Data Classification and Usage Policy

University Operations – Information Security

CWU Policy 204-04

Effective: February 3, 2021

Policy Review Date: YEAR

Policy Executive: Chief of Staff

Responsible Office/Unit: Office of Institutional Effectiveness, Research and Planning (IERP)

Policy Statement:

Applicability:

Content:

Policy

---

(1) Policy

A. Central Washington University (university) faculty, students, and staff require access to institutional data in support of the university's teaching, research, and outreach missions. The university's institutional data is a valuable asset and must be maintained and protected as such. The purpose of this policy is to help ensure the protection of the university's institutional data from accidental or intentional unauthorized access, damage, alteration, or disclosure while preserving the ability of authorized users to access and use institutional data for appropriate university purposes.

B. Institutional data is defined as all data created, collected, maintained, recorded or managed by the university, its staff, and agents working on its behalf. It includes data used for planning, managing, operating, controlling, or auditing University functions and data used for university reporting.

(2) Scope

A. This policy applies:

1. To enterprise-level operational and administrative institutional data as well as data sets containing these data and systems that may access these data.

2. Regardless of the environment, media, or device where the data resides or is used and regardless of how the data may be transmitted. It also applies regardless of the form the data may take or the data presentation format.

3. to all extracts of covered institutional data, feeds of these data from enterprise systems, and data maintained within so-called shadow or secondary database systems whether derived from enterprise systems or collected or assembled directly by university units. Data in these systems must be classified and protected in the same manner as prescribed by the data steward, or designee, for similar data in primary enterprise systems.

4. To all university community members, whether students, faculty, staff, or agents, who have access to University institutional data. In addition, to the extent possible, it applies to any person or organization, whether affiliated with the university or not, in possession of university institutional data.

(3) Policy Statements

A. Data Regulatory Compliance

1. University employees working with or using institutional data in any manner must comply with all federal, state, and other applicable laws; all applicable university policies, procedures and standards; and all applicable contracts and licenses. For a complete list of privacy laws and regulations related to data classification and usage that impart a duty on the university, see the Security Services department website.

B. Data Roles and Responsibilities

1. All university employees are responsible for ascertaining, understanding, and complying with all laws, rules, policies, standards, contracts and licenses applicable to their own and their subordinates' specific uses of institutional data.

C. Data Classification

1. Data classification provides a basis for understanding and managing institutional data based on the level of criticality and required confidentiality of the data. Accurate classification provides the basis for an appropriate and cost-effective level of security and protection. The university's institutional data will be assigned one of three classifications:

    a. **Public**: Data intended for broad distribution in support of the university's missions or freely available to any person or organization with no restrictions.

    b. **Restricted**: Data that is circulated on a need-to-know basis or sensitive enough to warrant careful management and protection to safeguard its confidentiality, integrity, and availability, as well as appropriate access, use, and disclosure.

    c. **Confidential**: Data protected or regulated by law or critical to university operations including sensitive personal information. Unauthorized disclosure of this information could seriously and adversely impact the university or the interests of individuals and organizations associated with the university.

2. Data stewards must implement a formal data classification process for institutional data under their stewardship. This process must assess the criticality and required confidentiality of data

elements, as well as the risk of exposure or loss. For a detailed description of the data steward role and responsibilities, see CWU 204-03 Information Security and Privacy Roles and Responsibilities. For examples of what constitutes public, restricted, and confidential data, please see the Security Services website.

D. Reporting Responsibilities

1. Breaches, losses, or unauthorized exposures of restricted data must be immediately reported to the Chief Information Security Officer and handled in accordance with CWU 204-05 Information Security and Privacy Incident Management Policy. University employees must also report actual or suspected criminal activity associated with any such incident to the University police department.

E. Data Retention

1. The university's institutional data may often reside in university records, is often used to produce university records, and may itself be university records. University records must be managed in accordance with an approved records retention and disposition schedule.

(4) Policy Maintenance

A. The Chief Information Security Officer, in collaboration with all stakeholders, shall review and approve this policy statement at least annually or more frequently as needed to respond to changes within the institution and the regulatory environment.

(5) Implementation

A. Failure by an individual to comply with the university policy on data classification and usage 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. In a perceived emergency situation, university staff may take immediate steps, including denial of access to the university network and institutional data as well as seizure and quarantine of university-owned data processing and storage assets, to ensure the integrity of university data and systems or protect the university from liability.

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 policy on data classification and usage.

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 2-70-020, June 2025