CARE COMPASS NETWORK

CCN IT Security Requirements Guide

Document Owner: Information Security Manager

Document Number: SEC_PS7-2b

Purpose:
This document provides an operational guide for CCN staff on CCN's IT Security requirements and related processes for both onsite and teleworking CCN staff.

Requirements:

Computer Security:

- Lock computer screen when leaving your desk (windows key + L)
- Be cautious when opening emails and attachments that you are not expecting.
  - Do not open emails or email attachments from unknown senders/sources.
  - If you are unsure of the legitimacy of the email or attachment, err on the side of caution and contact the Information Security Manager for advice.
  - Report all suspicious emails or attachments with the “Phish Alert Report” button in Outlook or to the Information Security Manager.
    - If you click on a link or open an email and then suspect that it was a phish, report it immediately to the Information Security Manager and the IT Director/Security Officer.
- Laptops are required to be locked via a cable lock when they are in the office.
  - Store cable lock keys in discrete and secure location.

Individual Account Standards:

- Account Responsibilities
  - Users are responsible for all activity performed with their CCN accounts.
  - CCN accounts may not be utilized by anyone but the individuals to whom they have been issued.
  - Users must not allow others to perform any activity with their CCN accounts.
  - Any suspected unauthorized access to a user account should be reported immediately to the Information Security Manager.
- Passwords

    - Regardless of the circumstances, passwords must never be shared or revealed to anyone else besides the authorized user. To do so exposes the authorized user to responsibility for actions that the other party takes with the password.
    - All users are responsible for both the protection of their user account password and the data stored in their user account.
    - Do not write passwords down.
    - Make your password complex and difficult to guess – suggestion: use a passphrase instead of a password, substituting numbers and special characters for some of the letters. Don’t use your name or the name of your child, dog, favorite sports team, etc.
        - CCN requires at least 10 characters with a combination of special characters, upper- and lower-case letters.
    - Common passwords are ***prohibited*** from being used for your password (e.g., Password123, Qwerty1234)
    - Password expirations limits are enforced on all accounts.
    - Password expiration durations are based on the type of data housed in the system.

Office Suite Requirements:

- Remind guests entering the CCN office suite to Sign in and Sign out of the Visitor Log
- Guests must wear visitor identification and be escorted by a CCN Staff member while they are in the CCN Office Suite
- When entering and leaving the CCN office area, ensure that doors close completely behind you.
- Never connect external computers or devices to the CCN Network (hardwired or Wi-Fi (CCN-NET))
    - **CCN-Wi-Fi** is available for Guest Devices
- Lock Print Jobs with a PIN when prints contain sensitive or confidential information.
- Non-CCN USB media (thumb drive, CD, DVD) is ***restricted*** from use on CCN devices.
    - Encrypted USB thumb drives are available to be signed out for use from the IT Helpdesk

Data Storage and Protection Requirements:

- CCN Staff are ***prohibited*** from transmitting ***unencrypted*** PHI, PII, and sensitive information.
    - CCN staff can encrypt emails with AppRiver Secure Message encrypted email through the Outlook plug-in.
    - The CCN SFTP site is also available to staff for securely sending information. Ad-Hoc Requests to send files through the SFTP site are sent to the IT helpdesk to

initiate the file transfers. Files uploaded to the SFTP site are stored in a secure environment that is segregated from CCN's business network.

- If users receive unencrypted sensitive or confidential data, they are required to contact CCN Corporate Compliance and Privacy Officer
    - After the incident has been reported, users are required to:
        - Delete the Data immediately and empty the trash/recycle bin.
        - Never retransmit the sensitive information to anyone (CCN or external)

- Files containing PHI, PII, and Sensitive Information:
    - are prohibited from being left unattended or available for unauthorized individuals, i.e. Visitors, contractors, family members (teleworking) to access, including on desks, printers, copiers, fax machines, and computer monitors.
    - are required to be always stored in a secure location and only in the designated and approved system or other appropriately secured system approved by the Information Systems Director.
        - Physical copies (e.g., paper copies) of documents that contain PHI, PII, and sensitive information must be stored in a locked drawer or file cabinet.
    - are required to be stored ***only on CCN-owned encrypted storage devices*** with applicable security functions enforced.
        - CCN prohibits the storage of PHI, PII, and Sensitive Information on unencrypted devices including hard drives, removable storage, and other external media.
    - are prohibited from being stored in CCN business network file shares (i.e., G:, H:, U: drive)
    - are prohibited from being locally or remotely copied (including print screen), moved, printed, and stored without a prior defined business need.

Data Retention and Destruction:

- PHI, PII and other sensitive should only be kept for the time deemed necessary to complete CCN staff duties and responsibilities.
- Once data is no longer deemed necessary to be stored at CCN, proper data sanitation processes must be followed.
    - Digital Files containing PII, PHI and sensitive data should be cut and pasted into G:_PHI(ToBeDestroyed) for proper destruction this includes local files and files stored on the G:
    - Physical copies (e.g., paper copies) of documents that contain PHI, PII, and sensitive information must be placed in the locked blue bins near the printers in the CCN Office Suite. CCN contracts with a third-party vendor to properly dispose of this information by shredding it.

- Contact the IT Helpdesk with questions or for assistance.

Video Teleconferencing Privacy and Security Guidelines

- Restrict showing/discussing PHI, PII or sensitive information during the meeting.
  - If you expect to show or discuss PHI, PII or sensitive information, request the HIPAA settings for Zoom to be applied to your account.
- Some video teleconferencing applications are HIPAA compliant; when in doubt assume that it is not.
- Keep your video conferencing software updated to keep current with privacy, security, and reliability.
- Keep meeting ID#s private and password protect meetings to stop unwanted people from eaves dropping or "Zoom Bombing" your meeting.
  - if an unidentified number shows in the meeting as host you should identify the person and change the name to the appropriate person
    - If an unidentified number fails to identify themselves, they should be removed from the meeting.

Insider Threat:

- Insider Threat is the potential for an individual (current or former employee, contractor, or business partner) who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization.
- Consequences of Insider Threats:
  - Theft of Sensitive Data
  - Induce System and Network Downtime
  - Destruction of Property
  - Damage to Reputation
- Indicators of a potential insider threat:
  - *Behavioral Indicators* are actions directly observable by peers, HR personnel, supervisors, and technology. Over time, behaviors create a baseline of activities from which changes may be considered a threat indicator.
  - *Technical Indicators* involve network and host activity and require direct application of IT systems and tools to detect.
  - *Environmental Indicators* can escalate or mitigate stressors that may contribute to behavioral changes and an individual's progression from trusted insider to insider threat.

  - *Violence Indicators* are specific behaviors or collections of behaviors that can instill fear or generate a concern that a person might act; these behaviors include, but are not limited to, intimidation, harassment, and bullying.

Incident Reporting:

- If data containing PHI, PII, or sensitive data is suspected to be compromised or breached, the incident must be immediately reported to the CCN Corporate Compliance and Privacy Officer, or the Information Security Manager either directly or via the anonymous compliance reporting.
- In the event of a suspected security incident, immediately report it to the Information Systems Director or the Information Security Manager. Examples include:
  - Clicking on a suspicious link;
  - Computer Virus;
  - Spyware/Malware Infections;
  - Password Compromise;
  - Suspicious actions of individuals or evidence of Insider Threat;
  - Suspected data/device loss/theft;
  - Unauthorized interactions or removal of CCN devices or information.

- **CCN Compliance Hotline:** https://bit.ly/CareCompass-Compliance
- **Corporate Compliance and Privacy Officer**:
  Andrea Rotella: (607) 240-2591
  ARotella@carecompassnetwork.org
- **Information Security Manager**: Dustin Moore: (607) 240-2589
  DMoore@carecompassnetwork.org

Disciplinary Actions

Failure to adhere to IT and Security policies and procedures may result in disciplinary actions, as described in the HR1-11 Disciplinary Actions Procedure.

My Signature below indicates my acknowledgment and understanding of the IT security Requirements outlined in this guide.

Printed Signature ______________________________________ Date: ________________

Signature____________________________________

Versions: 5/29/19, 5/25/21, 4/11/2022, 6/8/2023, 5/1/2024

CARE COMPASS
NETWORK