

# R345, Information Technology Resource Security<sup>1</sup>

**R345-1 Purpose:** To provide minimum security standards and requirements for protecting Personally Identifiable Information at institutions in the Utah System of Higher Education (“USHE”) from potential threats such as human error, accident, system failures, natural disasters, and criminal or malicious action.<sup>2</sup>

## R345-2 References

- 2.1 [Board Policy R124](#), Government Records Access and Management
- 2.2 [Board Policy R341](#), Computing Systems Programs
- 2.3 [Board Policy R1010](#), Data Breaches
- 2.4 [Board Policy R1011](#), Contractual Standards for Use of Personally Identifiable Student Data by Third-Party Contractors
- 2.5 [Center for Internet Security Critical Security Controls](#)
- 2.6 [Utah Code Title 78B, Chapter 4, Part 7](#), Cybersecurity Affirmative Defense Act
- 2.7 [Utah Code Title 53H, Chapter 14, Part 5](#), Higher Education Student Data Protection
- 2.8 [Utah Code 63A, Chapter 19](#), Government Data Privacy Act
- 2.9 U.S. Department of Homeland Security Handbook for Safeguarding Sensitive PII/Privacy Policy Directive 047-01-007, Revision 3
- 2.10 [34 Code of Federal Regulations Section 99.3](#)

## R345-3 Definitions

- 3.1 **Center for Internet Security (“CIS”) Critical Security Controls:** means a prescriptive, prioritized set of cybersecurity best practices and defensive actions that can help prevent the most pervasive and dangerous attacks, and support compliance in a multi-framework era. These actionable best practices for cyber defense are formulated by a group of IT experts using the information gathered from actual attacks and their effective defenses. The CIS Controls provide specific guidance and a clear pathway for organizations to achieve the goals and objectives described by multiple legal, regulatory, and policy frameworks.
- 3.2 **Critical IT Resource:** means an IT Resource which is required for the continuing operation of the institution and/or its colleges and departments, including any IT Resource which, if it

---

<sup>1</sup> Adopted March 21, 2008; amended September 16, 2016, November 16, 2018, November 18, 2022; and March 26, 2026.

<sup>2</sup> Technical edits September 10, 2024.

fails to function correctly and/or on schedule, could result in a major failure of mission-critical business functions, a significant loss of funds, or a significant liability or other legal exposure. For example, General Ledger monthly financial reporting may be considered non-Critical IT Resources by the institution, but financial reporting at fiscal year-end may be considered a Critical IT Resource.

**3.3 Information Security Office(s) (“ISO”):** means the office that develops and maintains security strategies for the institution’s IT Resource systems, risk assessments, compliance with ISO policies and guidelines, and for the resolution of campus IT security incidents. The institution may have ISO functions performed by one or more individuals or offices. If multiple individuals or offices are involved, their respective roles and assignments should be clearly delineated.

**3.4 Information Technology Resource (“IT Resource”):** means a resource used for electronic storage, processing or transmitting of any data or information, as well as the data or information itself. This definition includes but is not limited to electronic mail, voice mail, local databases, externally accessed databases, Internet-based storage, mobile devices, removable storage, CD-ROM, recorded magnetic media, photographs, digitized information, or microfilm. This also includes any wire, radio, electromagnetic, photo optical, photo electronic or other facility used in transmitting electronic communications, and any computer facilities or related electronic equipment that electronically stores such communications.

**3.5 IT Resource Steward:** means the individual who has policy level responsibility for determining what IT Resources will be stored, who will have access, what security and privacy risk is acceptable, and what measures will be taken to prevent the loss of Information Resources.

**3.6 IT Resource Custodian:** means the organization or individual who implements the policy defined by the IT Resource Steward and has responsibility for IT systems that store, process, or transmit IT resources.

**3.7 IT Resource Administrator:** means institutional staff that, under the direction of the IT Resource Steward and with operational instructions from the IT Resource Custodian, have day-to-day operational responsibility for data capture, maintenance, and dissemination.

**3.8 Personally Identifiable Information (“PII”):** has the same meaning as “personal data” as defined under [Utah Code section 63A-19-101\(24\)](#), and includes information that is linked

or can be reasonably linked to an identified individual or an identifiable individual. PII must be protected prior to release in accordance with applicable laws including but not limited to the Utah Government Records Access Management Act (“GRAMA”), the Utah Government Data Privacy Act, the Family Educational Rights and Privacy Act (“FERPA”), and as otherwise required by law. PII includes but is not limited to the following:

**3.8.1** Personally identifiable student data as defined under [Utah Code section 53H-14-501](#).

**3.8.2** Personally identifiable information from the education records of students, as defined by FERPA under [34 CFR § 99.3](#).

**3.8.3** Protected Health Information, as defined by the Health Insurance Portability and Accountability Act (“HIPAA”).

**3.8.4** PII does not include “public information” as defined by GRAMA, or in the case of student records, “directory information” as defined by FERPA.

**3.9 Security:** means measures taken to reduce the risk of: (a) unauthorized access to IT Resources, via either logical, physical, managerial, or social engineering means; and/or (b) damage to or loss of IT Resources through any type of disaster, including cases in which a violation of security or a disaster occurs despite preventive measures.

**3.10 Security Plan:** means a formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

**3.11 User:** means any person, including a faculty member, staff member, student, patient, contractor, consultant, intern, or temporary employee, who accesses and uses institutional IT Resources.

**R345-4 Policy:** Each USHE institution including its colleges, departments, and divisions shall take measures to protect PII that is stored, processed, or transmitted using IT Resources under their control.

**4.1** Institutions shall adopt and strive to implement the CIS Critical Security Controls as a guiding security framework and the minimum institutional security standard. Institutions may implement additional frameworks, standards, or regulations as required by law, contract, or specific circumstances and may be more restrictive than this policy. Each institution shall develop and maintain a written information Security Plan and program informed by the CIS

Critical Security Controls, best practices, and other applicable requirements. The purpose of this plan is to present information to drive informed decisions regarding risk mitigation and identify prudent resource allocation and investment in cybersecurity.

- 4.2** Institutions shall design reasonable and appropriate security procedures informed by their written Security Plan to prevent unauthorized individuals or organizations from accessing IT Resources that store, process, or transmit PII or any IT Resources that provide a possible vector or avenue to a breach of PII or Critical IT resources with specific prioritization given to high-risk vectors including web and email safeguards.
- 4.3** Institutions shall provide mandatory and recurring cybersecurity awareness training, that is reviewed frequently to keep up with evolving security threats and aligns with best practices, for all users to reduce risks associate with human error.
- 4.4** Institutions shall maintain commercial insurance, captive insurance, and/or self-insurance covering loss or breach of PII.

**R345-5 Roles and Responsibilities:** Each USHE institution shall clearly define the roles and responsibilities of persons charged with the security of institutional information resources. The ISO office(s) at an institution may be comprised of one or more persons or groups based on the institution’s IT Security needs. The institution may also choose to use designations other than “IT Resource Steward, IT Resource Custodian, and IT Resource Administrators” to describe the persons charged with the following roles and responsibilities. The president is accountable for the institution’s compliance with this policy and the effectiveness of its Information Security Plan. The president shall ensure that cybersecurity risks are integrated into the institution’s enterprise risk management process and reported to the Board of Trustees annually.

**5.1 Institutional ISO:** The ISO reports directly to a senior institutional administrator. The ISO is responsible to coordinate, review, and approve procedures used to provide the requisite security for PII or Critical IT Resources. The ISO is also responsible for coordinating compliance with this policy and shall:

- 5.1.1** Implement and enforce adherence to the CIS Critical Security Controls;
- 5.1.2** Develop and maintain security policies, plans, procedures, strategies, architectures, best practices, and minimum requirements;
- 5.1.3** Provide guidance consistent with institutional policy to IT Resource Stewards and IT Resource Custodians;

- 5.1.4** Operate or coordinate the operation of technical security controls and security systems;
- 5.1.5** Conduct periodic and ongoing security audits, including independent technical validation such as penetration testing to assess the real-world effectiveness of implemented controls, to confirm compliance with this policy;
- 5.1.6** Direct the campus Incident Response Team, incident response activities, and incident resolution at institutional, departmental, and individual levels, and take appropriate and reasonable remedial action to resolve security incidents;
- 5.1.7** Assist institutional or third-party auditors in the analysis of campus IT Resources to further ensure policy compliance;
- 5.1.8** Monitor compliance with security policies and procedures and report compliance violations to the relevant cognizant authority; and
- 5.1.9** Ensure compliance with the Government Data Privacy Act data breach response requirements.

**5.2 IT Resource Custodian:** IT Resource Custodians (Computer Services and other IT Resources related work units or individuals) will manage the campus network and other IT systems and resources and, as related to their security roles and responsibilities, shall:

- 5.2.1** Implement and administer the security of IT Resources in accordance with the CIS Controls;
- 5.2.2** Inform the Information Security Officer of indicators of attack, which pursuant to best practices, procedures, and standards, may indicate a potential or actual threat to the network and campus IT Resources; and
- 5.2.3** Apply security policy and procedures to IT Resources as directed by the ISO.

**5.3 Incident Response Team:** Under the direction of the Information Security Officer, the Incident Response Team is responsible for immediate response to any breach of security. This team is also responsible for determining and disseminating remedies and preventative measures that develop as a result of responding to and resolving security breaches.

**5.4 IT Resource Steward:** The IT Resource Steward is designated by the cognizant authority of the relevant group or work unit, is familiar with data issues, laws, and regulations.

**5.4.1** The IT Resource Steward shall:

**5.4.1.1** Determine the purpose and function of the IT Resource;

**5.4.1.2** Determine the level of security required based on the sensitivity of the IT Resource;

**5.4.1.3** Determine the criticality of the IT Resource;

**5.4.1.4** Determine accessibility rights to the IT Resource;

**5.4.1.5** Determine the appropriate method for providing business continuity for Critical IT Resources (e.g., performing service continuity at an alternate site, performing equivalent manual procedures, etc.); and

**5.4.1.6** Specify adequate data retention, in accordance with the institution's policies, and state and federal laws for IT Resources consisting of applications or data.

**5.4.2** An IT Resource Steward in a work unit that lacks the professional IT staff or expertise to accomplish items 5.4.1 through 5.4.7, or to fulfill the responsibilities of the IT Resource Administrators, may request assistance from the Information Security Officer.

**5.5 IT Resource Administrator:** The IT Resource Administrator(s) performs security functions and procedures as directed by the IT Resource Steward and implements and administers the security of IT Resources in accordance with institutional policy and industry best practices and standards.

## **R345-6 Sanctions and Remedies**

**6.1 Emergency Action by the ISO:** The ISO may discontinue service to any User who violates this policy or other IT policies when continuation of the service threatens the security (including integrity, privacy, and availability) of the institution's IT Resources. The ISO may also discontinue service to any network segment or networked device if the continued

operation of such segments or devices threatens the security of the institution's IT Resources. Unless non-compliance is causing a direct and imminent threat to the institution's IT Resources necessitating emergency action, the ISO will notify the IT Resource Steward or their designee to assist with resolving non-compliance issues before discontinuing service(s).

**6.2 Emergency Action by the IT Resource Steward:** The IT Resource Steward may discontinue service or request that the ISO discontinue service to network segments, network devices, or Users under their jurisdiction, that are not in compliance with this policy. Unless non-compliance is causing a direct and imminent threat to the institution's IT Resources necessitating emergency action, the IT Resource Steward will notify, or request that the ISO notify, affected individuals to assist with resolving non-compliance issues before discontinuing service(s).

**6.3 Restoration of Access:** A User's access may be restored as soon as the direct and imminent security threat has been remedied.

**6.4 Revocation of Access:** USHE institutions shall reserve the right to revoke access to any IT Resource for any User who violates the institution's policy, or for any other business reasons as allowed by applicable institutional policies.

**6.5 Disciplinary Action:** Violation of the institution's policy may result in disciplinary action, including termination of employment. Employees may appeal revocation of access to IT Resources or disciplinary actions taken against them pursuant to institutional policy.