was a top threat contingency plan activated? Yes / No			
Document the containment, response, eradication, and recovery actions taken below to address prioritized critical business functions.			
Action	**Date & Time**	**Performed By**	**Details**

Action	Date & Time	Performed By	Details
Date and Time Incident Mitigated:		**Date and Time Normal Business Operations Resumed:**	
Was the Recovery Time Objective (RTO) met?		**Was the Recovery Point Objective (RPO) met?**	
Were systems and business functions tested to confirm recovery?		**Was data integrity validated?**	
Describe activities to resume normal business operations and confirm all information collected while working in recovery mode was securely updated in required systems:			

Incident Review
Describe corrective actions needed to prevent similar incidents in the future:
What precursors or indicators should be watched for in the future to detect similar incidents?
What additional tools or resources are needed to detect, analyze, and mitigate future incidents?
Was communication effective throughout the incident?
What changes would you make to the recovery process to minimize risk and harm to the organization?
What changes would you recommend improving the Business Continuity and Disaster Recovery Plan?
What changes would you recommend improving the Incident Response Plan?
Comments
Incident Status: Active / Closed

Information Security Policy

Effective Date		**Review Frequency**	Annually or at a major change in business function or system
Approval Date		**Approved By**	
Reviewed Date	12/19/2025	**Reviewed By**	Head of Operations

Version History

Version	Date	Prepared By	Approved By	Summary of Modifications
1.0	12/19/2025	Operations Team		First Draft

Table of Contents

Purpose

This Information Security Policy defines how Connecticut Green Bank will protect information and assets through the implementation of security measures as aligned with NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations. The topics within this policy are developed to consistently implement standards and set expectations with the workforce to minimize risk and safeguard the confidentiality, integrity and availability of information.

Scope

This policy applies to:

- All employees, contractors, interns and third-party vendors with access to the Green Bank's systems.
- All information systems, applications, cloud environments, networks and data owned or managed by the Green Bank.
- Both digital and physical forms of data.

Objectives

Develop and disseminate an organization-wide Information Security Policy that:

- Protects the Green Bank's information from unauthorized access or disclosure;
- Defines roles and responsibilities;
- Complies with applicable legal, regulatory and contractual requirements;
- Defines standards for the security controls implemented in Green Bank's Systems.

Roles and Responsibilities

Role	Responsibilities
Board of Directors	Approve this policy and related policies and procedures, oversee and support the Information Security program, document agendas, minutes and signatures showing oversight of the development and performance of internal controls.
Head of Operations	Review and provide feedback on this policy, approve risk management strategy, allocate resources, approve vendor onboarding, provide direction and support the Information Security program.
Operations Team	Develop policies, coordinate risk assessments and audits, maintain risk register, perform security, privacy and compliance related

	activities as delegated by the Head of Operations, implement and maintain security and privacy controls and perform vendor risk management activities.
Department Heads	Ensure compliance with security requirements in their teams, identify and report risks in their area, ensure controls are followed. Define service requirements and monitor vendor deliverables. Communicate vendor performance, security or privacy concerns immediately to the Head of Operations.
Legal	Review and provide guidance on all contracts and regulatory obligations. Provide feedback on policies as needed.
All Staff and Contractors	Follow policies and procedures, report incidents and potential risks in a timely manner, complete required training.
System Owners/ Administrators	Ensure access is authorized, documented and granted based on the principle of least privilege, required security controls are configured, and system is periodically monitored. Stay up-to-date and address system upgrades, new features and updates that may increase risk.
Third-Party Vendors	Meet contractual security obligations and undergo due diligence audits as applicable.

Risk Management

The Risk Management strategy defines how the organization will implement sufficient measures to identify, manage and reduce risks and vulnerabilities that may impact the organization's ability to achieve its objectives to a reasonable and appropriate level. The organization will conduct ongoing activities to minimize risk and safeguard the confidentiality, integrity and availability of company information.

Risk management involves identifying, assessing, mitigating, reporting and monitoring risks to the organization's critical data and assets. Once risks are discovered in this manner the process of selecting and implementing the most appropriate methods to avoid, mitigate, transfer or accept the risks will be completed.

Definitions

- **Risk**: The possibility of an event occurring accidently or intentionally that will have an impact on business objectives.
- **Likelihood/Probability**: The probability that a risk will occur and of a given threat triggering or exploiting a particular vulnerability.
- **Impact/Severity**: The consequence or adverse effect if a risk occurs.
- **Risk Appetite**: The level of risk the organization is willing to accept.
- **Mitigation**: Actions to reduce risk likelihood or impact.
- **Residual Risk**: Remaining risk after mitigation.

- **Vulnerability**: A flow or weakness in system security procedures, design, implementation or internal controls that could be exploited (accidently or intentionally) and result in a security breach or a violation of the security policy.
- **Threat**: The potential for a person or thing to exercise (accidently or intentionally) a specific vulnerability.

Risk Management Process

The organization's objective is to identify the risks to its systems, data and assets and remedy these risks in a prioritized manner to minimize harm. This process will also provide the information required and expected to support the internal control and achievement of the Green Bank's service commitments and system requirements. The following procedures will be conducted to manage risk. The organization's Head of Operations is responsible for the overall completion of risk management activities and may delegate tasks as needed to other internal or external resources including third party vendors.

1. **Risk Assessment:**
   A risk assessment will be completed and documented at least annually or at any significant change in technical environment, operations, business system or function that could significantly impact the system of internal control. The following phases are performed during risk assessments:
   a. **Identify:** The identification phase includes listing out risks that exist in the environment. This phase provides a basis for all other risk management activities.
   b. **Assess:** The assessment phase considers the level of risk to the business.
2. **Risk Mitigation:**
   The **mitigation** phase includes putting controls, processes, and other physical and virtual safeguards in place to prevent and detect identified and assessed risks to an acceptable level.
   a. A Remediation Plan will be developed to mitigate risks and implement technical and nontechnical measures.
   b. This Remediation Plan will be presented to Head of Operations for approval.
   c. The Head of Operations will complete activities in the Remediation Plan or delegate to internal resources or third-party vendors as appropriate.
3. **Reporting:**
   The **reporting** phase includes providing risk reports to applicable third party vendors and managers of other stakeholder teams to support them in making effective business decisions and complying with internal policies and relevant regulations.
   a. Progress to the Remediation Plan will be tracked, monitored, controlled and reported to the Head of Operations as needed.

4. **Monitoring**:
   The **monitoring** phase includes the Green Bank's management monitoring activities to evaluate whether controls, processes, initiatives, functions, and/or activities mitigate the risk as designed.
   a. Risks will be maintained in a central tracking mechanism.
   b. Risks will be reviewed quarterly and after major incidents.
   c. If new risks arise or the business climate changes, the Remediation Plan may be re-prioritized.

Communication & Training

Workforce members will be trained on security best practices annually, provided information on common and relevant security threats to the organization as well as any relevant items identified in the Remediation Plan. Updates will be shared with stakeholder teams as necessary.

Document Control

All completed risk management and related documentation will be stored in a central location and maintained in accordance with other security documentation, policies and procedures.

Control Assessments

Control assessments will be performed by means of a SOC 2 Type 2 annual audit to ensure that the Green Bank meets information security requirements, to identify weaknesses and deficiencies in the system design and development process, and provide essential information needed to make risk-based decisions. The Green Bank will engage assessors with qualified skills and technical expertise to conduct effective assessments. Information reported from these assessments will be reviewed by the Green Bank's CEO and Head of Operations to plan and provide direction on any response or mitigation needed.

Personnel Security

To ensure all members of the workforce have the appropriate access to company information, and those who should not have access are prevented from doing so, specific controls will be in place to standardize personnel security practices. The goal is to grant access to workforce members with the required clearances, approvals, and authorization as well as terminate access in a timely manner.

Personnel Screening

Management will verify the required experience and qualifications of workforce members during the selection process. Background and reference checks will be conducted and assessed prior to hire.

Job Descriptions and Responsibilities

Job descriptions will be documented and provided to employees upon hire to define the clear responsibilities of their roles.

Supervision and Authorization

An organization chart will be maintained to depict the chains of command and lines of authority where authorization and supervision will occur.

Onboarding, Offboarding and Transfers

The Green Bank will use standard processes to facilitate consistent onboarding, offboarding and transfer practices to minimize risk and prevent unauthorized access to information.

Acceptable Use

The Employee Handbook is the central source of acceptable use information for employees. This document contains the following sections as they relate to Acceptable Use of company assets:

- Computer Use Policy, which provides guidelines governing the use of computers, company issued assets and other electronic communications.
- Hardware section, which defines how employees must handle hardware available to them.
- Personal Use, which outlines the restrictions of using company-owned equipment for personal use and for using personal devices.
- Contract and Freelance staff, which restricts the use of company-owned assets for business purposes only.
- Company Data section, which provides information on permitted and restricted use of company information.

Security Awareness Training

The purpose of providing security awareness training is to minimize risk to confidential and nonpublic information by providing knowledge of security best practices to the workforce. The goal is to give the workforce the information they need to make secure choices and implement the organization's security procedures in a consistent manner.

Training will be scheduled and tracked by the Operations Team and the organization's third-party vendor. The security awareness and training program will be monitored and evaluated annually to ensure updated, accurate and relevant information is provided to the workforce.

Security Incident Procedures

To minimize risk to confidential and nonpublic information the Green Bank will develop, implement and maintain an Incident Response Plan to document policies and procedures for preparing for, responding to and learning from potential and actual security incidents. This plan outlines the detailed phases of incident response including procedures for preparing for, detecting, responding to, recovering, and reporting security incidents.

Contingency Planning

The Green Bank will create and maintain contingency plans to safeguard the confidentiality, integrity and availability of company information during an incident, emergency or significant event. Plans will be implemented to minimize downtime and recover data in a timely manner.

Business Continuity and Disaster Recovery Plan

The Green Bank has created a Business Continuity and Disaster Recovery Plan to minimize interruptions to critical business processes from the effects of major failures or incidents. This plan also provides important information pertaining to communication and recovery phases to facilitate a smooth and rapid restoration of service and business functions.

Data Backup and Retention

The Green Bank creates backups and has implemented systems to retain required information. These are stored in a secure location and can be used in the event of:

- Accidental deletion of important material

- A disaster or incident necessitating complete recovery of one or more of the company's systems.

The organization currently uses a third-party vendor to backup relevant content including email, SharePoint, OneDrive and Teams data in Microsoft 365. Software as a Service applications are backed up by the vendor based on their parameters.

System Availability and Performance

System availability and performance are monitored by the assigned system owners where possible. System owners will identify and report issues to the Head of Operations when necessary. The organization's third-party vendor implements monitoring tools to track availability and performance of the Green Bank's network and Microsoft 365 environments.

Physical Security

The Green Bank will reduce the risk to critical assets by implementing physical security standards for all facilities.

Authorization

Physical access authorization will be granted based on role and assigned location. Individuals with permanent physical access authorization code/fobs are not considered visitors in assigned locations. The organization's fob system will be the central source to manage and assign authorized access.

Minimum Security for Facilities

The following includes all countermeasures (both physical and procedural) to address identified threats and minimize risk.

- Green Bank office suite doors will be locked at all times.
- All authorized employees will be provided with a code/fob to access their assigned work location based on their role.
- Authorized employees will use fobs/codes provided to unlock doors and gain access.
- The Operations Team will monitor access to main entrances.
- Surveillance monitoring and security systems will be implemented to detect and respond to physical security incidents where applicable.
- Authorized personnel will be provided access to the surveillance system for their assigned location.
- Visitor Access Procedures will be implemented in all facilities where possible.

- Emergency exits and reentry procedures allow only authorized personnel to reenter restricted areas after emergency or drill.
- Deliveries should use the visitor's procedures.
- Employees are not to share their assigned codes/fobs or keys with others.
- Employees must report lost or stolen fobs or keys to their supervisor immediately, who should then inform the Operations Team.
- Fobs, keys and other facility access items will be collected from employees upon termination.
- Unassigned fobs, keys and other access items will be stored in secure locations.

Visitor Access Procedure

The following procedure will be followed in all Green Bank locations:

- Facilities have a visitor logging process, where visitors are required to sign in and enter their information before gaining access to other areas of the building.
- The visitor's desired location will be contacted for authorization. A member of that area will meet the visitor at the front office and escort them to the desired location.
- Visitors are escorted if they need to move to different areas of the building.

Alternate Work Sites

As outlined in the Telecommuting section of the Employee Handbook, the Green Bank provides a flexible and customized telecommuting option for employees based on four categories that define the requirements for a hybrid work environment.

Maintenance Work and Records

The Green Bank understands that maintenance work will occur as needed and will implement the following security controls:

- Vendors who are performing maintenance must follow the Visitor Access Procedure.
- Maintenance records will be collected and centrally stored for reference as needed.

Media Protection

The purpose of media protection is to govern the receipt, tracking and removal of hardware and electronic media that contain company information into and out of the facility, and the movement of these items within the facility. The goal is to track, wipe and dispose of media and devices to prevent unauthorized disclosure of company information.

Media Use

The Green Bank has identified a list of approved external devices. Employees request a device from the Office Manager who approves and tracks these in her asset management system. Employees are only allowed to use these company approved external devices.

Encryption

All company-owned endpoints that store confidential or nonpublic information must be encrypted.

Media Transport

In the case that media must be transported, devices with confidential or nonpublic information will be backed up prior to transport, maintaining the security of devices during transport and promptly reporting the damage or loss of devices.

Disposal

The organization will implement the following procedures to address the final disposition of the hardware or electronic media on which company information is stored.

- All company information will be backed up/copied prior to device disposal.
- The method of sanitization will depend upon the type of equipment.
- An attempt must be made to sanitize any hardware, devices or electronic media. In the event it is impossible to sanitize the hardware, device or electronic media, it must be physically dismantled and rendered useless.
- In the case where a disposal service or outside vendor is used to sanitize and dispose of equipment, documentation must be received from the vendor performing the service certifying that the equipment was sanitized and disposed of with the date and method of sanitization.

Device or Media Reuse

The following procedures outline the process to remove company information from electronic media before the device or media are made available for reuse. The organization will ensure that company information previously stored is backed up or copied and cannot be accessed and reused by unauthorized individuals.

- All company information will be backed up/copied prior to assignment for reuse.
- The method of sanitization will depend upon the type of equipment.
- In the case where a disposal service or outside vendor is used to sanitize equipment, documentation must be received from the vendor performing the

service certifying that the equipment was sanitized of with the date and method of sanitization.
- Once equipment has been properly sanitized and all previously stored company information cannot be accessed, the equipment may be reassigned to a workforce member for use. A record of the reassigned hardware and/or electronic media will be made in the formal inventory system.

Device Inventory

To maintain a record of the movements of company equipment, the following will be implemented.

- All equipment, devices and electronic media will be formally inventoried and tracked including the documentation of the assigned workforce member.
- Any unassigned equipment, device or electronic media must be kept physically secure and inventoried.
- All devices and electronic media will be collected from the assigned workforce member at the time of termination. The equipment will be assessed for reuse. A record of the collected equipment, device and/or electronic media will be made in the formal inventory system.
- All new equipment, devices and electronic media will be added to the formal inventory system before they are provided to the assigned workforce member.

Access Control

The Green Bank will implement the following access control process standards to prevent the likelihood of unauthorized access.

Principle of Least Privilege

To minimize risk to the Green Bank's systems and data, users will be granted the least privileged access to perform their job functions. Administrators to systems will be limited to only those required to perform elevated functions.

Account Management

Unique user accounts are in place to access business information, email and Microsoft 365 applications as a standard. System owners manage accounts in assigned systems.

The following types of accounts are present in Green Bank systems:

- Privileged accounts
- Standard user accounts

- Shared or group accounts
- Guest/external accounts
- Vendor accounts
- System accounts
- Service accounts
- Developer accounts
- Emergency accounts

Access Authorization

System owners will obtain and document access authorization prior to granting access to confirm role, job functions and permission level to data required based on the least privileged access needed. All exceptions or elevated access requests will also be authorized and documented prior to access being granted.

Role Based Group Access

Where possible, system owners/administrators will implement role-based access groups instead of individual access to minimize error and risk, as well as, to simplify the onboarding, offboarding and transfer processes.

Disable/Terminate Accounts

Upon termination of employment or contract, user accounts will be terminated. System owners will disable/remove access in a timely manner.

Inactivity Security

Users are required to lock their workstations if they are leaving their computer unattended. Where the functionality exists, procedures will be implemented to terminate an electronic session after a period of user inactivity. This automated lock will occur if users leave their computer idle for 15 minutes.

Account Monitoring

The Green Bank and third-party vendors monitor systems by receiving alert-based notifications related to impossible travel or standard login monitoring processes.

Access Review and Updates

User access will be reviewed on a periodic basis to ensure users are granted the correct level of access as business changes. Updates will be made to ensure active users are

enabled, inactive users will be disabled and generic/shared account, service account, privileged accounts will be reviewed as applicable.

Identification and Authentication

Unique Identification

The Green Bank will issue unique accounts to users as a standard approach to obtaining access to all systems.

Multifactor Authentication

Where applicable, multifactor authentication is enabled for all standard user and administrator accounts. Any exceptions will be tracked and approved by the Head of Operations.

Local Access

Standard user accounts do not have local administrative access. Approved administrative accounts have local access as required to support user functions.

Network Access

In Green Bank facilities, network access relies on physical access controls. Critical systems are cloud based, and alternate controls are in place to minimize risk.

Single Sign-On

Single sign-on enables users to log in once and gain access to multiple system resources. The Green Bank will consider the operational efficiencies provided by single sign-on capabilities with the risk introduced by allowing access to multiple systems via a single authentication event and configure where necessary.

Remote Access

Remote access is provided to authorized users only. Business needs are assessed and approved if necessary.

User Provisioning and Deprovisioning

Standard onboarding and offboarding processes are used to minimize error and streamline user provisioning and deprovisioning. Help desk tickets are used to capture requests and changes made to user accounts for Microsoft 365.

Password Authentication

Per the Data Security section of the Employee Handbook, all employees and staff (consultants, third-party contractors, and administrators) are assigned a username and password when they join the company. The administrator will require complex passwords to be used. Employees must select passwords that cannot be easily guessed or that appear in a standard dictionary. Company owned devices are password protected, including computers and tablets.

System Security

See the Software section of the Employee Handbook for governance related to software license use and software installation on company hardware. The descriptions of systems used by the majority of Green Bank employees are outlined in this section.

Configuration Management

See the Computer Use Policy, including the Standard Configuration section of the Employee Handbook for standard configuration guidance as it relates to employees.

System and Services Acquisition

The third-party vendor who manages the network and Microsoft 365 environments, has a standard change management process implemented with details related to system changes and rollback procedures.

System and Information Integrity

The following are in place to maintain system and information integrity:

- Logging & system monitoring will be implemented in applicable systems by a third-party vendor to centralize logs and report on detected events.
- Automated patching, software and firmware updates will be deployed to reduce risk and eliminate room for error.

Audit Controls and Monitoring

The following protections are in place in applicable systems:

- Event Logging
- Centralization of audit logs/compilation of audit records from multiple sources
- Auditing privileged functions

- Real-time alerts/automation
- Audit log review, analysis and reporting
- Protection of audit information

Data Protection, Privacy, PII Processing and Transparency

The Green Bank takes the privacy and confidentiality of personal information seriously. The following are in place to protect this data:

- The General Rules of Conduct section in the Employee Handbook includes a Confidential Disclosure Policy, which Green Bank personnel attest to.
- The Professional Services Agreement with third parties includes a Disclosure of Information section to address the protection of confidential information.
- A Website Privacy Policy
- A Privacy Policy

Data Retention & Disposal

The organization has implemented an archiving service for data in Microsoft 365 to meet FOIA and other retention requirements.

Privacy

A Privacy Policy has been developed to protect the privacy of personal information collected, used and processed by the Green Bank.

Third Party/Vendor Management

The Vendor Management Policy establishes the requirements for onboarding, monitoring and offboarding third-party vendors to ensure they meet the organization's standards for security, compliance, performance, and risk management. This helps safeguard organizational data, maintain compliance with applicable regulations, and reduce vendor-related risks.

Vendor Selection and Onboarding

The goal of onboarding is to only disclose information to a vendor after satisfactory assurances have been obtained that they will appropriately safeguard the information as stated in a fully executed Professional Services Agreement (PSA).

The following procedure will be completed upon onboarding a new vendor:

1. The organization will assess the proposal, quote or statement of work received from the desired vendor to determine the vendor's ability to meet contractual obligations and conduct research as required of the vendor's reputation.
2. The Green Bank will perform additional due diligence for any vendor handling nonpublic or confidential data or has access to critical systems used to meet customer commitments and deliverables. This includes obtaining a SOC 2 Report from these vendors and potentially auditing the vendor's security posture via electronic questionnaire. Designated Green Bank personnel will perform an assessment of the identified subservice organization's SOC report when they become available to ensure that key controls are designed appropriately and operating effectively and that they coordinate with the controls implemented at the Green Bank. See the Monitoring section for details of how SOC 2 Report assessments are performed. If the desired vendor does not have a SOC 2 attestation, the Green Bank will engage their managed IT services partner to assess the risk inherent in a possible working relationship.
3. All vendor engagements must be approved by the Head of Operations.
4. A Professional Services Agreement (PSA) must be fully executed by the vendor and the Green Bank. Agreements with vendors include clearly defined terms, conditions, and responsibilities between the Green Bank and the vendor and are required to be executed prior to the commencement of a business relationship. If a vendor is not providing services and they are only providing products or licenses, they may not be required to sign a PSA and a Purchase Order (PO) may be used it's place. In some cases, a Memo of Understanding (MOU) may be used depending on the type of vendor or service.
5. All Vendor Agreements will be centrally stored.
6. As aligned with the Employee Handbook, Vendor Management Policy, security controls will be in place to minimize risk of vendor's accessing Green Bank systems and data.
7. Vendor access must be authorized, access requests and approvals must be documented, and access must be granted the least privileged level of access to systems and data required to perform necessary functions.
8. Vendors will be added and classified by risk level in the organization's vendor management tracking system, including start date, termination date, and any access third parties may have to the company's systems.

Tracking

Vendors will be centrally organized by the Operations team using a vendor tracking platform.

Monitoring

Vendor compliance must be reviewed at least annually for all critical vendors who handle nonpublic or confidential data or have access to critical systems used to meet customer commitments and deliverables. These reviews may include security and compliance attestations via SOC 2 Report assessments and security questionnaires. Issues or deficiencies must be tracked, remediated, and reported to management.

The following SOC 2 Report assessment procedure will be completed for applicable vendors:

1. A designated Green Bank employee and/or external partner will review the vendor tracking platform to identify new and recurring vendors who require a SOC 2 Report assessment.
2. This designee will reach out to these vendors and request an updated SOC 2 Report.
3. These SOC 2 Reports will be centrally stored for ease of access.
4. A standard form will be used to document the assessment of vendor SOC 2 Reports.
5. This designated employee will assess the SOC 2 Reports for:
    a. The auditor's opinion: Verified that within the Independent Auditor's Report section, a clean or unmodified opinion was issued by the auditor. If a modified opinion was issued, the reason for the opinion will be assessed along with the impact it has to the Green Bank's operations.
    b. Management's assertion and Systems Description sections to verify the scope and description align with the services and commitments required from the vendor.
    c. Complementary user entities control section: Verify that the Green Bank has the appropriate internal controls in place at the Company to address the relevant complementary user entity controls mentioned in the report, where applicable.
    d. Subservice organizations: Assess if the organization outsourced any functions relevant to the plan's internal control over financial reporting to another service organization (a subservice organization), and if the subservice organization is carved out of the type 2 report.
    e. Exceptions found: Assess the testing procedures and results mentioned in Section 4 of the report. For any exceptions identified, determine the nature of the exception and the impact it has to the Green Bank's operations, if applicable.
    f. Management's response section to exceptions found: Analyze the responses provided to exceptions, identify if any were resolved prior to this assessment,

determine if alternate mitigating controls are in place and assess the overall risk and impact to the Green Bank's operations.

6. If needed, the vendor will be asked to make modifications to mitigate exceptions and provide assurance that they have met their service commitments and system requirements. In cases where a significant carve out of subservice organization work is present, depending on the nature of this work and impact on CT Green Bank's operations, a SOC 1 Report or additional SOC 2 Report may be required.
7. The SOC 2 Report Assessment forms and all related documentation will be centrally stored along with the vendor's SOC 2 Report.

Termination and Offboarding

Terminated vendors will be addressed consistently and in a timely manner to minimize risk to the organization.

The following procedure will be completed upon terminating a vendor:

1. Access credentials, integrations, and vendor accounts will be revoked promptly.
2. The vendor will be required to return or securely destroy all organization data and provide confirmation of secure destruction in a timely manner.
3. For applicable vendors, an exit strategy and transition plan will be created to reduce interruption to operations and facilitate a smooth transition.
4. A post-termination review may be conducted to assess lessons learned and properly closeout any agreements with the vendor.
5. All evidence of offboarding and vendor termination must be maintained in accordance with the internal employee termination process.

Compliance & Monitoring

The Green Bank takes violations of security policies and procedures very seriously. Suspected or actual violations will be documented, investigated and tracked per the Progressive Discipline Policy in the Employee Handbook. Non-compliance with this policy may result in disciplinary action, up to and including termination of employment.

Policy Management

The Green Bank will maintain this policy in accordance with other security polices to comply with required frameworks, regulations and company standards. If modifications are made to this policy, they will be documented, reviewed and approved prior to implementation across the workforce. This policy will be reviewed annually internally at the

staff level or as business needs and regulatory requirements evolve and approved by the Head of Operations. Any substantive changes will be presented for Board of Directors' review and approval prior to implementation. This policy will be made available to employees and centrally stored with other company policies and procedures.

Acknowledgement

Employee acknowledgement will be collected when this policy is updated and when new employees join the Green Bank.

Privacy Policy

Effective Date		**Review Frequency**	Annually or at a major change in business function or system
Approval Date		**Approved By**	
Reviewed Date	12/19/2025	**Reviewed By**	Head of Operations

Version History

Version	Date	Prepared By	Approved By	Summary of Modifications
1.0	12/19/2025	Operations Team		First Draft

Table of Contents

Purpose

This Privacy Policy defines how Connecticut Green Bank will collect, use, disclose, retain and protect personal information. The topics within this policy are developed to consistently implement standards and set expectations with the workforce to minimize risk and safeguard the confidentiality of personal information.

Scope

This policy applies to:

- Personal information processed by the Green Bank
- All employees, contractors, interns, website visitors
- All information systems, applications, cloud environments, networks and data owned or managed by the Green Bank.

Objectives

Develop and disseminate an organization-wide Privacy Policy that:

- Protects personal information processed by the Green Bank
- Set clear roles and responsibilities
- Support data subject rights

Definitions

Personal Information (PI): Any information that can be linked to an identifiable individual, relates to or describes the individual, excluding publicly available information.

Sensitive Personal Information: Personal information requiring heightened protections due to potential harm if disclosed.

Processing: Any operation performed on personal information, including collection, use, storage, disclosure, or deletion.

Data Subject: An identified or identifiable individual whose personal information is collected and processed.

Roles and Responsibilities

Role	Responsibilities
Board of Directors	Approve this policy and related policies and procedures, oversee and support the Privacy program, document agendas, minutes and signatures showing oversight.
Head of Operations	Review and provide feedback on this policy, approve risk management strategy, allocate resources, approve vendor onboarding, provide direction and support the Privacy program. Act as the contact for all privacy inquiries and complaints from data subjects.
Operations Team	Develop policies, coordinate risk assessments and audits, maintain risk register, perform security, privacy and compliance related activities as delegated by the Head of Operations, implement and maintain security and privacy controls and perform vendor risk management activities.
Department Heads	Ensure compliance with privacy requirements in their teams, identify and report risks in their area, ensure controls are followed. Define service requirements and monitor vendor deliverables. Communicate vendor performance, security or privacy concerns immediately to the Head of Operations.
Legal	Review and provide guidance on all contracts and regulatory obligations. Provide feedback on policies as needed.
All Staff and Contractors	Follow policies and procedures, report incidents, potential risks or unauthorized disclosure of personal information in a timely manner, complete required training.
System Owners/ Administrators	Ensure access is authorized, documented and granted based on the principle of least privilege, required security and privacy controls are configured, and system is periodically monitored. Stay up-to-date and address system upgrades, new features and updates that may increase risk.
Third-Party Vendors	Meet contractual security obligations and undergo due diligence audits as applicable.

Data Collection and Use of Personal Information

The Green Bank collects personal information as well as some sensitive personal information for specific uses. Most often, information is provided by the data subject directly into relevant Green Bank systems or security transmitted to the Green Bank for processing and management.

The categories of personal information include:

- Identifiers (personal contact information like name, phone number, email address, physical address)

- Account information
- Business contact information
- Usage and device data
- Sensitive personal information (social security numbers, tax information)

The Green Bank limits the use of personal information to the following uses:

- Account management
- Underwriting
- Customer support

Legal Basis and Consent

Where required, the Green Bank obtains consent from data subjects prior to processing personal information. The Terms and Conditions in Program documentation provide notice of privacy practices to data subjects.

Disclosure or Sharing of Personal Information

The Green Bank discloses or shares personal information with:

- Authorized employees with a need to know
- Service providers when necessary
- Legal and regulatory authorities when required by law

Data Retention and Disposal

Data is retained for a minimum of two years. If data disposal is required, approved methods will be used to securely dispose of required information.

Data Subject Rights

Data subjects provide consent to the use and processing of their personal information. The Green Bank supports the following when requested by data subjects:

- Access to personal information
- Correction of inaccurate or outdated information
- When possible, requests for deleting personal information or restricting the processing of certain processing activities will be accommodated

In most cases, data subjects can update their personal information directly in systems they have access to, however the Green Bank will correct, amend or append personal information based on information provided by data subjects when required. The Green Bank's goal is to collect and maintain accurate, up-to-date, complete and relevant personal information.

Data Privacy Contact

The Head of Operations will be the main point of contact for all privacy related inquiries, complaints and disputes from data subjects.

Information Security Safeguards

The Green Bank implements an Information Security Policy, which outlines the security controls to safeguard confidential and nonpublic information, including personal information. In systems where data subjects have access to their personal information, access is granted only for identified and authenticated data subjects.

Incident Response and Breach Notification

An Incident Response Plan is in place to prepare, detect, respond, recover, report and learn from incidents. In the case an incident occurs that impacts data the Green Bank collects, uses or processes, an analysis of the types of data impacted and regulatory requirements will be performed. If it is determined that unauthorized disclosure of personal information took place, a record will be retained and reported to affected individuals.

The Green Bank also has Professional Service Agreements in place with third parties who have access to personal information. The Professional Service Agreement requires third parties to notify the Green Bank of any actual or suspected unauthorized access, acquisition, disclosure, alteration or loss of confidential or nonpublic information. Upon notification, the Green Bank will perform an analysis of the types of data impacted and create a record of unauthorized access to be retained and reported to affected individuals.

Privacy Training

As aligned with the security awareness training program, the purpose of providing privacy training to the workforce is to minimize risk to confidential and nonpublic information by providing knowledge of privacy best practices. Training will be scheduled and tracked by the Operations Team and the organization's third-party vendor.

Compliance & Monitoring

The Green Bank takes violations of privacy policies and procedures very seriously. Suspected or actual violations will be documented, investigated and tracked per the Progressive Discipline Policy in the Employee Handbook. Non-compliance with this policy may result in disciplinary action, up to and including termination of employment.

Policy Management

The Green Bank will maintain this policy in accordance with other security polices to comply with required frameworks, regulations and company standards. If modifications are made to this policy, they will be documented, reviewed and approved prior to implementation across the workforce. This policy will be reviewed annually internally at the staff level or as business needs and regulatory requirements evolve and approved by the Head of Operations. Any substantive changes will be presented for Board of Directors' review and approval prior to implementation. This policy will be made available to employees and centrally stored with other company policies and procedures.

Acknowledgement

Employee acknowledgement will be collected when this policy is updated and when new employees join the Green Bank.

845 Brook Street, Rocky Hill, CT 06067
T 860.563.0015
ctgreenbank.com

CONNECTICUT GREEN BANK

Memo

To: Audit, Compliance and Governance Committee

From: Eric Shrago, Executive Vice President of Operations

Date: January 5, 2026

Re: Environmental Impact Measurement Update

Describing the environmental contributions of the portfolio of projects supported by the Connecticut Green Bank helps illustrate the contributions of the organization and is a key part of the Societal Impact section of the Evaluation Framework. The organization has been using the US Environmental Protection Agency (EPA)'s AVoided Emissions and geneRation Tool (AVERT) since the Board approved it in 2017. The AVERT model is widely used and accepted as the best-in-class air quality model for energy-related emissions impacts. The model is integrated with the EPA's Co-Benefits Risk Assessment (COBRA) health impacts model.

In consultation with the EPA, Customized Energy Solutions (our current EM&V partner for Energy Storage Solutions), and Guidehouse (the former EM&V partner for Energy Storage Solutions) we propose that we leverage the model to estimate our air quality impacts for energy storage and electric vehicles.

Further, the updated AVERT model now produces estimates of impacts for changes to Volatile Organic Compounds (VOC) and ammonia (NH3) emissions, both of which have significant public health impacts. We propose to start tracking our impact regarding both of these pollutants and leverage the outputs of AVERT in terms of tracking the timing of ozone pollution to show what we are alleviating in terms of summertime smog.

We intend to use the model in the same manner as we have for energy generation and energy efficiency where we use factors that estimate the air quality impacts based on the size in MW of the storage installed or the number and type of electric vehicle supported. This operationalization is supported and copied by the EPA and is aligned with recent reporting requirements from EPA.

Resolution

RESOLVED, that the Audit, Compliance and Governance Committee hereby recommends to the Board of Directors for approval on its consent agenda the EPA AvERT Model for the Evaluation and Measurement of the environmental impact of Green Bank supported energy storage and electric vehicle projects as well as the estimation of the aforementioned pollutants.

Office locations
75 Charter Oak Ave., Suite 1 – 103, Hartford, CT 06106
700 Canal Street, 5th Floor, Stamford, CT 06902

Phone
T: 860.563.0015
F: 860.398.5510