University Policy Advisory Committee Policy & Procedure Review

Title:	Old Title: Information Security and Privacy Incident Management Policy New Title: Information Security Incident Response Policy
Date Submitted:	4/8/2024
Submitted by (Individual):	Brian Holley
Department:	Security Services
Division:	Information Services and Security
Policy Number:	CWUP 2-70-030
Procedure Number:	1-60-060

☐ New ☑ Revision

þ The policy or procedure has been formatted to be consistent with CWUP standards.

The policy and/or procedure change has a budget impact. Yes ☐ No þ

(*If yes, please attach a spread sheet that provides an analysis of the impact.*)

Consultation and Review

Please indicate consultation completed in the preparation of your proposed policy or procedure, including the name of the individual or groups consulted, the date of the consultation, and any written feedback/recommendations from the group consulted.

Date	No Budget Impact	Date	Budget Impact
	Issue-area stakeholders		Issue-area stakeholders
	Provost's Council		Affected budget authority
	Executive Leadership Team		PBAC
	UPAC		Provost's Council
			Executive Leadership Team
			UPAC

Summary of impact: Briefly explain why this policy or procedure has been created/changed.

This policy has been changed to adhere to NIST SP 800-61 – Computer Security Incident Handling Guide. This is the standard set by the Federal Government for information security incident response.

Summary of policy/procedure:

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

Itemization of changes (revision documents): brief narrative

This is a complete rewrite of the incident response policy, so everything is different.

Policy impact on equity:

1. What does this policy aim to do?

This policy details the foundational elements of an effective response for an information security incident. This policy sets the stage for the preparation phase of incident response. The associated Incident Response Plan will contain the actual steps to be taken to respond to an active incident.

A. Who benefits from this policy?

The entire university, including students, faculty, staff and administration.

B. Who is left out of this policy?

No one.

2. What are the basic assumptions of this policy?

That all members of the CWU community will be trained on how to report a suspected information security incident, and certain members of the ISS division will be trained on how to respond to reported information security incidents.

A. How do these assumptions impact equity?

The training applies to individuals regardless of race, ethnicity, age, gender, religion, sexual orientation, gender identity, gender expression, disability, economic status and other diverse backgrounds.

For clarification and consultation, contact Dr. Lucinda.Carnell, Interim Vice President of Diversity, Equity, and Inclusion at Lucinda.Carnell@cwu.edu

(Insert page number (bottom right) and Footer that denotes the section and sub-section of the P/R in the bottom left of the footer. Footer example below).

CWUP X-XX-XXX Policy Title

(Describe the purpose and scope of the policy, who is responsible for it and how it will be maintained. Use common language, present tense, active voice. Keep it simple, straight forward and easy for the reader to understand.)

Add the following sentence at the end of the policy description.

The department manager/director or other designee through the vice president of operations is responsible for this policy and relevant procedure, CWUR X-XX-XXX.

Include signature line. ***Include all previous approval dates.***

[Responsibility: Operations Division; Authority: ELT/UPAC; Reviewed/Endorsed by: ELT/UPAC; Review/Effective Date: XX/XX/20XX; Approved by: A. James Wohlpart, President]

~~CWUP 2-70-030 Information Security and Privacy Incident Management Policy~~

CWUP 2-70-030 Information Security Incident Response Policy

(1) Purpose

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.

~~(1) Scope~~

~~This policy 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.~~

(2) Scope

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.

~~(2) Responsibilities~~

~~The Chief Information Security Officer, or designee, provides oversight and direction for all information security related incidents and may designate an incident manager, as the situation dictates and in accordance with this policy. In the event a crime has been committed, the Chief Information Security Officer will coordinate with the campus police department and/or other legal enforcement entities to determine responsibilities for the incident.~~

~~(3) Disclosure Limitations~~

~~Care shall be taken in handling evidence and information related to incidents in order to comply with federal or state laws that limit disclosure—e.g., Health Information Portability and Accountability Act (HIPAA) and Family Education Rights and Privacy Act (FERPA).~~

~~Documentation related to the incident may include information regarding the infrastructure and security of computer and telecommunications networks, security recovery plans, and security risk assessments; or, may include information for which disclosure is prohibited by federal law. As a result, incident-related information may be exempt from public disclosure and a list of the relevant regulatory reference is available on the Security Services website.~~

~~(4) Policy Maintenance~~

~~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.~~

~~(5) Additional Information~~

~~For further information on this policy or to report an incident, please contact the Security Services department.~~

(3) Policy

(A) Incident Response Training

The university must:

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

a. 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.

b. 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

The university must:

1. 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.

2. 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

The university must:

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

2. Coordinate incident handling activities with contingency planning activities.

3. 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

The university must:

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

(E) Incident Reporting

The university must:

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

a.Primary and secondary methods for reporting

b. Specific recipients to receive incident reports

c. The minimum information needed

d. 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

The university must:

1. 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

The university must:

1. Develop an incident response plan that:

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

b. Describes the structure of the incident response capability.

c. Provides a high-level approach for how the incident response capability fits into the Emergency Management Plan or COOP.

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

e. Defines reportable incidents.

f. Provides metrics for measuring the incident response capability.

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

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

i. 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.

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

a. associate vice president / chief information officer

b. data governance & privacy coordinator

c. director of project management office

d. director of IT infrastructure

e. director of customer experience

f. director of application development & integrations

g. director of enterprise applications

h. Other parties as appropriate

3. Review the incident response plan annually.

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

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

(4) Policy Exceptions

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

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

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

Revision History

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

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, CWUR 2-70-030.

~~*[5/04/2011; Responsibility: AVP of ISS; Authority: Cabinet/PAC; Reviewed/Endorsed by: Cabinet/PAC; Review/Effective Date: 6/4/2014; Approved by: James L. Gaudino, President]*~~

[Responsibility: ~~Information Services and Security~~ Finance and Administration~~Division~~; Authority: ELT/UPAC; Reviewed/Endorsed by: ELT/UPAC; Review/Effective Date: 05/04/2011; 06/04/2014; XX/XX/20XX; Approved by: A. James Wohlpart, President]