Information Security and Privacy Roles and Responsibilities

University Operations – Information Security

CWU Policy 204-03

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. The Chief Information Security Officer (CISO) oversees the university information security and privacy activities through the implementation of an information security program that supports the principles of confidentiality, integrity, and availability for university institutional information. The security program is implemented in support of and according to the Information Services and Security strategic plan and CWU 204-06 Information Security Controls.

(2) Roles and Responsibilities

A. Various positions across the university have responsibility for information security and privacy.

B. Security, Privacy, and Data, Advisory Council

1. The Security, Privacy, and Data, Advisory Council (SPDAC) provides institutional advisory services for information security and privacy to the Chief Information Security Officer and broad strategic guidance to support the university-wide information security program. The council is led by the Chief Information Security Officer and the Director of Institutional Effectiveness and reports up to the Enterprise Information Services Committee. The membership of the council is composed of staff representing key areas of the university. The responsibilities of the council include, but are not limited to:

a. Advise, seek wide input, and recommend strategic direction to the Chief Information Security Officer on university-wide information security and privacy;

b. Review and recommend university-wide information security and privacy policies, standards, guidelines, and operating procedures related to institutional information in any form (e.g. electronic or paper);

c. Review and coordinate with the Chief Information Security Officer regarding privacy and compliance requirements related to information security and privacy laws and regulations that impart a duty upon the University;

d. Review institutional risk issues and provide appropriate recommendations in support of the university's larger risk management programs and objectives;

e. Serve as a point of contact for the Chief Information Security Officer as well as for the organizational area(s) for which they are responsible in matters related to information security and privacy; as well as

f. All additional responsibilities outlined in the SPDAC charter.

C. Data Owners

1. Data owners are cabinet level employees, with overall responsibility for the business results or the business use of the data within their delegations of authority (e.g. the Chief Financial Officer, Provost, or Vice President of Operations). The responsibilities of the data owners include:

   a. Overall responsibility and accountability for the data within their subject area domains; and

   b. Recommend policies, standards and guidelines regarding information security and privacy, business definitions of information, and the access and usage of that information, within their delegations of authority.

D. Appointing Authorities

1. Appointing Authorities are assistant vice presidents, associate provosts, deans, executive directors and other individuals with delegated authority for an organizational area as provided in CWU 203-02 Appointing Authority and Delegation of Authority. These individuals, or their designee(s), have the following information security and privacy responsibilities:

   a. As needed, develop, recommend, implement, and maintain policies, standards, or guidelines that are consistent with the university policies on information security and privacy, within the organizational area(s) for which they are responsible;

   b. Be accountable for risks, compliance obligations, and financial costs associated with university information security and privacy, including information security and privacy incidents and information security breaches, within the organizational area(s) for which they are responsible; and

   c. Follow the recommendations of the Chief Information Security Officer or designee, in connection with an information security and privacy incident investigation, and direct others to do so.

E. Data Stewards

1. Data stewards are designated by and responsible to the appointing authority or designee (such as payroll, accounts payable, purchasing, or human resources business leads). Data stewards have knowledge of and work in accordance with numerous federal, state, and university rules and policies, including university policies on information security and privacy. The data steward role focuses on managing data content and the business logic behind all data transformations. The responsibilities of data stewards include:

    a. Help define, interpret, implement, and enforce federal, state, and university policies, standards, and guidelines for institutional information within their purview;

    b. Identify systems of record containing institutional information;

    c. Categorize institutional information within systems of record as public, restricted, or confidential, as defined in CWU 204-04 Data Classification and Usage policy;

    d. Define usage and quality standards and guidelines for institutional information within their purview; and

    e. Develop and implement formal and auditable data access processes for institutional data under their stewardship.

F. Data Custodians

1. Data custodians report to the Chief Information Officer (CIO) or Director of Business Intelligence (BI), or their designee(s). The data custodians are responsible for the safe custody, transport, and storage of institutional data. The responsibilities of the data custodians include:

    a. Support and manage the day-to-day confidentiality, integrity, and availability of the information systems for which they are responsible;

    b. Document and disseminate administrative and operational procedures to ensure consistent storage, processing and transmission of data;

    c. Determine user access and obtain approval(s), as delegated;

    d. Make and be accountable for operational decisions about the use and management of an information systems in accordance with established business rules and policies; and

    e. Maintain critical information system documentation.

G. Data User

1. Data users are faculty, student employees, staff or third party vendors. Data users shall consult with and follow the applicable laws, regulations, and university rules, policies, standards and guidelines. Data users shall only access and use University information systems and institutional information to fulfill authorized job duties or activities for the university and in compliance with the Acceptable Use Policy CWU 701-07.

2. Any agreements to provide a third party access to or use of institutional information shall ensure that such agreement is approved through the appropriate department.

(3) 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.

(4) 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.

History:

Responsibility: AVP of ISS; Authority: Cabinet/UPAC; Reviewed/Endorsed by: Cabinet/UPAC; Review/Effective Date: 6/4/2014; 02/03/2021; Approved by: James L. Gaudino, President
Reformatted and Assigned new Policy Number - Previous Policy CWUP 2-70-010, June 2025