NORTHWEST MISSOURI STATE UNIVERSITY POLICY

Policy Name:	Information Security
Effective Date:	October 21, 2022
Last Revision Date:	October 20, 2022
Last Review Date:	October 20, 2022
Approving Authority:	Board of Regents
Responsible Office:	Information Technology
Category:	Information Technology

Purpose

This Policy Document encompasses all aspects of security surrounding Northwest Missouri State University owned equipment and Northwest Missouri State University confidential information and applies to all Northwest Staff, Faculty, and Students. This document will be reviewed and updated as appropriate.

Acceptable Use Policy

The Information Technology's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Northwest's established culture of openness, trust, and integrity. We are committed to protecting the Staff, Faculty, and Students from illegal or damaging actions by individuals, either knowingly or unknowingly.

- Northwest reserves the right to monitor, access, review, audit, copy, store, or delete University-owned technology resources, and network traffic/electronic communications for any purpose;
    - Actively monitoring a single individual or group of individuals by IT staff (beyond the normal performance of duties related to their employment) without an official directive from a member of the Northwest Leadership Team in consultation with the AVP of Information Technology, or law enforcement, is prohibited and actionable.
- Staff, Faculty, and Students are responsible for exercising good judgment regarding the reasonableness of personal use.
- Staff, Faculty, and Students should ensure that they have appropriate credentials and are authenticated for the use of technologies.
- Staff, Faculty, and Students should take all necessary steps to prevent unauthorized access to confidential data.
- Staff, Faculty, and Students should ensure that technologies should be used and setup in acceptable network locations.
- Keep passwords secure and do not share accounts.
- Do not use e-mail, internet, and other Northwest resources to engage in any action that is threatening, discriminatory, defamatory, slanderous, obscene, harassing, or illegal.

- Do not disclose sensitive information unless authorized.
- Authorized users are responsible for the security of their passwords and accounts.
- All PCs, laptops, and workstations should automatically lock when not in use.
- All devices should be appropriately protected and secured so they cannot be tampered or altered.
- Staff, Faculty, and Students must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

Access to Sensitive Data

All access to sensitive data is controlled. Any job functions that require access to sensitive data are subject to the following:

- Access rights to privileged user IDs is restricted to least privileges necessary to perform job responsibilities.
- Privileges are assigned to individuals based on job classification and function.
- The data governance committee provides oversight of the availability, usability, integrity, and security of enterprise data.

Protect Stored Data

All sensitive data stored and handled by Northwest and its employees must be securely protected against unauthorized use at all times. Any sensitive data that is no longer required for business reasons must be discarded in a secure and irrecoverable manner.

Physical Information Technology Security

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorized individuals from obtaining sensitive data.

- An inventory of devices must be maintained.
- Devices are periodically inspected to detect tampering or substitution.
- Authorized users are responsible for the security of their passwords and accounts.
- Media containing sensitive information must be handled and distributed in a secure manner by trusted individuals.
    - Media is defined as any printed or handwritten paper, received faxes, floppy disks, back-up tapes, computer hard drives, USB drives, etc.
- Visitors must always be escorted by a trusted employee when in areas that hold sensitive information.
    - A “visitor” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
- Network Jacks located in public and areas accessible to visitors must be disabled and only enabled when network access is explicitly authorized.

Protect Data in Transit

All sensitive data must be protected securely if it is to be transported physically or electronically.

- Sensitive data (SSN, Credit Card #, etc.) should not be sent over the internet via email, instant chat, or any other end user technologies without a business justification.
- If there is a business justification to send sensitive data via email or via the internet or any other modes, then it should be done by using a strong encryption mechanism

Disposal of Stored Data

- Data must be retained in accordance with applicable State retention standards.
- All data must be securely disposed of when no longer required by Northwest, regardless of the media or application type on which it is stored.
- All hardcopy materials containing sensitive data must be shredded, so they cannot be reconstructed when disposed.
- All sensitive data on electronic media must be rendered unrecoverable when deleted e.g., through degaussing or electronically wiped using military grade secure deletion processes or the physical destruction of the media.

Network Security

- Firewalls are implemented at each internet connection, and the internal company network.
- A firewall and router configuration document must be maintained which includes a documented list of services, protocols, and ports.
- Firewall and router configurations restrict connections between untrusted networks and any systems in University network.
- The firewall rules must be reviewed on a periodic basis to ensure validity.

Security Awareness and Procedures

The protection of sensitive data demands regular training of all employees and contractors.

- Handling procedures for sensitive information are periodically reviewed.
- Annual Cyber Security training is required for employees
- All employees that handle sensitive information undergo background checks (such as criminal and credit record checks, within the limits of the local law) before they commence their employment with Northwest.
- Northwest security policies are reviewed and updated as needed.

System and Password Policy

The purpose of this Policy is to inform members of the Northwest Missouri State University community how to create and maintain a secure password.

- Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Northwest's computer network.

- This policy establishes a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.
- Passwords must be created and managed in accordance with this section.

Password Requirements

- All user-level Northwest network passwords will expire annually and must be changed.
- New passwords cannot be the same as the previous passwords.
- Passwords must be at least fourteen characters in length. Longer is better.
- Accounts shall be locked after 10 failed login attempts within 15 minutes and shall remain locked for at least 15 minutes or until the System Administrator unlocks the account.
- Passwords should not be shared with anyone.
    - All passwords are to be treated as sensitive, confidential information. If someone requests your password(s), please inform them that you cannot provide that information per Northwest policy and contact the Information Technology Help Desk. If you suspect an account or password has been compromised, report the incident immediately and change all related passwords.
- The Information Technology Department or authorized outside "penetration testers" may perform password cracking or guessing on a periodic or random basis to test the security of the Northwest network. If a password is guessed or cracked during one of these scans, the user will be required to change it. Password cracking and guessing are not to be performed by anyone outside of the Technology Department or an approved third-party auditor.
- Passwords should never be written down or stored online. Employees should try to create pass phrase made up of 4 or more smaller words that can be easily remembered. The password must be 14 or more-character phrases (with or without spaces for readability). One way to do this is to create a pass phrase based on a song title, affirmation, or other phrase.

Anti-Virus Policy

- All machines are configured to run the latest anti-virus software as approved by Northwest.
- Systems are configured to retrieve the latest updates to the antiviral program automatically on a daily basis. Periodic scanning is enabled for all the systems.
- All removable media (for example USB drives and others) should be scanned for viruses before being used.
- Master Installations of the Antivirus software are set up for automatic updates and periodic scans.
- End users must not modify any settings or alter the antivirus software.
- E-mail with attachments coming from suspicious or unknown sources should not be opened. All such e-mails and their attachments should be reported to the Help Desk and deleted from the mail system as well as from the trash bin. No one should forward any e-mail, which they suspect may contain virus.

Patch Management Policy

- All Workstations, servers, software, system components, etc. owned by Northwest must have up-to-date system security patches installed to protect the asset from known vulnerabilities.
- Wherever possible, all systems and software must have automatic updates enabled for system patches released from their respective vendors.
- Security patches must be installed ASAP.
- Any exceptions to this process must be documented.

Remote Access Policy

- Secure remote access must be strictly controlled.
- Control will be enforced by multi factor authentication.
- Vendor accounts with access to the Northwest network will only be enabled during the time period the access is required and must be disabled or removed once access is no longer required.
- Remote access connection must be setup to be disconnected automatically after inactivity.
- All hosts that are connected to Northwest networks via remote access technologies must be monitored on a regular basis.
- All remote access accounts used by vendors or 3rd parties must be reconciled periodically, and the accounts will be revoked if there is no further business justification.
- Virtual Private Network (VPN) access may be required for employees or contractors that administer systems remotely.
    - VPN is not required for internet enabled applications such as Northwest Email, myNorthwest, Northwest Online, CatPAWS, Microsoft Office, etc.
    - Northwest employees can request remote access (VPN) by completing the VPN Access Request form in myNorthwest.

Incident Response Plan

Northwest security incident response plan is as follows:

1. Affected user must report a security incident to the Help Desk.
2. The Help Desk will report the security incident to a member of the Information Technology Leadership Team.
3. The member of the team receiving the report will notify other members of the Team, in addition notifying the CMT Leader as appropriate.
4. The Team will investigate the incident and assist the potentially compromised department/user in limiting the exposure of data and in mitigating the risks associated with the incident.
5. The Team will resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties.

6. The Team will determine if policies and processes need to be updated to avoid a similar incident in the future, and whether additional safeguards are required in the environment where the incident occurred, or for the institution.

User Access Management

- Access to Northwest systems is controlled through a formal user registration process beginning with a formal notification from HR.
- Each user is identified by a unique user ID so that users can be linked to and made responsible for their actions. The use of group IDs is only permitted where they are suitable for the work carried out.
- There is a standard level of access; other services can be accessed when specifically authorized by HR/line management.
- The job function of the user decides the level of access the employee has to sensitive data.
- Access to all Northwest systems is provided by appropriate administrators and can only be started after proper procedures are completed.
- Network Accounts will be disabled after leaving Northwest:
    - Students: One year following their last date of attendance from Northwest due to graduation, withdrawal, or other personal, professional, or academic issues.
    - Faculty and Staff: Immediately disabled after last shift or after 5 p.m. on the last full day of scheduled work.
    - The exceptions to the above rules are for students who are expelled for disciplinary reasons and faculty/staff whose employment was terminated due to disciplinary reasons and/or their accounts pose a network security risk.

Access Control Policy

- Access Control systems are in place to protect the interests of all users of Northwest computer systems by providing a safe, secure, and readily accessible environment in which to work.
- Northwest will provide all employees and other users with the access they need to carry out their responsibilities in as effective and efficient manner as possible.
- Generic or group IDs shall not normally be permitted but may be granted under exceptional circumstances.
- The allocation of privilege rights (e.g., local administrator, domain administrator, super-user, root access) shall be restricted and controlled, and authorization provided jointly by the system owner and IT Services. Technical teams shall guard against issuing privilege rights to entire teams to prevent loss of confidentiality.
- Access rights will be accorded following the principles of least privilege and need to know.
- Every user should attempt to maintain the security of data, even if technical security mechanisms fail or are absent.

- Users are obligated to report instances of non-compliance to the Help Desk.
- Access to Northwest IT resources and services will be given through the provision of a unique Active Directory account and complex password.
- No access to any Northwest IT resources and services will be provided without prior authentication and authorization of a user's Active Directory account.
- Password length, complexity, and expiration times are controlled through Windows Active Directory Group Policy Objects.
- Access to Confidential, Restricted, and Protected information will be limited to authorized persons whose job responsibilities require it, as determined by the data owner or their designated representative. Requests for access permission to be granted, changed, or revoked must be made in writing and submitted to the Data Governance Committee.
- Access control methods include logon access rights, Windows share and NTFS permissions, user account privileges, server and workstation access rights, firewall permissions, IIS intranet/extranet authentication rights, SQL database rights, isolated networks, and other methods as necessary.

Wireless Policy

- Installation or use of any unauthorized wireless device or wireless network intended to be used to connect to any of the Northwest networks or environments is prohibited.
- Authorized wireless networks must implement industry best practices and strong encryption for authentication and transmission of data.
- An Inventory of authorized access points along with a business justification must be maintained.
- Guest Wireless networks will require users to authenticate.

Disciplinary Action

Violation of the standards, policies, and procedures presented in this document by Staff, Faculty, or Students are subject to disciplinary proceedings including monetary fines, suspension or loss of system privileges, expulsion from the University, termination of employment and/or legal action as may be deemed appropriate.