

RESOLUTION NO 3,599

A RESOLUTION TO AUTHORIZE AND IMPLEMENT SECURITY AWARENESS TRAINING FOR WOODBURY COUNTY EMPLOYEES USING THE WCICC-IT NETWORK

WHEREAS, cyber-attacks and ransom-ware threats can lead to a compromised workstation or spread malware through the County's internal network which could potentially cripple or shutdown our entire network and

WHEREAS, WCICC-IT is responsible for the network which serves the County and desires to educate its users on tools and methods used in Cyberthreats and test them for social engineering vulnerabilities related to cyber-attacks and

WHEREAS, WCICC-IT desires to employ additional training and restrictions for repeatedly failing simulated cyber-attacks,

BE IT THEREFORE RESOLVED by the Board of Supervisors, Woodbury County, Iowa, hereby declare that users will only be granted to appropriate network resources based on need and successful training and

BE IT FURTHER RESOLVED that the Woodbury County Supervisors declare that all new county employees needing access to the County's network must complete basic computer security awareness training administered by WCICC-IT before they are granted network access and


BE IT FURTHER RESOLVED that the Woodbury County Supervisors declare that all currently employed county employees are to complete basic computer security awareness training administered by WCICC-IT within fourteen days of notification by WCICC-IT and the Woodbury County Human Resources Department and

BE IT FURTHER RESOLVED that the Woodbury County Supervisors declare that WCICC-IT is authorized to measure employee's security awareness through the use such tools as phishing campaigns and

BE IT FURTHER RESOLVED that the Woodbury County Supervisors declare that WCICC-IT is authorized to require additional training and restrict access to network resources for county employees that repeatedly expose the county network to cyber-attacks that are identified as real or simulated phishing emails.

SO RESOLVED this 16 day of May, 2023 and supersedes resolution #12,323 of May 10th, 2016.

Board Chair: 

Attestation: 

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.

WOODBURY COUNTY, IOWA

Acceptable Use – Technology Policy

Last Update Status: May 2023

PURPOSE

This policy outlines the acceptable use of computer equipment and electronic communication. These rules help protect the County's employees and data from serious risks, including virus attacks, compromise of network systems and services, public relations issues, and legal issues.

The goal of publishing an Acceptable Use Policy is to protect the County's employees, partners, and data against damaging actions committed either unintentionally or intentionally.

Internet/Intranet/Extranet-related systems, including, but not limited to, computer equipment, software, operating systems, storage media, network accounts, electronic mail, and WWW browsing, are the property of Woodbury County.

It is a team effort to maintain an effective security program. All employees and affiliates working with information or information systems must participate in safe security behaviors daily. Users are responsible for understanding these guidelines and conducting business accordingly. Additional training will be provided upon request to aid that understanding. Any lack of specifics within this policy does not imply a lack of employee responsibility, should specific actions necessitate managerial review or redress.

SCOPE

This policy applies to the use of information, electronic and computing devices, and network resources used to conduct Woodbury County business or interact with internal networks and business systems, whether owned or leased by Woodbury County, the employee or a third party. All employees, contractors, consultants, temporary workers, and other workers at Woodbury County and its subsidiaries are responsible for exercising good judgment regarding the appropriate use of information, electronic devices, and network resources under Woodbury County policies and standards and local laws and regulations. This policy applies to all employees, elected officials, contractors, consultants, temporary workers, and other workers at Woodbury County, including all personnel affiliated with third parties. This policy applies to all equipment owned or leased by Woodbury County.

RESPONSIBILITY

It is the responsibility of all County employees to be familiar and maintain compliancy with this policy. Department Directors and Elected Officials will work with supervisors to ensure employees are informed of this policy. The County reserves the right to monitor electronic communication without prior notification to employees. Woodbury County will verify compliance with this policy through various methods, including but not limited to business tool reports, internal and external audits, and feedback to the policy owner.

DEFINITIONS

Principle of least access - every module (such as a process, a user, or a program, depending on the subject) must be able to access only the information and resources that are necessary for its legitimate purpose.

POLICY/PROCEDURE

General Use and Ownership

- Proprietary information stored on electronic and computing devices remains the sole property of Woodbury County, whether owned or leased by Woodbury County, the employee, or a third party.
- Employees are responsible for promptly reporting the theft, loss, or unauthorized disclosure of the County's proprietary information.
- Employees may access, use, or share Woodbury County proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.
- Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should follow departmental policies for personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
- For security and network maintenance purposes, authorized individuals within Woodbury County may monitor equipment, systems, and network traffic at any time.
- Woodbury County reserves the right to audit networks and systems periodically to ensure compliance with this policy.

Security and Proprietary Information

- All mobile and computing devices that connect to the internal network must comply with the principle of least access.
- Providing access to another individual, deliberately or through failure to secure access, is prohibited.
- You must lock the screen or log off when the device is unattended.

- Postings by employees from a County email address should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Woodbury County unless posting is during business duties. Employees should only use Woodbury County accounts for work-related services and platforms.
- Employees must use extreme caution when opening email attachments from unknown senders, which may contain malware.

Unacceptable Use

The following activities are, in general, prohibited. Employees may get an exemption from these restrictions during their legitimate job responsibilities (e.g., systems administration staff may need to disable a host's network access if that host is disrupting production services).

Under no circumstances is an employee of Woodbury County authorized to engage in any illegal activity under local, state, federal, or international law while utilizing Woodbury County-owned resources.

The electronic communications systems may be used for minor, incidental personal uses, as determined by management, that is not intentional misuses. Personal use shall not directly or indirectly interfere with the County's business services, interfere with job performance, directly or indirectly interfere with another user's duties, or burden Woodbury County with more than a negligible cost.

The lists below are by no means exhaustive but attempt to provide a framework for activities that fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations. Violations include, but are not limited to, the installation or distribution of "pirated" or other software products that were not appropriately licensed for use by Woodbury County.
- Unauthorized copying of copyrighted material, including, but not limited to, copyrighted music, and installing any copyrighted software for which Woodbury County or the end user does not have an active license is strictly prohibited.
- Accessing data, a server, or an account for any purpose other than conducting Woodbury County business, even if you have authorized access, is prohibited.
- Exporting software, technical information, encryption software, or technology in violation of international or regional export control laws is illegal. The appropriate management should get consulted before the export of any material that is in question.
- Introducing malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).
- Revealing your account passwords to others or allowing the use of your accounts by others. This includes family and other household members when working from home.

- Using Woodbury County computing asset to actively procure or transmit material that violates sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Employees make fraudulent offers of products, items, or services from any of Woodbury County accounts.
- Making statements about warranty, expressly or implied, unless it is a part of regular job duties.
- Effecting a security breach, including, but not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access unless these duties are within the scope of regular duties. For this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is prohibited unless approved and performed by the Information Security Team.
- Network monitoring is prohibited unless this activity is a part of the WCICC-IT employee's regular job/duty or unless the activity is explicitly approved by the Network Manager.
- Performing any circumvention of user authentication or security of any host, network, or account.
- Introducing honeypots, honeynets, or similar technology on Woodbury County network.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command or sending messages of any kind with the intent to interfere with, or disable, a user's terminal session via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, Woodbury County employees to parties outside Woodbury County.
- Damaging computer equipment intentionally, or unintentionally by using excessive force.

Email and Communication Activities

Users must realize they represent the organization when using organizational resources to access and use the Internet. Employees are responsible for the context of all communications. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the organization."

- Sending unsolicited email messages, including sending "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages.

- Transmission of any improper communication that is pornographic, derogatory, defamatory, or obscene.
- Unauthorized use or forging of email header information.
- Solicitation of email for any other email address other than that of the poster's account, with the intent to harass or to collect replies.
- Work email accounts used for signing up for non-work-related accounts such as online shopping or social media.
- Creating or forwarding "chain letters," "Ponzi," or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within the County's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Woodbury County or connected via the County's network.
- Access to Woodbury County resources, including organizational email, from outside the US will only be granted with prior approval by a direct supervisor.

Social Media

- Posting on social media by employees, whether using the County's property and systems or personal computer systems, is also subject to the terms and restrictions outlined in this Policy.
- Limited and occasional use of the County's systems to engage in posting is acceptable, if it gets done professionally and responsibly, does not otherwise violate the County's policy, is not detrimental to the County's best interests and does not interfere with an employee's regular work duties.
- Posting from the County's systems is subject to monitoring.
- Employees are prohibited from revealing Woodbury County confidential or proprietary information when engaged in social media.
- Employees shall not engage in any posting on social media that may harm or tarnish the image, reputation, or goodwill of Woodbury County or any of its employees. Employees are prohibited from making discriminatory, disparaging, defamatory, or harassing comments when posting.
- Employees may also not attribute personal statements, opinions, or beliefs to Woodbury County when engaged in social media. If an employee is expressing their beliefs or opinions on social media, the employee may not, expressly, or implicitly, represent themselves as an employee or representative of Woodbury County. Employees assume all risks associated with posting on social media.
- Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, the County's trademarks, logos, and any other Woodbury County intellectual property may also not be used in connection with any social media activity.