The Community Foundation for Greater New Haven

Acceptable Use of Information Systems

Effective Date: December 12, 2025

This policy outlines the acceptable use of The Community Foundation for Greater New Haven's (“The Foundation") information technology resources, including company-provided laptops and personal mobile devices used for work purposes. The purpose is to protect the Foundations data and systems, ensure compliance, and promote a secure and productive work environment for all employees. This policy applies to all Foundation employees, affiliates and anyone else who accesses our IT resources.

Acceptable Use Guidelines (What You Can Do)

CFGNH provided systems, applications, and hardware are intended for business use. Limited personal use is permitted, provided it does not interfere with job responsibilities, compromise system integrity, or violate any company policies. Acceptable uses include:

- **Using Foundation-Provided Devices:** Use your assigned computer, laptop, or phone for work-related tasks.
- **Using Approved Software:** Use only software and applications that have been approved and provided by The Foundation.
- **BYOD Reimbursement**: The Foundation will reimburse data plans, voice plans, or other costs associated with personal devices per separate policy

---

Acceptable Use Guidelines (What You Can't Do)

Users are strictly prohibited from using CFGNH systems for any illegal, unethical, or disruptive activities. To protect our data and systems, certain activities are strictly prohibited:

- **Physical Security**: Users shall take all reasonable and prudent measures to physically secure all information system assets.
- **Using Unapproved Software:** Do not download or install any unauthorized software, shareware, or freeware on any Foundation-owned device.
- **Passwords**: Users shall follow guidelines for strong, unique passwords and enable multi-factor authentication (MFA), when available. Best practices regarding passwords, especially when MFA is not available, are:

- Passwords should be at least 14 characters in length, with passphrases (combinations of words) being more secure.
- Users are responsible for safeguarding their passwords and must not reveal them to anyone, use the 'remember password' function, or store them unencrypted.
- Multifactor Authentication enabled for CFGNH assets containing Restricted or Confidential data.
- Avoid using sequential or repeated characters, knowledge-based authentication (e.g., "What was the name of your first pet?"), or context-specific words within passwords.
- Do not use the same password for different CFGNH systems (unless configured to do so) or for systems inside and outside of work.
- Sharing credentials or Foundation laptop with anyone, including other CFGNH employees or contractors, is prohibited.
- Do not save your passwords in a document on your computer or write them on sticky notes or other physical items around your workstation.

- **Unauthorized System Changes:** To help prevent unauthorized changes and to maintain integrity, security, and compliance, software installation is only completed by Novus Insight. CFGNH reserves the right to monitor its information system. Users are prohibited from disabling or interfering with any function installed by the Foundation.

- **Storage & Sharing**: Users must store and share data only through Foundation approved software platforms. Sending work files to personal email or cloud accounts is prohibited. When sharing Confidential or Restricted data externally, users must use encryption. Use of removable media (e.g., USB drives) is not allowed for Confidential Information. Do not send Personally Identifiable Information (PII) or other sensitive data through email.

- **Improper Content and Behavior:** The technology environment is an extension of our work environment. The following activities are prohibited by this policy:
  - Accessing or distributing illegal, bullying, harassing, or discriminatory content.
  - Using pirated software or violating copyright laws.
  - Spoofing, falsifying identities, or unauthorized data sharing.
  - Circumventing established security controls or monitoring tools
  - Information must not be stored on unauthorized personal devices or public cloud services.

- **Artificial Intelligence (AI):** The use of Artificial Intelligence (AI) tools is permitted for non-sensitive internal communications, document summarization, basic data analysis, and process automation, but employees must never input confidential or proprietary

information into any AI system. All AI-generated content is considered draft material and requires a human review and verification for accuracy, with the user retaining full responsibility for the final output; additionally, be mindful that bias can affect AI results. All AI-created material must be clearly identified as such, and any uncertainty regarding the accuracy of the results must be explicitly disclosed in the material. **No paid subscriptions for AI services are authorized for purchase by staff.**

- **Training:**

  Phishing and Security Training: The The Foundation uses **KnowBe4** to conduct regular, random phishing tests. If you fail a phishing test (e.g., by clicking on a malicious link or downloading an attachment), you will be automatically enrolled in mandatory, additional security training. The results from the KnowBe4 software will be considered final, and the Foundation will not entertain disputes regarding the testing process.

Security and Privacy:

Physical Security: Users shall take all reasonable and prudent measures to physically secure all information system assets. Users shall not attempt to circumvent any security systems, protocol, or configuration on the information system or technology infrastructure.

Handling Personally Identifiable Information (PII): We **do not accept PII into our environment** unless it is explicitly required for a legitimate business purpose and handled through approved, secure channels. Personally Identifiable Information (PII) is any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information.

- **Definition of PII (Connecticut Law)**

  For the purposes of this policy, Personally Identifiable Information (PII) refers to any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. PII often includes, but is not limited to:

  - Social Security number
  - Driver's license number or state identification card number

- Financial Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account
- Passport number or Military identification number
- Username or email address in combination with a password or other means of access

Other forms of information that should not be in our environment include:

A. Medical information

B. Credit Card information

Enforcement:

Employee Involvement in Security Incidents: Violations of this policy may result in disciplinary action, including loss of access, termination, or legal action. CFGNH reserves the right to update this policy at any time.

Reporting Incidents: Users must immediately report any suspected or confirmed security incident or threat to the IT services provider (Novus) via email at help@novusinsight.com or by phone at (860) 282-4200. Incidents include lost or stolen devices or data, computer virus, compromised password, unauthorized access or use of data and policy violations. The internal contact for security incidents is Wendy Gamba.

No Expectation of Privacy:

Users should have no expectation of privacy when using CFGNH information systems, as all system assets and user accounts are the property of CFGNH and are provided solely to support job related duties or other authorized purposes. While using the information systems, users expressly waive any right to privacy in anything they create, store, send, or receive, and consent to access and review of such materials by executive leadership. CFGNH may monitor system use. Users must understand that electronic communications, including email, are neither private nor secure and may be subject to legal discovery at the direction of counsel.

By using The Community Foundation for Greater New Haven's technology resources, you agree to abide by this policy. Failure to comply may result in disciplinary action, up to and including termination of employment.

Acknowledgment

I, _____, acknowledge that I have read, understood, and agree to abide by the terms and conditions set forth in this User Acceptance Policy. I understand that failure to comply with this policy may result in disciplinary action, up to and including termination of employment.

Employee Signature: _____

Printed Name: _____

Date: _____

Policy Interdependencies
Password Complexity Policy
Social Media Policy
Confidentiality Policy