WOODBURY COUNTY, IOWA

SECURITY AWARENESS POLICY

Last Update Status: Updated May 2023

PURPOSE

Cyberattacks and *ransomware* threats take advantage of common Internet traffic, such as email, which can bypass perimeter security in attempt to compromise *networks* by exploiting weaknesses in human nature. The purpose of this Administrative Policy (AP):

- Define *Security Awareness* Training (SAT) for a *network client.*
- Outline tools used by *WCICC-IT* to regularly test the network client with simulated cyberattacks.
- Define disciplinary actions for failing simulated and legitimate cyberattacks.

SCOPE

This policy applies to all network clients operating on the behalf of the City of Sioux City.

RESPONSIBILITY

- WCICC-IT is responsible for providing education and testing for vulnerabilities related to Cyberattacks for all network clients.
- The Human Resources Department, along with the network client's immediate supervisor, are responsible for notifying WCICC-IT of all new network clients' need for network access and for promptly notifying WCICC-IT of all terminated network clients.
- The Human Resources Department, along with the network client's immediate supervisor, are responsible for ensuring the initial and annual training are completed within 14 calendar days.

DEFINITIONS

Cyberattacks – An attempt to gain access to a computer or computer systems for the purpose of causing harm to the confidentiality, integrity, and availability of the network system.

Incident – Clicking a link, opening an attachment, entering credentials, or some other action on a simulated or a legitimate phishing email is also considered an incident.

Network – a system containing any combination of computers, printers, audio, or visual display devices and/or telephones interconnected by telecommunication equipment or cables used to transmit or receive information.

Network Client – Any individual that makes a direct or wireless connection to the WCICC-IT network infrastructure using an electronic device.

Phishing – The act of sending email that falsely claims to be from a legitimate organization, with the goal of tricking the person into providing information that can be used against the organization.

Ransomware - A type of malicious software designed to block access to a computer system until a sum of money is paid.

Security Awareness – The knowledge and attitude of members of an organization possess regarding the protection of the physical and informational assets of that organization.

Woodbury County Information and Communication Commission Information Technology (WCICC-IT) – As defined by the 28E Agreement between the City of Sioux City and Woodbury County for 911 communications and information systems.

Woodbury County Agents (WCA) – Any person operating on behalf of Woodbury County, including but not limited to employees, volunteers, contractors, and elected officials.

POLICY/PROCEDURE

- All network clients must complete the initial SAT before they are granted network access.
- Annually, SAT must be completed within 14 calendar days upon notification to maintain network access.
- WCICC-IT is authorized to periodically measure the network client's security awareness using simulated phishing campaigns and/or security trainings.
- If interaction such as clicking a link or opening an attachment is taken during the simulated test, it is considered an incident and will be met with the tiered incident response.
- In the case of a legitimate phishing attack, it will be considered an incident if there is an action taken that could cause harm to the network system

  - **First Incident:** The network client is notified. The network client must complete the refresher training within 7 calendar days of the notice and notify WCICC-IT upon completion.
  - **Second and Third Incident:** The network client and their immediate supervisor are notified. The network client must take remedial security awareness training within 5 calendar days of the notice and notify WCICC-IT upon completion.
  - **Fourth Incident:** The network client, their supervisor, and the Director of Human Resources or designee are notified, and the network access is temporarily disabled until the network client re-completes the initial security awareness training. The network client must coordinate with the Director of Human Resources or designee to complete the training and notify WCICC-IT upon completion.
  - **Fifth and Subsequent Incidents:** The network client's Director and Director of Human Resources or designee are notified, and network access is disabled pending further disciplinary action as defined by Human Resources.

All Incidents are calculated on a 12-month revolving cycle. Failure to complete any of the mandatory training within the allotted time will result in network access being disabled. Arrangements to regain access need to be coordinated with Human Resources and WCICC-IT.