

Information Security Standard

Information Technology Disruption Standard

Initially Approved: July 13, 2023

Revised: April 11, 2024

Administering Office: Office of the CIO

I. STANDARD STATEMENT

This standard operates under University Policy 117 Information Security. ISO 27002, WCU's information security framework, includes the following controls: Information security incident management planning and preparation, Response to information security incidents, Information security during disruption, ICT readiness for business continuity and Information security event reporting. This *Information Technology (IT) Disruption Standard* address portions of each of those controls. Specifically, it addresses the planning and preparation for responding to various disruptions to WCU's information technology.

II. SCOPE AND APPLICATION OF THE STANDARD

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

III. DEFINITIONS

"Information security incident" is defined as an event or series of events that are likely to result in demonstrable harm to the university. This harm could come through loss of control of sensitive data, unauthorized access or changes to IT resources, or other violations of security and privacy policies that may have wide-ranging impacts (e.g. catastrophic data loss, prolonged organizational downtime, or major financial impact)

"Ransomware" is a type of malicious software (malware) that threatens to publish or blocks access to data or a computer system, usually by encrypting it, until the victim pays a ransom fee to the attacker.

"Disaster" is defined as an event destroying, or making significantly inoperable, one of our two on campus data centers. The ultimate determination of a disaster may include additional considerations and is at the discretion of the CIO (or if unavailable – the Associate CIO or Assistant CIO).

IV. **IT DISRUPTION RESPONSE STANDARD**

The IT Division shall develop, test, and update response and recovery plans to address the ISO 27002 controls related to disruptions or emergencies.

Depending on the nature of the emergency or disruption to WCU's information technology one or more of the following response plans may be activated:

1. In the case of an information security incident, as defined above, the [Information Security Incident Management Standard](#) and related Information Security Incident Response Plan will be followed.
2. If the information security incident is deemed to be a ransomware incident, then the Ransomware Incident Response Plan will be followed.
3. If the disruption is declared a disaster, as defined above, the IT Disaster Recovery Plan will be followed.

V. **REVIEW AND REVISIONS**

The Information Security and Privacy Committee is to regularly review and revise this policy as may be appropriate. There may be events that trigger reviews such as changes in laws or regulations, information security best practices, threat models, or changes in business processes.

VI. **REFERENCES**

International Standards Organization (ISO/IEC 27002:2022, Clause 5 Organizational Controls)

[University Policy 117 Information Security](#)

[University Policy 97 Information Security and Privacy Governance](#)

[Information Security Incident Management Standard](#)

Information Security Incident Response Plan

Ransomware Incident Response Plan

IT Disaster Recovery 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.