University Policy 551: Information Security

Category: Operating Policies
Subcategory: Information Technology
Covered Individuals: Employees or Persons with access to Institutional PII/CID
Responsible Executive: Chief Information Officer (CIO)
Policy Custodian: Institutional Security Officer (ISO) role, Information Technology Services (ITS)
Last Revised: 2022/03/23
Previous USU Policy Numbers: *551: Computer Management (2008) and 558: Information Security (2010)*

551.1 PURPOSE AND SCOPE

This policy is established to protect Critical Institutional Data (CID) and Personally Identifiable Information (PII) while stored, accessed, processed, or transmitted by Utah State University (USU). The purposes of this policy will be achieved through proper assignment of responsibility, and appropriate management and protection of accounts and credentials, access levels, devices, services, and incident response.

This policy and its associated procedures are intended to comply with and implement the requirements of Utah State of Higher Education Policy R345, Information Technology Resource Security and the Protection of Personal Information Act, Utah Code 13-44-101 et seq.

Proper implementation and management of roles, responsibilities, accounts, credentials, access levels, devices, services, and response, reduces risk of loss and the legal, reputational, and financial consequences that may result.

551.2 POLICY

2.1 Protecting and preserving PII and CID

2.1.1 USU and its employees, colleges, departments, centers, and divisions, must take measures to protect institutional PII and CID that are stored, accessed, processed, or transmitted using USU services, systems, and resources.

2.1.2 **Data Trustees** are USU Administrative Officers (President, Provost, Vice Presidents, Deans, etc.) who have oversight responsibilities for data governed by or used within their divisions. The responsibilities of Data Trustees include: designating data stewards, ensuring the establishment of practices that will protect and preserve the PII and CID collected and/or used, development of processes for reviewing and approving data transfer, integration, and use requests by other units, and designing and implementing workflows and/or procedures to reduce risk.

2.1.3 **Data Stewards** are management level officials (Controller, Registrar, Directors, Managers, etc.) who have operational level responsibility for specific data or services that may include PII and/or CID. Data Stewards are responsible for: coordinating with Data Trustees, classifying specific data as PII or CID, authorizing specific data users to access data as needed for their job functions, and enforcing the policies, procedures, programs, and practices that apply.

2.1.4 System Administrators or Support Technicians are IT professionals with assigned responsibilities to technically manage IT resources, computers, software, and services which store, process or transmit PII and/or CID. They are responsible for technical system and service data preservation, system-level security features, and to configure, secure, and maintain such according to best practices, policies, procedures, and software that apply to the services and systems they are assigned to support.

2.1.5 Data Users are any persons who are authorized to examine or utilize data, including PII and/or CID, as part of their duties. Data Users must protect against unauthorized access, duplication, or release of PII as well as loss or corruption of CID from their user-controlled equipment, accounts, and credentials, and to follow all service and access policies, programs, and procedures established by their units and/or USU.

2.1.6 USU requires anyone with access to institutional credentials, systems, services, or resources that may store or transmit institutional PII/CID to:

1) understand and comply with policies, procedures, and programs established for the equipment, service, data classification, and role assigned.
2) report to Data Stewards or Data Trustees any access to PII and/or CID outside of the scope of their role for correction and remediation.
3) understand how to effectively utilize multifactor authentication, including denying unauthorized attempts, and reporting and updating credentials if such occurs.
4) effectively participate in required trainings, including annual, service, procedure, and compliance.
5) follow best practice protection of any data or IT Resource used to store, view, process, or transmit information. Protection from electronic, social, and physical compromise or loss is required.
6) promptly report to the IT Service Desk or the IT Enterprise Systems and Security Team, all evidence or suspicion of network, device, credential, or service intrusion attempts, information security breaches, and other security related incidents perpetrated against data and information resources.

2.1.7 Internal Audit Services, Legal Affairs, and the Office of Information Technology Services (ITS) have authority to review and audit all systems, devices, services, procedures, and controls used during the storage, processing, and transfer of institutional data.

2.1.8 ITS is directed to develop and maintain a written cybersecurity program, reasonably conforming to necessary cybersecurity frameworks (see policy Guidance section and applicable procedures for more information), and to establish and maintain procedures with regard to this policy in collaboration and consultation with the Office of Legal Affairs, Office of the Vice President for Research, and other units as may be appropriate to reduce cybersecurity risk.

2.2 Account and Credential Security (to services, applications, data, and resources)

2.2.1 Services that utilize USU credentials (including employee A# accounts), which provide access to services that contain or process institutional PII and/or CID, or other systems identified by the ISO as necessary to safeguard institutional data and/or systems, must be protected by multifactor authentication.

2.2.2 Authentication credentials will be provisioned, updated, and revoked according to USU employment, position, service, and role assignments.

2.2.3 Authentication credentials (including passwords) will be reviewed for vulnerability, and such may be expired, revoked, or reset to reduce risk or if there is evidence of compromise or misuse.

2.2.4 Persons in possession of credentials are required to comply with account, service, and credential requirements, and to protect and secure such against misuse. Individual credentials (including A# username/password) may not be shared.

2.2.5 Use of shared credentials and/or orphan accounts are to be minimized to necessary circumstances and should not be used to store or access PII. Data Trustees and/or Data Stewards shall ensure that shared credential accounts have processes in place to reduce risk, including appropriate onboarding and offboarding practices, such as changing the shared credential password whenever any team member with access changes.

2.3 Access Level Security (within services, applications, data, and resources)

2.3.1 Data Stewards and Data Trustees (see 2.1) are required to establish and maintain documented procedures for assigning, changing, and revoking rights to data within services and applications under their stewardship, and to ensure that access levels assigned to credentials remain appropriately monitored, scoped, assigned, controlled, and revoked.

2.3.2 Access must be restricted, wherever possible, to the minimum set of data and services necessary to the current role and function to be performed.

2.4 Device Security (computers, laptops, servers, storage, etc.)

2.4.1 All institutional devices, computers, servers, storage, and other IT Resources must be configured and managed by employees who have ongoing responsibilities for those resources to reduce vulnerability in compliance with best practice and USU Computer Management Procedures.

2.4.2 The transfer and storage of PII and/or CID to end-user equipment is restricted to necessary circumstances and is to be minimized and eliminated wherever possible. Certain service or data classifications may prohibit storage on end-user devices entirely.

2.4.3 When PII and/or CID is transferred or stored it must be protected by encryption, strong credentials, and all other measures appropriate for the specific data classification.

2.4.4 When IT Resource media are being disposed, destroyed, or recommissioned, industry standard procedures for thorough obliteration of PII and/or CID must be employed by the media owner/user, system administrator/support technician, and/or by USU Surplus Property Sales.

2.4.5 USU does not accept liability for PII that is transmitted through, or stored on, IT Resources by the end user for non-university related purposes.

2.5 Personal Accounts

2.5.1 Use of personally owned accounts and services to store institutional PII and/or CID is prohibited. Such cannot be assumed or assured to meet regulatory, compliance, classification, security, retention, or preservation requirements.

2.6 Service Security

2.6.1 Storage, processing, provisioning, or backup of PII and/or CID and related services and applications must use service providers, software, and systems evaluated and approved by the responsible Data Steward, in consultation with the Office of Information Technology Services, designated Systems and Technical Support, and other individuals or units as the specific data classification may necessitate, including following USU contract review policies and procedures.

2.6.2 Such systems must be configured and supported technically, procedurally, and operationally according to this policy and in compliance with other applicable procedures, regulations, controls, or requirements.

2.7 Incident Response

2.7.1 Upon discovery or notification of a security incident, ITS will evaluate and where necessary, promptly and systematically convene a technical incident response team to investigate, escalate, remediate, and collaborate with other units and USU Administration to resolve the issue.

2.7.2 ITS shall establish procedures, in collaboration and consultation with the Office of Legal Affairs, for convening a Technical Incident Response Team to respond to security breaches that may expose or destroy PII or CID.

2.7.3 USU compliance, legal, privacy, and regulatory leads must be promptly informed of any and all breach or loss of PII or CID.

2.7.4 To protect confidentiality and promote identification of perpetrators, any external notification about an incident must be handled by University Marketing and Communications (UMAC) after review and approval by impacted unit administration, CIO, General Counsel, and any President's designees.

2.7.5 Ransom payments or other demand responses may not be made without approval by the President or President's designee(s).

2.7.6 If an incident is judged by ITS, in consultation with available administrators, to be a critical threat to the confidentiality of data and/or the integrity of Information Resources, ITS is authorized to take immediate action to eliminate the threat. This action may include the interruption of service, addition of controls, denial of access, or removal of systems from the network while the incident is being resolved. Such actions will be reported to the CIO and the affected members of the USU community. Actions required to control a critical security incident will take precedence over business continuity. Losses due to a security incident must be weighed against losses due to interruption of services to the USU community in assessing the criticality of a threat.

551.3 RESPONSIBILITIES

3.1 Anyone with access to USU data, systems, or services has a responsibility to understand and comply with this policy.

3.2 Every service that acts as a system of record for PII or CID must have Data Trustees, Data Stewards, and System Administrators/Support Technicians identified and reported to ITS through the Office of the CIO.

3.3 Data Trustees will be assigned, where necessary, by a committee consisting of the CIO, the Vice President for Finance & Administrative Services, the Vice President for Academic Instructional Services, and the Provost.

551.4 REFERENCES

- Utah System of Higher Education Policy R345, Information Technology Resource Security
- Protection of Personal Information Act, Utah Code 13-44-101 et seq.

551.5 RELATED USU POLICIES

- Information Technology Policies (550-579)
- Policy 588: Research Data
- Policy 528: Contract Signature Authority and Delegation

551.6 DEFINITIONS

- **Compromise** - Loss of exclusive, authorized control of an IT Resource to an unauthorized person or to unauthorized software resulting in exploitation, control and/or use of the IT Resource beyond USU's purpose or intent for that IT Resource.
- **Critical Institutional Data (CID)** - Any USU institutional data that cannot be regenerated from readily available sources if corrupted or lost and is necessary for the function of USU. CID may be private or public. CID is any information that is generated or acquired, stored and required for the continued function of USU, including but not limited to: academic records, employment records, financial records, schedules, etc.
- **Critical IT or Information Resource** - Any IT Resource which, if it fails to function when needed, would cause an unacceptable disruption to mission critical academic or business services of USU or expose USU to liability. Examples include: the wired network, essential communications systems, the enterprise administrative computing system (Banner), the learning Management System (Canvas), etc.
- **Device** – Any piece of technology used to store, transmit, access, or utilize data.
- **End-user equipment –** Any device that is used by the ultimate intended unit, consumer, manipulator, accessor, user, or producer of data in USU systems.
- **Incident Response Team** - An ad hoc team of specialists convened to investigate the causes of a security breach or other data exposure event, to evaluate the extent and cost of a loss, and to formulate corrective actions to prevent recurrence.
- **Information or IT Resource** - Any electronic equipment, infrastructure or software used to transmit, process or store digital data or information. This policy is concerned only with IT Resources owned or leased by USU or privately owned client-side equipment that is directly connected to USU IT infrastructure. IT Resources include, but are not limited to: servers, network wiring, routers, switches, wireless access points, desktop, laptop, handheld and other portable client equipment and peripherals such as printers, scanners, web cameras, as well as programs and operating systems used on any of that equipment. For the purposes of this policy "IT Resource" does not include the data (PII, CID or other) that is transmitted, processed or stored on the IT Resource.
- **Orphan Accounts** - These are USU credentials (usernames and passwords) that are not assigned directly and exclusively to an individual.
- **Personally Identifiable Information (PII)** - Non-public information maintained by or accessible through IT Resources such as networks and/or computers, that can be used to identify an individual alone (e.g., full social security number, biometric records, etc.) or when an individual's first name or initial and last name is combined with other information linkable to that person, including but not limited to the following: last four digits of a Social Security number, date or place of birth, mother's maiden name, government issued identification numbers such as driver license or state identification card number, and/or protected health information . Access to such data is governed by state and federal laws, both in terms of protection of the data, and requirements for disclosing the data to the individual to whom it pertains. Private Sensitive Information does not include public information that is lawfully made available to the general public from federal, state, or local government records and/or pursuant to the Utah Government Records Access and Management Act (GRAMA), or in the case of student records, "directory information" as defined by the Family Education Rights and Privacy Act (FERPA).
- **Security** - The process of managing risks to prevent or reduce loss.
- **Security Breach** - An identified compromise which exposes PII to unauthorized access or an IT Resource to unauthorized use.
- **Server** - A computing device used to provide services or data to multiple users.
- **Service** - A software application or system, purchased, subscribed to, or created, to meet a set of business objectives that stores, manipulates, or transmits data. Examples include Software as a Service, software applications, cloud or locally hosted software.
- **System** – A bounded collection of components, including hardware, software, services, data, and processes unified (often as a service) to meet a set of business objectives.
- **System of Record** - A system of record is a server or service that is the authoritative source for a given set of data or set of information.
- **Unauthorized Access** - Access to a USU IT Resource or to USU data that is outside of the approved uses.

- **Vulnerability** - The lack of adequate controls to prevent an IT Resource from becoming compromised. A weakness in a system allowing possible or actual unauthorized action.

Information below is not included as part of the contents of the official policy. It is provided only as a convenience for readers/users and may be changed at any time by persons authorized by the president.

RESOURCES

Procedures

- Computer Management Procedures
- Data Management and Storage
- Equipment Management Procedures and Forms
- Cybersecurity Program (under development)
- Technical Incident Response Team Procedures (under development)

Guidance

- Center for Internet Security CIS Critical Security Controls (USHE 2022 selected core cybersecurity framework): https://www.cisecurity.org/controls
- Guidance For Implementing National Security Presidential Memorandum 33 (Nspm-33) On National Security Strategy for United States Government-Supported Research and Development: https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf
- Executive Order 14028, Improving the Nation's Cybersecurity:
  - https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity
  - https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity

Related Forms and Tools

- Equipment Management Forms

Contacts

- USU IT Services: https://it.usu.edu
  - Chief Information Officer, Eric Hawley, (435) 797-1134
  - ISO role, Blake Rich, (435) 797-1134
  - Service Desk, (435) 797-HELP
- Office of Legal Affairs: https://www.usu.edu/legal/
- Office of Research: https://research.usu.edu
- Internal Audit Services: https://www.usu.edu/internal-audit-services/
- List of Data Trustees, Data Stewards, and Support Technicians (under development)

POLICY HISTORY

Original issue date: 2022/03/23

Last review date: 2022/03/23

Next scheduled review date: 2023/Q2

Previous revision dates: 0202/03/23