POLICY

SECURING INFORMATION SYSTEMS

This policy applies to all employees using WWU data networks and information systems. Upon consultation with WWU’s Office of the Chief Information Officer, academic or research networks or information systems that are not interconnected with covered WWU networks or information systems may be considered for exemption from this policy.

Purpose
The purpose of the Western Washington University (WWU) Information Security Policy (“Policy”) is to protect WWU’s computing resources and data through the creation of an Information Security Program that supports the University’s mission of being a public comprehensive institution dedicated to serving the people of the State of Washington. The WWU Information Security Program will also support the realization of the goals set forth in the University’s strategic plan, and particularly the academic, business, housing, health and safety systems services goals, by providing the necessary controls for safe and secure information technology-related activities. Compliance with the WWU Information Security Program will also reduce the risk of violating state and federal laws and the potential associated risks of negative impacts on the University’s reputation, litigation, fines, and substantial revenue losses.

Definitions:

Electronic Protected Health Information (ePHI): Electronically stored Protected Health Information.
**Individually Identifiable Health Information:** Information that is a subset of health information, including demographic information collected from an individual, and is 1) Created or received by a health care provider, health plan, employer, or health care clearinghouse; and 2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and 3) Either identifies the individual or, with respect to which there is a reasonable basis, provides enough information to identify the individual (45 CFR § 160.103).

**Personal Information:** Information about an individual as defined in RCW 19.255.005. A partial list of common Personal Information includes an individual's first name or first initial and last name in combination with social security number, license or state ID number, date of birth, private (encryption) key, student, military, or passport identification number, health insurance policy number or health insurance identification number, medical history or mental or physical condition, medical diagnosis or treatment, biometric data (fingerprints, voice, etc.), and username or email in combination with password.

**Personally Identifiable Information (PII):** Personal Information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

**Protected Data:** Data that falls into one of three data classifications. “Sensitive Information” may not be specifically protected from disclosure by law, but is for official use only. “Confidential Information” is information that is specifically protected from disclosure by Washington State law. It may include but is not limited to personal information about individuals, information concerning employee personnel records, or information regarding IT infrastructure and security of computer and telecommunications systems. “Confidential Information Requiring Special Handling” is information that is specifically protected from disclosure by law and for which especially strict handling requirements are dictated, such as by statutes, regulations, or agreements, or that serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions (OCIO 141.10, 4.1).

**Protected Health Information (PHI):** Individually Identifiable Health Information that is transmitted or maintained by electronic or any other form of media. It may exclude 1) Individually Identifiable Health Information found in Family Educational Rights and Privacy Act (FERPA) education records (20 U.S.C. 1232g, 20 U.S.C. 1232g(a)(4)(B)(iv)); and 2) Employment records held by a HIPAA covered entity in its role as employer; and 3) Records for a person who has been deceased for more than 50 years (45 CFR § 160.103).

**Supervisor:** Employees who have authority, in the interest of the employer, to perform all or some of the duties to hire, transfer, suspend, lay off, recall, promote, discharge, direct, reward, or discipline employees, or to adjust employee grievances, or effectively to recommend such action, if the exercise of the authority is not of a merely routine nature but requires the consistent exercise of individual judgment (RCW 41.80.005).
1. **WWU is Committed to Protecting University Computing Resources and Data**

WWU is committed to complying with state and federal laws regarding information systems. The WWU Information Security Program will reduce the risk of compromises to the computing resources and data held by the University. Compromises to the computing resources and data held by the University could result in an interruption of academic, business, housing, health and safety services.

2. **WWU Establishes and Maintains an Information Security Program**

WWU will establish an information security program ("Program"). The Program will promote, through policy, standards, and guidelines, a secure environment for protecting the integrity, confidentiality and availability of University data and for safeguarding University computing resources. The Program will have goals similar to those produced by applying the Washington State Office of the Chief Information Officer (OCIO) Standard 141.10, Securing Information Technology Assets. These goals include:

   A. Appropriate levels of security and integrity for data exchanges and business transactions.
   B. Effective authentication processes, security architectures(s), and trust fabric(s).
   C. Staff security awareness trainings.
   D. Staff support for interpreting and implementing security policy and standards.
   E. Compliance, testing and audit provisions.
   F. Standardization on the National Institute of Standards and Technology (NIST) Cybersecurity Framework.


Under the authority of WWU’s Chief Information Officer (CIO), the Director of Information Security is charged with developing and implementing an information security strategy to execute this policy in accordance with WWU’s legal and contractual obligations, institutional values, and overarching strategic direction. Information security covers the protection of University data in any form, and the safeguarding of IT resources. The protection of data (both physical and electronic) includes:

   A. Safeguarding the confidentiality of Protected Data recorded on any type of media (paper, magnetic, electronic, whiteboards, etc.).
   B. Protecting the integrity of data (preventing malicious or unintentional alteration).
C. Ensuring the availability of data (i.e., systems are up when expected and data is always accessible).

D. Protecting the infrastructure that houses and processes our data.

E. Enforcing the same high security standards for data handled, housed and processed by contractors, vendors, and cloud services providers.

4. All Individuals Using University Systems are Responsible for Information Security.
   All university employees (including student employees), interns, and other users who have access to University information systems, equipment, or infrastructure shall comply with information systems standards established by the WWU Information Security Program. Failure to comply with information systems standards could result in disciplinary action.

   University contracts with contractors, vendors, and cloud providers must include language that contains security provisions consistent with this policy and any related standards established by the WWU Information Security Program.

6. Supervisors Are Responsible for Enforcement of Policies within Division
   Supervisors will enforce University information security policies by applying appropriate corrective actions against employees and other system users (interns, volunteers, contractors, vendors, etc.) who fail to comply with those policies. The corrective actions should be appropriate for the type and frequency of the offense up to and including termination. Supervisors are responsible for reporting malicious behavior and potential criminal activity to Human Resources, who may decide to involve the Chief Information Officer, the Information Security Office (ISO), and/or law enforcement.

7. Departments and Units Responsible for Administration of University Information Security
   The University relies on a combination of responsibilities spread among the ISO, IT employees (both under and independent from Information Technology Services), Supervisors, and end-users. Functions for centralized administration of University information security includes the following elements:

   A. The CIO is tasked with appointing a Director of Information Security to administer the University’s Information Security Program. The Director also manages the ISO.

   B. The Director of Information Security is responsible for:
      1) Developing and maintaining the administrative policies related to the security of the University’s information and IT resources.
      2) Maintaining the Information Security Policy (this document) and related Information Security Standards and Guidelines.
      3) Coordinating and administering federal, state, PCI-DSS, University and other information security audits.
4) Developing and maintaining guidelines for Disaster Recovery Plans and testing procedures throughout the University.

5) Providing ongoing security procedural and awareness training throughout the University.

6) Preparing and disseminating state and federal reports as required by statute.

7) Participating in the WWU IT Advisory Council (ITAC). This group provides the Chief Information Officer with timely input on IT planning, policies, and project portfolio.

8) Reviewing and approving proposed exceptions to this policy.

C. **The ISO is responsible for:**

1) Performing risk assessments for mission critical systems and those containing Personally Identifiable Information (PII), Protected Health Information (PHI), and other data specifically subject to state and federal laws.

2) Performing security assessments and disseminating the information to responsible parties for remediation.

3) Ensuring a comprehensive inventory of University computing and data assets is maintained.

4) Using security tools to monitor the University’s environment, reporting on findings, and offering strategies for remediation.

5) Performing security design reviews.

6) Providing consultative and advisory services to managers and users throughout the University on matters pertaining to information and IT resource security, risk analysis and disaster recovery.

7) Collaborating in University business continuity planning.

8) Providing oversight of Incident Management.

9) Reporting key metrics to senior management.

10) Reviewing the Securing Information Systems Policy (this document) and related standards annually.

11) Developing and presenting Information Security Awareness training.

12) Supporting departments and business units with compliance with this policy.

D. **The WWU Information Technology Services (ITS) division and non-ITS computing offices and personnel** are responsible for key security systems and practices including and not limited to:

1) Providing an inventory of assets including systems, databases, and applications to the ISO.

2) Implementing proper physical and environmental controls for the data centers, data
POLICY

closets, plant, and workstations.

3) Network security including network segmentation, access control lists, and secure transport.

4) Access control and systems for authentication, authorization and accounting including multifactor authentication.

5) Permissions auditing for systems containing Personally Identifiable Information (PII) or any data specifically regulated by a state or federal regulation such as Protected Health Information (PHI).

6) Configuration management for virtual infrastructure (hosts and servers), physical servers, network equipment, other network-connected devices (HVAC, locks, i.e.), databases, and applications.

7) Complying with university security standards on the application of patches to systems and devices.

8) Enforcing mobile device management for devices handling sensitive or confidential information.

9) Securely managing cloud deployments.

10) Auditing of activity on systems with PII or any state or federally regulated data.

11) Encryption of data when mandated by state or federal regulations.

12) Monitoring of network, system, database, and application logs.

13) Secure Development Lifecycle processes including system acquisition, design, development, and maintenance.

14) Complying with standards for change and release management.

15) Backing up mission-critical and enterprise systems, systems of record containing personally identifiable information (PII), and systems required by state or federal laws and creating Disaster Recovery Plans (DRPs) for those systems.

16) Anti-malware deployment, administration and monitoring.

17) Providing secure electronic messaging, telecom, and other communication systems.

18) Responding to vulnerability scans, security assessments and audits, and remediating deficiencies especially for systems containing, transmitting, or accessing PII or any Category 3 or 4 data as defined in OCIO 141.10.

19) Collaborating in the detection, investigation, and reporting of IT-related security incidents with the WWU ISO.

20) Safeguarding information requiring special handling as per state and federal regulations and laws.

21) Assuring vendors implement security measures consistent with this policy and the
WWU Information Security Program.

**E. Supervisors** are tasked with:

1) Tracking, classifying and protecting their data.
2) Understanding how to grant appropriate access to the systems they use for their business operations.
3) Collaborating with Human Resources on personnel onboarding and departure and for changes in an employee’s duties.
4) Ensuring their employees receive security training.
5) Fostering awareness of information security risks and best practices.
6) Cooperating with other WWU IT employees and the ISO to enhance the University’s security posture.
7) Verifying any information security incidents have been reported to the Help Desk and ISO.
8) Reporting known data breaches to the appropriate privacy officer.

**F. All employees, student employees, faculty, and contractors** are responsible for:

1) Complying with University communications about information security and following best practices.
2) Reporting any suspected information security incident or data breach to their Supervisor and their Help Desk.

**8. Exceptions to this Policy Must Be Received in Writing**

Situations may occur where implementing the policy or a related Standard conflicts with business needs. An exception to policy may be requested in writing. This request must detail the business need for the exception, the technical steps to be taken to address any security concerns, and the process and timeframe for implementation. All requests will be addressed to the WWU Director of Information Security for approval.