Policy title	Category
Graham-Leach-Bliley Act Information (Data) Security Program	Information Technology
Owner	**Approved by**
CSIT	Ad Council

Purpose of this policy

Nebraska Wesleyan University (NWU) recognizes the importance of and is committed to creating effective administrative, technical, and physical safeguards to protect faculty, staff and student information from unauthorized access. NWU is an academic community dedicated to intellectual and personal growth within the context of a liberal arts education and in an environment of Christian concern. In the normal course of pursuing this mission, NWU receives some sensitive information from our faculty, staff and students which may include financial, educational or medical information.

In compliance with federal and state laws, NWU has developed this information (data) security program ("ISP") which outlines the University's policy and procedures for evaluating and addressing the electronic and physical methods for accessing, collecting, storing, using, transmitting and protecting faculty, staff and student information.

Policy statement

The Chief Information Officer is designated as the person who shall be responsible for overseeing and updating the ISP as needed (ISP Representative). The ISP Representative reports directly to the NWU Vice President for Finance and Administration. The ISP Representative may assign or delegate other NWU representatives to oversee and coordinate elements of the ISP. Any questions regarding the implementation of the ISP or with interpreting this document should be directed to the ISP Representative or their designees.

The ISP Representative will verify compliance with this policy through various methods, including but not limited to, periodic walkthrough, monitoring, business tool reports, and internal and external audits. The ISP Representative will report all findings, regulatory and state security laws changes, and any other information technology security related matters directly to the NWU Vice President for Finance and Administration.

Compliance with this policy is mandatory for all University employees and any independent contractors. Employees should notify their immediate supervisor of any member of management upon learning of violations of this policy. The supervisor or member of management will be responsible for notifying the University's ISP representative. Violations for this policy (including knowingly failing to notify a supervisor or member of management of a violation) will be subject to disciplinary action, up to and including termination of employment.

Information Security Program Components

Risk Identification and Assessment

NWU has undertaken, as part of the ISP, to identify and assess potential internal and external risks to the security, confidentiality and integrity of information held or managed by NWU that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromises of such information.

The risk assessment and safeguard control policies described here shall apply to all methods of handling or disposing of client information, whether in electronic, paper or other form. The ISP Representative will, on a regular basis, implement safeguards to control the risks identified through such assessments and regularly test or otherwise monitor the effectiveness of such safeguards in relevant areas of the University's operations, including:

- Information systems: The ISP representative will assess the risks to institutional information associated with the University's information systems, including network and software design, information processing and the storage, transmission and disposal of financial information. The ISP Representative will coordinate with relevant departments, as appropriate, to assess the following procedures:
- Detecting and managing system failures: The ISP Representative will evaluate procedures and methods of deferring, detecting, preventing and responding to attacks or other system failures and existing network access and security policies and procedures, as well as procedures for coordinating responses to network attacks and developing incident response teams and policies.
- The ISP Representative may elect to delegate the responsibility for monitoring and participating in the dissemination of information related to the reporting of known security attacks and other threats to the integrity of networks utilized by the University, and will coordinate with relevant departments, as appropriate.
- Employee management and training: The ISP Representative will evaluate the effectiveness of the University's procedures and practices relating to access and use of client information. This evaluation will include assessing the effectiveness of the University's current policies and procedures in coordination with relevant departments, as appropriate, as well as adequate training of employees.

The NWU ISP Representative will implementation methods to identify potential risks to the security, confidentiality and integrity of NWU information and monitor the effectiveness of safeguards implemented to mitigate those risks. These methods may include (but are not limited to):

- The annual performance of external penetration testing against the University's Internet accessible systems and services, conducted by an outside agent with appropriate cyber security expertise.
- The annual performance of a network vulnerability test against the University's information systems and services, conducted by an outside agent with appropriate cyber security expertise.
- The annual audit of NWU user accounts conducted by internal information services staff in coordination with the NWU Human Resources and NWU Registrar's Office.
- Annual cyber security training for all NWU employees, including periodic cyber security threat vulnerability testing for designated employee groups.

Safeguards for the Protection of Institutional Information

NWU has identified critical areas of internal and external risk to the security, confidentiality and integrity of institutional information and which could result in the unauthorized access, disclosure, misuse, alteration, destruction or some other way compromise such information. The University has implemented safeguards for controlling risks associated with these risks related to the handling, collecting, storing, using, transmitting and protecting information.

- User Account Management
    - All computer users at NWU are provided with their own, unique account and password for access to NWU systems and services.
    - Computer users are expressly prohibited from sharing account credentials with others.
    - User accounts are audited regularly by NWU CSIT in cooperation with account authorities in NWU Registrar's Office and NWU Human Resources.
    - NWU adopts role-based access to critical administrative systems, assuring that the least possible access is granted to institutional data.
    - NWU requires all computer accounts to use complex passwords:
        - 12 -14 characters
        - At least three of four character types: upper case letter, lower case letter, number and symbol
        - No more than two consecutive identical characters
        - No part the account username, first name of last name.
    - NWU requires all account holders to change passwords not more than every 120 days.
    - NWU monitors and restricts the use of password management tools for designated user accounts with access to sensitive information.
- Network Access Restrictions
    - NWU implements a "least necessary access" policy for management of the campus firewall, opening only those ports on specific systems which are necessary for services to function.

    - All NWU systems and services providing access the sensitive Institutional data are protected from direct Internet exposure and by routing rules which limit network access internally.
    - All external access to systems and services providing access to sensitive Institutional data must be routed through the NWU Virtual Private Network (VPN) and required multifactor authentication (MFA).

- Physical Security for Systems, Network Infrastructure
    - Access restrictions
        - All NWU critical systems are protected by two-factor security access and camera surveillance.
        - All critical network components (wiring, network edge switches, firewall and core router) are protected in locked locations and under camera surveillance.
    - Redundancy
        - Critical network services (DNS, DHCP) are provisioned with redundant serves behind network applicant load balancers.
        - Critical core network appliances are provisioned with redundant power supplies.
        - The NWU server room is protected against electrical outage by and emergency generator, supported by rack-mounted UPS devices.
        - All critical servers, storage nodes and network components are protected by hardware and software support agreements.

- Multifactor Authentication
    - All access to protected NWU systems and services from non-NWU networks is routed through the NWU Virtual Private Network and requires multifactor authentication (MFA).
    - MFA is required for selected NWU users accounts, including user accounts with elevated privilege (e.g. domain administrators) and accounts with demonstrated vulnerability to malicious actors.

- Data Loss Prevention
    - All centrally managed, critical NWU servers, central data storage are regularly backed up. Backup data is stored both locally (temporarily) and off-site.
    - Backup data is stored and transmitted encrypted.
    - Backup data is periodically tested to assure integrity of the backup process.
    - NWU has established a cold standby site in the event it becomes necessary to restore critical systems.

- Other information protection safeguards:
    - All NWU computer provisioned for use by faculty and staff include protection against malicious software by cloud-based anti-virus and anti-malware software.
    - All NWU computers provisioned for use by faculty and staff are protected under extended warrantee agreements.
    - NWU has developed policies for the protection and retirement of institutional hardware and data, including
        - Data retention policies
        - Hardware lifecycle management policies
    - Policies have been developed for protecting the accessibility and integrity of central information systems and services, including
        - Change Management Policy
        - Patch Management Policy
        - Core Network Management Policy
        - Security Incident Response Policy
        - Email Privacy Policy
        - Acceptable Use of Computing Resources Policy
    - NWU provides all employees with cyber security awareness training and has implemented regular cyber security threat vulnerability testing.
    - NWU maintains institutional cyber security insurance.

Third-party Service Providers

The ISP Representative shall coordinate with those responsible for the third-party service procurement activities within NWU CSIT and other affected departments to raise awareness of, and to institute methods for, selecting and retaining only those service providers that are capable of maintaining appropriate safeguards for institutional information to which they will have access. In addition, the ISP Representative will work with the NWU Controller or other designate official to develop and incorporate standard, contractual protections applicable to third-party service providers, which will require such providers to implement and maintain appropriate safeguards. Any deviation from these standard provisions will require the approval of the NWU Controller or designate official.

Review, Evaluation and Update

The ISP Representative will be responsible for reviewing the ISP at least annually and reporting the results of that review to the Vice President for Finance and Administration. The ISP Representative will evaluate the program based on the risk identification and assessment activities undertaken under the terms of the program, as well as any material changes to the University's operations or other factors that may have an impact upon the program. The ISP Representative will propose adjustments to the program based on this review.

Last revised date December 15, 2023