Information Security Controls

University Operations – Information Security

CWU Policy 204-06

Effective: February 3, 2021

Policy Review Date: YEAR

Policy Executive: Chief of Staff

Responsible Office/Unit: Information Services and Security

Policy Statement:

Applicability:

Content:

Policy

---

(1) Policy

A. Central Washington University (university) shall implement and maintain procedural, physical, technical, and regulatory safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of institutional information that it creates, receives, maintains, or transmits.

B. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27001:2013 information security standard , along with the National Institute of Standards and Technology (NIST) frameworks, will be used as a guideline of best practice, and all implemented security controls will be commensurate with asset value, aligned with the appropriate compliance requirements, and as determined by an internal risk assessment process.

C. In accordance with ISO/IEC 27001:2013 and NIST, the following information security control domains are therefore implemented:

1. Information Security Policies
2. Organization of Information Security
3. Human Resource Security
4. Asset Management

5. Access Control
6. Cryptography
7. Physical and Environmental Security
8. Operations Security
9. Communications Security
10. System acquisition, Development and Maintenance
11. Supplier Relationships
12. Information Security Incident Management
13. Business Continuity Management
14. Compliance

D. The specific information security controls associated with each security domain listed above, are detailed in the information security procedure that accompanies this policy.

(2) Scope

A. This policy is applicable to all information systems, networks, staff, faculty, students, student employees, and outside contractors that are affiliated or conduct work on behalf of the university. The policy also applies to any information that is created, used, and disseminated on behalf of the University in accordance with CWU 204-04 Data Classification and Usage Policy.

(3) Responsibilities

A. The Chief Information Security Officer is overall responsible for the development and enforcement of the enterprise-wide information security program. It is understood that certain security controls, as appropriate, will be implemented by other functional areas in compliance with this policy.

(4) Risk Assessment

A. Resources employed in implementing security controls need to be balanced against the institutional harm likely to result from security issues in the absence of those controls. The results of a risk assessment will help guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks.

B. It is understood that follow-on risk assessments may identify changes in the university's risk appetite, thereby driving a change in the implemented security controls to ensure the identified risks are appropriately mitigated.

(5) Internal Audit

A. The Security Services department shall plan, establish, implement and maintain an audit program, including the frequency, methods, planning requirements, and reporting associated with the program.

(6) Policy Maintenance

A. The Chief Information Security Officer shall review and recommend changes to this policy statement at least annually or more frequently as needed to respond to changes within the institution and the regulatory environment.

(7) Implementation

A. Failure by an individual to comply with the university policies on information security and privacy may result in disciplinary action up to and including termination for university employees, contract termination in the case of contractors or consultants, dismissal for interns and volunteers, or suspension or expulsion in the case of a student.

B. The university reserves the right to pursue appropriate legal actions to recover any financial losses suffered as the result of a violation of the university policies on information security and privacy.

(8) Additional Information

A. For additional resources, further information on this policy statement, or for a definition of any term used in this policy document, please see the Security Services website.

History:

Responsibility: AVP of ISS; Authority: Cabinet/UPAC; Reviewed/Endorsed by: Cabinet/UPAC; Review/Effective Date: 06/04/2014, 02/03/2021; Approved by: James L. Gaudino, President
Reformatted and Assigned new Policy Number - Previous Policy CWUP 2-70-050, June 2025