Information Security Incident Response

University Operations – Information Security

CWU Policy 204-05

Effective: May 29, 2024

Policy Review Date: YEAR

Policy Executive: Chief of Staff

Responsible Office/Unit: Information Services and Security

Policy Statement:

Applicability:

Content:

Policy
Appendix A – Information Security and Privacy Incident Management Procedure

---

(1) Purpose

A. This policy defines the parameters necessary to ensure that Information Services and Security (ISS) properly prepares for, detects, analyses, contains, eradicates, recovers from, reports, and learns from information security incidents.

(2) Scope

A. This policy applies to all departments and users of ISS resources and assets, and all assets connected to the enterprise network. This policy also applies to incidents involving institutional information in all forms (e.g. electronic or paper) and information systems either managed by the university or by a third party on behalf of the university and pursuant to a written agreement.

(3) Policy

A. Incident Response Training

1. The university must:

a. Provide incident response training to information system users consistent with assigned roles and responsibilities:

i. For users without a role defined in the Incident Response Plan, users are responsible for reporting incidents to the appropriate business unit or personnel as specified in the incident reporting process. Users are responsible for attending training for recognizing and reporting incidents within the university.

ii. For users with a role defined in the Incident Response Plan, training must be completed within 6 months of assuming the incident response role or responsibility or when required by information system changes, and annually thereafter.

2. Incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations.

3. Employ automated mechanisms to provide a more thorough and realistic incident response training environment.

4. Incorporate lessons learned from incident response training activities into incident response procedures, training, and testing/exercises.

B. Incident Response Testing

1. The university must:

a. Test the incident response capability for the information system at least every two years using a tabletop exercise with defined test cases to determine the incident response effectiveness and document the results.

b. Coordinate incident response testing with areas responsible for related plans such as Business Continuity Plans, Contingency Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, and Occupant Emergency Plans.

C. Incident Handling

1. The university must:

a. Implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

b. Coordinate incident handling activities with contingency planning activities.

c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implement the resulting changes accordingly.

D. Incident Monitoring

1. The university must:

a. Employ automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

E. Incident Reporting

1. The university must:

a. Create a written process for users to report a security incident, including:

i. Primary and secondary methods for reporting

ii. Specific recipients to receive incident reports

iii. The minimum information needed

iv. Timeframes for reporting incidents

2. Require personnel to report suspected security incidents to the IS Service Desk within 24 hours.

3. Report security incident information to the IS Service Desk at 509-963-2001 or the chief information security officer at 509-856-7313.

4. Require the Service Desk to escalate incident reports to the Office of Information Security within 1 hour.

F. Incident Response Assistance

1. The university must:

a. Provide an incident response support resource, integral to the incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

G. Incident Response Plan

1. The university must:

a. Develop an incident response plan that:

i. Provides a roadmap for implementing its incident response capability.

ii. Describes the structure of the incident response capability.

iii. Provides a high-level approach for how the incident response capability fits into the Emergency Management

iv. Plan or COOP.

v. Meets the university's unique requirements, which relate to mission, size, structure, and function.

vi. Defines reportable incidents.

vii. Provides metrics for measuring the incident response capability.

viii. Defines the communication incident response activities to appropriate entities.

ix. Defines the resources and management support needed to effectively maintain and mature an incident response capability.

a. Is reviewed and approved by the associate vice president / chief information officer (AVP/CIO). This review may also occur following an incident or tabletop exercise.

b. Distribute copies of the incident response plan and any additional updates or changes to:

i. associate vice president / chief information officer

ii. data governance & privacy coordinator

iii. director of project management office

iv. director of IT infrastructure

v. director of customer experience

vi. director of application development & integrations

vii. director of enterprise applications

viii. other parties as appropriate

c. Review the incident response plan annually.

d. Update the incident response plan to address system changes or problems encountered during plan implementation, execution, or testing.

e. Protect the incident response plan from unauthorized disclosure and modification.

(4) Policy Exceptions

A. Requests for exceptions to this policy shall be reviewed by the chief information security officer (CISO) and the associate vice president / chief information officer (AVP/CIO). Departments requesting exceptions shall provide such requests to the CISO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IS Department, initiatives, actions, and a timeframe for achieving the minimum compliance level with the policies set forth herein. The CISO shall review such requests and confer with the requesting department.

(5) Policy Owner

A. chief information security officer (CISO)

(6) Policy References

A. NIST SP 800-16 – Information Technology Security Training Requirements: a Role- and Performance-Based Model

B. NIST SP 800-50 – Building an Information Technology Security Awareness and Training Program

C. NIST SP 800-61 - Computer Security Incident Handling Guide

D. NIST SP 800-84 - Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities

E. NIST SP 800-115 - Technical Guide to Information Security Testing and Assessment

(7) Policy Maintenance

A. This policy will be reviewed and updated annually and as needed by the Office of Information Security

B. Revision History

1. Each time this document is updated, this table should be updated.

Version	**Revision Date**	**Revision Description**	**Name**
DRAFT	3/25/2024	Initial draft	Brian Holley

C. The chief information security officer or other designee through the associate vice president of information services and security is responsible for this policy and relevant procedure, Appendix A.

History:

Responsibility: Finance and Administration; Authority: ELT/UPAC; Reviewed/Endorsed by: ELT/UPAC; Review/Effective Date: 05/04/2011; 06/04/2014; 05/29/2024; Approved by: A. James Wohlpart, President
Reformatted and Assigned new Policy Number - Previous Policy CWUP 2-70-030, June 2025
Attached Procedure CWUR 7-70-010 as Appendix A, June 2025

Appendix A - Information Security and Privacy Incident Management Procedure

(1) Procedure

A. This procedure describes the process used for assessing, responding to, and managing information security and privacy incidents (hereafter "incidents"). Incidents include, but are not limited to, unauthorized access, disclosure, modification, and destruction of institutional information and information systems.

(2) Incident Management

A. High Level Incident Management Process Flow

1. Figure 1 illustrates the high-level incident management process flow and is described in the sections below.

B. Obligation to Report and Assist

1. Students, faculty, and staff shall immediately report potential incidents to their supervisor or Security Services department or designated office, as defined below. The incident reporting form is available on the Security Services website.

2. Third parties are contractually bound to limit the access, use, or disclosure of institutional information, information systems, computerized devices, or infrastructure technology, and shall promptly report potential incidents to the university employee who authorized their access, use, or disclosure. In addition, third parties are required to sign a non-disclosure agreement (NDA) and review university policies and procedures prior to commencement of any work.

3. Student, faculty, staff, and third parties shall provide full assistance with the investigation of any potential incident.

C. Analysis and Assessment

1. Based on the type of incident, the Chief Information Security Officer shall coordinate with the university designated offices identified in Table 1 in the analysis and assessment of a potential incident. Depending on the type of incident, the overall responsibility of the incident management process shall lie with the designated office.

2. Table 1. Designated Offices for Analysis and Assessment of Potential Incidents

Analysis and Assessment of Potential Incidents		
Type of Incident	Designated Office	Scope
All incidents unrelated to student educational records, cardholder data, or protected health information	Security Services	All areas of the university
Student Educational Records	Registrar Services	All areas of the university
Cardholder Data	Financial Services	All areas of the university
Protected Health Information (PHI)	Medical Services	All areas of the university

3. Concurrent with the analysis and assessment, the designed office shall, where appropriate, work with data stewards and data custodians to obtain and preserve the necessary evidence associated with the incident.

4. If the designated office determines that an incident actually occurred, they shall conduct a risk assessment based on the sensitivity of the institutional information, impact to users, compliance requirements, criminal activity, and criticality of the information system to determine whether an incident should be referred to or shared with another designated office.

D. Incident Management

1. The Chief Information Security Officer shall, in collaboration with the designated office, assign an incident manager and assemble an incident management team that may include, but is not limited to, the following individuals or functional areas:

   a. Chief Information Officer

   b. Risk Management

   c. Assistant Attorney General

   d. Public Affairs

   e. The appropriate data owner or data custodian

f. Executive heads of major university organizations

g. Chief Human Resources Officer

h. Academic and Student Life

i. University's subject matter experts on privacy laws or regulations related to the incident

2. The incident management team shall:

a. Review the initial analysis and assessment to determine the potential impact of the incident;

b. Assign additional resources, as needed, for further investigation and forensic analysis;

c. Develop and implement a plan to communicate within the University about the incident. The communication plan shall specify the recipients, content, and methods of communication; and

d. Determine whether notification of the incident to parties outside the university is necessary.

[02/21]

E. Notification

1. Notification of an incident shall be made as directed by the incident management team, and shall be carried out in accordance with applicable legal, regulatory, or contractual requirements. The incident manager, in collaboration with the designated office and the Public Affairs department, shall facilitate any notification to parties outside the University.

F. Reporting and Documentation

1. The incident management team shall prepare a written incident summary for each incident. The Chief Information Security Officer shall develop an incident log and perform a quarterly analysis of these summaries to identify trends.

G. Remediation

1. Remediation means efforts to address harm caused by the incident, if any, and efforts to address issues that led to the incident. Remediation may begin at any time, as appropriate, during the incident management process, provided evidence is preserved.

2. If an incident occurred and an incident management team is convened, the incident manager and designated office shall review and approve all proposed remediation actions. The

designated office may also require the departmental unit(s) involved in the incident to develop a formal remediation plan.

3. If an incident did not occur and an incident management team was not convened, the Chief Information Security Officer will use the process described in Section (2)(C) to determine whether remediation is appropriate, and if so, the scope of any such effort.

H. Designated Office Responsibility

1. Each designated office shall develop, maintain, and follow an incident response plan that defines its procedures for analyzing and assessing a potential incident. The Chief Information Security Officer shall review and approve the incident response plans and the plans shall address, at minimum:

   a. Documentation

   b. Preserving evidence and chain of custody

   c. Analysis and assessment

   d. Referral and communication to designated official

   e. Containment

   f. Remediation

   g. Reporting

(3) Procedure Maintenance

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

(4) Additional Information

A. For further information on this procedure or to report an incident, please contact the Security services department.