Corporate Network Security Policy Guidelines

David A. Bush

University of Wisconsin -Stout

CNIT 583 Introduction to Network Security

CONTENTS

OVERVIEW

This policy is for XYZ Company and will be referred to in this document as the company.

This policy applies to the use of information, electronic and computing devices, network resources, and digital content to conduct business or interact with the internal networks and business systems owned or leased by the company, employees, or third parties. Employees, contractors, vendors, consultants, temporary or other workers are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with corporate policies and standards outlined in this document in addition to local laws and regulations.

This policy applies to employees, contractors, vendors, consultants, temporary or other workers including all personnel affiliated with third parties. This policy is applicable to all equipment that is owned or leased by the company. Violation of this policy is enforceable up to and including facility debarment or termination of contracts or employment.

ACCEPTABLE USE POLICY

Proprietary information stored on any electronic device owned or leased by the company or brought onto company premises remains the sole property of the company. It is the user's responsibility to ensure that proprietary information is protected.

It is the responsibility of those that are assigned equipment to report the theft, loss, or misuse of company electronic resources including data, information, or equipment.

Proprietary information can be used and shared only to the extent necessary and authorized to fulfill assigned job duties.

The Information Technology Department will monitor equipment and networks on an ongoing basis and reserves the right to audit network systems on a periodic basis to ensure policy compliance.

The following activities are considered unacceptable use and are a violation of this policy:

1. Accessing company resources (data, information, network equipment) for personal use or use other than the conduction of company business is prohibited.
2. Copying or exporting software or technical information from the company intranet without proper management approval is prohibited.
3. Introduction of malicious programs into the network or server such as viruses, worms, trojan horses or email bombs, or similar threats are prohibited.
4. Using the company network to engage in procuring or transmitting material that violates cooperate sexual harassment or hostile workplace laws is prohibited.
5. Accessing webmail other than company email services through the company network is prohibited.
6. Involvement in security breaches or disruptions of network communications such as accessing data not intended for the recipient or logging into a device with someone else's credentials.
7. Using any program, script, or command with the intent of ending another user's session is prohibited (Purplesec, n.d.).
8. Leaving a workstation unsecured giving some else the opportunity to access your account is prohibited.

USER ACCT. MANAGEMENT

User accounts will be created under the concept of “least privilege”. Employees are granted only the accesses that are required for their job title and role within the company. Outlined below are user responsibilities regarding their user account.

1. All users must lock their screens whenever they leave their desks to reduce the risk of unauthorized access.
2. All users must keep their workplace clear of any sensitive or confidential information when they leave.
3. All users must keep their passwords confidential and not share them (Netwrix, 2021).
4. Passwords should be a minimum of 8 characters and should not contain names, birthdays, phone numbers or other words that are easily guessed. Passphrases are recommended and should be changed every 45 days.
5. Employees with a “user” account will be made an administrator of a company device.

EMAIL POLICY

This section outlines the appropriate use of email for the company and applies to all employees and agents operating on behalf of the company.

1. All use of email must be consistent with corporate policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
2. email account should be used primarily for business-related purposes; personal communication is permitted on a limited basis, but non-company-related commercial uses are prohibited.

3. Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail, etc. to conduct any company business. Such communications and transactions should be conducted through proper channels using the company-approved email client.
4. Employees shall have no expectation of privacy in any email sent, received or stored using the company's email system.
5. The company IT department may monitor messages without prior notice (Sans, 2021).
6. Employees should not click on any link acquired through email from outside the company network without being confident as to who sent it and what they are trying to access.

NETWORK ACCESS POLICY

This section outlines the standards to be adhered to by anyone accessing the local area network (LAN) or company network as it will be referred to in this section. These standards apply for both physical and remote access (Selby, 2013).

Outlined below are the minimum requirements for accessing the company network. Remote access, while touched on here, is covered more specifically in the following section.

1. All employees and contractors shall be given network access in accordance with the least-privilege principle.
2. All staff and contractors who have remote access to company networks shall be authenticated using the VPN authentication provided by the company's IT department.
3. Segregation of networks shall be implemented as recommended by the company's IT department with regards to network security and infrastructure best practices.

4. Network routing controls shall be implemented to support the access control policy (Netwrix, 2021).

REMOTE ACCESS

Accessing the network remotely requires a company-approved VPN supplied through the company's IT department and if personal computers are used to connect to the company's network, they must have corporate-approved anti-virus software installed also (Sans, 2021).

Third-party connections to the company network are prohibited unless they are sponsored by a knowledgeable employee of the company who will be in direct contact and able to watch the third-party activities. Furthermore, a third-party connection must be through a company-approved VPN service such as Cisco WebEx or another pre-approved vendor.

INTERNET ACCESS

General access to the internet for uses other than business is strictly limited to employees. Employees should use good judgment understanding that time should be limited. Live data streaming and other high bandwidth use activities are prohibited on company networks unless specifically authorized through the Information Technology department or management.

The Information Technology Department shall monitor Internet use from all computers and devices connected to the corporate network and will record the User ID of the person or account initiating the traffic (Sans, 2021).

Sites not allowed by corporate policy should be blocked by the use of a proxy server. If a legitimate site is blocked, users can contact corporate IT to have it reviewed for consideration to remove restrictions. Examples of blocked content will include but is not limited to the following types of content: adult explicit material, pop-ups and advertisements, chat and IM, gambling,

hacking, illegal drugs, P2P file sharing, dating, violence, intolerance and hate, and web-based email (Sans, 2021).

SERVER AND DESKTOP SECURITY

Only servers approved by the Information Technology department may be connected to the company network. These servers must be hardened and inspected in accordance with the IT department's best practices and installed in one of the approved data centers where they can be physically secured (City of Madison, 2015).

Only workstation devices that have a company-approved operating system image setup by the IT department are allowed to connect to the business network. Vendors, contractors, and visitors must connect through wi-fi via guest wireless.

Workstations will be supplied through the IT department only with all updates and security patches being initiated by the company's IT department.

SOFTWARE LICENSING

All software downloaded on company computers must be legally licensed, compliant with the configuration required for the device, and be approved through the IT department (City of Madison, 2015).

Preapproved software available for download can be found in the company's software center.

MOBILE DEVICES

Portable computing devices such as smartphones, laptops, and tablets must be configured and managed by the corporate IT department if they are to be connected to the corporate network. These type of mobile devices with the exception of laptops must also meet two-factor

authentication requirements. Laptops meet the workstation requirements provided at login. Personal smartphones and tablets can access company wi-fi through a guest account (City of Madison, 2015).

GUEST ACCESS

Visitors may gain access through the guest wi-fi network only. Devices other than company managed devices are not authorized to connect to the company network. Attempts to connect either wirelessly or through a wired connection are strictly prohibited and can result in legal action or expulsion from the premises. Guest accounts can be set up simply by clicking the guest network and filing out the form that follows.

MALWARE PROTECTION

Malware protection such as endpoint virus protection and software firewalls will be provided, downloaded, installed, and set up by corporate IT on all workstations prior to use. Mobile devices that are managed by the IT department will also have malware protection installed on them when they are setup.

CHANGE MANAGEMENT

Technology change requests are to be first reviewed by the department head of the requester and submitted to corporate IT for review and approval by the appropriate division (i.e., IT Security, Infrastructure Support, Application Development, etc.) before any changes can be made.

REFERENCES

City of Madison. (2015, September). *Network Security Policies and Procedures*. Retrieved from EmployeeNet: https://www.cityofmadison.com/mayor/apm/it/APM3-9AttachB.pdf

Netwrix. (2021). *Data Security and Protection Policy Template*. Retrieved from Netwrix: https://www.netwrix.com/data_security_policy_template.html

Purplesec. (n.d.). *50 Free Information & Cyber Security Policy Templates To Secure Your Network*. Retrieved from Purplesec: https://purplesec.us/resources/cyber-security-policy-templates/

Sans. (2021). *Security Policy Templates*. Retrieved from Sans: https://www.sans.org/information-security-policy/?category=general

Selby, N. (2013, August 25). *A sample network access policy*. Retrieved from Information Security & Law Enforcement Technology: http://www.nickselby.com/2013/08/25/a-sample-network-access-policy/