Adirondack Health Institute

Lead Empower Innovate

POLICY AND PROCEDURE

Title: Security Policy – Network Security

Department: Compliance

Effective Date: 10/2016

Annual Review Date: 01/2019

Date Revised: 01/2018

Definitions

Workforce member means employees, board members, volunteers, interns, independent contractors, vendors, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. This includes full and part time employees, affiliates, associates, volunteers, and staff from third party entities who provide service to the covered entity.

Purpose of Policy

The purpose of this policy is to describe the physical safeguards applicable for each server, desktop computer system and wireless computer system used to access, transmit, receive and store PII, PHI and sensitive company data to ensure that appropriate security is maintained and that access is restricted to authorized workforce members of AHI.

Network Security

AHI will take reasonable and appropriate steps to prevent unauthorized access to workstations, servers and portable devices including laptops, smartphones, CD-ROMs, DVDs, USB Drives, etc. that store or access PII, PHI and sensitive company data.

1) Workstations and laptops that are in common areas that store or access PII, PHI and/or sensitive company data should be physically placed with the monitor in a direction so that it prohibits unauthorized people from viewing confidential information such as logins, passwords, PII, PHI and/or sensitive company data.

2) Workstations and laptops that are in common areas that store or access PII, PHI and sensitive company data should utilize privacy screens to prevent unauthorized access to the data.

3) Workstations and laptops that are in common areas that store or access PII, PHI and sensitive company data should be secured by restraints such as locking cables.

4) To the extent technically feasible all portable devices that contain PII, PHI and/or sensitive company data should be encrypted to protect the contents. In addition, encryption should be used when sending any PII, PHI and/or sensitive company data across public networks and wireless networks. Public networks include email and Internet access.

5) Portable devices and media should be concealed from view when offsite to prevent theft.

6) All network servers, application servers, routers, database systems, device management system hardware, and other servers should be located in a room or an area that can be physically secured by lock and key or any other appropriate security mechanism to limit access to only authorized personnel.

7) All workstations, servers and portable devices will run anti-virus / anti-malware software that protect against malicious software. The software must be current and up to date with virus / malware definitions. Authorized workforce members must use and keep active current versions of approved anti-virus / anti-malware software scanning tools to detect and remove malicious software from workstations and files. Authorized workforce members must not disable these tools unless specifically directed by computer support personnel to do so in order to resolve a particular problem.

8) A network firewall should be in place to protect PII, PHI and/or sensitive company data. The firewall protection should be up to date. Firewalls should be monitored and alerts should be triggered in the event of unauthorized intrusion or suspected intrusion.

9) Log files from network equipment should be stored and retained. Log files from network equipment include; firewalls, network servers, desktops, laptops and other devices. The required length of retention of log files may vary depending on federal, state or industry regulations.

10) All workstations, servers and portable devices, where feasible, must implement a security patch and update procedure to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.

11) Periodic network vulnerability scans should be performed on all internal as well as external (Internet facing servers, websites, etc.) systems. Results of the vulnerability scans should be analyzed and known vulnerabilities should be remediated and/or patched. After all vulnerabilities are remediated, an external network penetration test should be performed to ensure that unauthorized external access into the network is prevented.

12) Reasonable and appropriate steps will be taken to prevent unauthorized access to workstations, servers and portable devices from misuse and physical damage, vandalism, power surges, electrostatic discharge, magnetic fields, water, overheating and other physical threats.

    a. Workstations must not be located where they will be directly affected by extremes of temperature or electromagnetic interference. Precautions should also be taken to

ensure that workstations cannot be affected by problems caused by utilities, such as water, sewer and/or steam lines that pass through the facility.

b. All facilities that store systems that contain PII, PHI and/or sensitive company data, should have appropriate smoke and/or fire detection devices, sprinklers or other approved fire suppression systems, and working fire extinguishers in easily accessible locations throughout the facility.

c. All servers that contain PII, PHI and/or sensitive company data, should be connected to an Uninterrupted Power Supply (UPS) to prevent server crashes during power outages or spikes. Servers should be configured to shut down in a controlled manner if the power outage is for an extended period of time.

d. All systems should be connected to surge protectors, where feasible, to protect against power spikes and surges.

13) A user identification and password authentication mechanism shall be implemented to control user access to the system. (See Security Policy - Access Control).

14) Authorized workforce members who suspect any inappropriate or unauthorized use of workstations should immediately report such incident or misuse to the Compliance Department Security Officer. The Compliance Department and Technology Director will address this issue accordingly.

Policy Compliance

The Compliance Department will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, business tool reports, internal and external audits, and any other necessary means of investigation.

Any workforce member found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or services. In cases where local, state, or federal laws have been violated, workforce members may also face prosecution.

Any workforce member that witnesses a violation of this policy is required to report the incident at the earliest possible moment to either a supervisor or to the Compliance Department. Any incident reported in good-faith is protected under AHI's whistleblower policy.

Contact Person: Corporate Compliance and Privacy/Security Specialist

Responsible Person: Security Officer

Approved By: Chief Executive Officer