Information Security Standard 16.1a

Information Security Incident Management Standard

Initially Approved: September 8, 2010
Modified: April 11, 2019
Revised: August 25, 2020 (as an Information Security Standard)
Administering Office: Office of the CIO

I. STANDARD STATEMENT

This standard operates under University Policy 117 Information Security. It is WCU policy to respond to suspected or known information security incidents in an appropriate, timely, and efficient manner. As soon as practicable, WCU shall mitigate the potential, harmful effects of security incidents to daily operations and the integrity and security of university data. WCU shall establish an Information Security Incident Response Team (IRT) that will develop and maintain an information security incident response plan pertaining to security incident reporting and escalation. This plan should address security incident identification, investigation, reporting procedures, escalation procedures, notification requirements, and documentation requirements.

II. SCOPE AND APPLICATION OF THE STANDARD

This standard applies to all University workforce members and any other person utilizing any form of University information technology.

III. DEFINITIONS

"Information security incident" means (i) any suspected or real adverse event, including accidental disclosure or unintentional actions, that compromises or circumvents the security and integrity of a computer system or network, resulting in unauthorized access, use or disclosure of personally identifiable information (PII) which includes protected Health information (ePHI), or (ii) the act of violating a computer system or data privacy and/or security policy or standard. Examples of information security incidents may be: attempts (either failed or successful) to gain unauthorized access to a computer system or its data; unwanted disruption or denial of service; the unauthorized use of a system for the processing or storage of data; or unauthorized changes to a computer system hardware, firmware or software.

“Personally Identifiable Information (PII)” means any information about an individual maintained by an agency, including (i) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number,

date and place of birth, mother's maiden name, or biometric records; and (ii) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

"Protected Health Information (ePHI)" is defined as any individually identifiable health information and is required to be protected through the Health Insurance Portability and Accountability Act (HIPAA).

"Workforce Member" includes, but is not limited to, faculty, staff, employees, guests, consultants, vendors, contractors, volunteers, interns, student workers or temporary workers associated with the University.

IV. INFORMATION SECURITY INCIDENT MANAGEMENT STANDARD

A. Accountability / Enforcement

- The Data Security and Stewardship Committee(DSSC), as defined in University Policy 97, is responsible for the development, implementation, communication, and oversight of information security policies. This committee has oversight of the Information Security Incident Management Policy and related response plan. Internal Audit will periodically review policy compliance.
- The standing membership of the IRT includes the CIO (IRT Leader), General Counsel, Chief Information Security Officer, and University Police. These positions or their designee are responsible for implementing the *WCU Information Security Incident Response Plan* referenced below.
- The following areas will have a primary and secondary representative appointed to serve as needed on the IRT: Emergency Services, Internal Audit, Public Information, Human Resources, Student Affairs and Advancement.
- Department managers are responsible for all initial and recurring information security policy training of members of their workforce, and for enforcing information security policies and procedures.
- All workforce members are responsible for reporting information security incidents and assisting the IRT in investigating and mitigating information security incidents.

B. Reporting Information Security Incidents

- As soon as an incident has been identified, the employee who discovered it must take immediate steps to report the incident to his or her supervisor. The supervisor must take immediate action to notify the IRT Leader. The IRT Leader should notify Legal Counsel of any reported incident as soon as possible.
- Any person utilizing any form of University information technology is required to note and report any observed or suspected information security weaknesses in systems or services to their supervisor and the Division of Information Technology.
- Reporting a computer security incident maliciously or in bad faith may constitute an abuse of this policy, and may result in disciplinary action against the person making the report.

.

C. Review and Revisions

The DSSC is to regularly review and revise this policy as may be appropriate, minimally every three years. There may be events that trigger additional reviews such as changes in laws or regulations, information security best practices, threat models, or changes in business processes.

V. REFERENCES

International Standards Organization (ISO/IEC 27002, 16.1 Management of information security incidents and improvements)

University Policy 117 Information Security

University Policy 97 Data Security and Stewardship

WCU Information Security Incident Response Plan

45 CFR Part 164, Subpart C – Security Standards for the Protection of Electronic Protected Health Information

- Response and Reporting [164.308(a)(6)(ii)] (Required) - Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.
- Security Incident Procedures [164.308(a)(6)(i)] (Standard) - Implement policies and procedures to address security incidents.