University Policy 5200: Information Security and Appropriate Use

Category: Facilities, Operations and IT
Subcategory: Information Technology
Covered Individuals: Employees, Students, and Guest Users of IT Resources
Responsible Executive: Chief Information Officer, Executive Vice President & Chief Operating Officer
Policy Custodian: Information Technology, Chief Information Security Officer
Last Revised: 2025/11/07
Previous USU Policy Number: 550: Appropriate Use and 551: Information Security[1]

5200.1 PURPOSE AND SCOPE

The purpose of this Information Security Policy is to establish a comprehensive framework for protecting the confidentiality, integrity, and availability of Institutional Information and Information Technology Resources at Utah State University (USU), safeguarding them from unauthorized access, use, disclosure, disruption, modification, or destruction. This policy enables the university to comply with regulations and maintain a secure environment for administration, academics, and research.

This policy applies to all faculty, staff, students, third parties, vendors, and any other individuals or entities with access to USU's Information Technology Resources and Institutional Information, also known as User(s).

5200.2 POLICY

2.1 Information Security Standards

All users must use the University's Information Technology Resources responsibly and in accordance with applicable laws, regulations, and policies. The use of these resources must align with assigned roles and be in accordance with the capacity and purpose of the resource.

USU maintains security policies, standards, procedures, and best practices to protect Institutional Information and University Systems. These resources are available at https://infosec.usu.edu and are regularly updated to address evolving security threats, compliance requirements, and industry best practices. Users should refer to this repository for required procedures and guidance on implementing security controls, understanding legal obligations, and managing risks effectively.

USU is committed to compliance with all applicable local, state, federal, and international regulations, including but not limited to FERPA, HIPAA, GDPR, GLBA, the Utah Governmental Data Privacy Act (GDPA), the Utah Protection of Personal Information Act, and the Government Records Access and Management Act (GRAMA), as well as internal university policies and procedures governing information security and privacy. Adherence to these requirements is critical to protecting university data, ensuring research integrity, and maintaining operational security. Additional compliance resources are available on the Information Security website.

2.2. Appropriate Use and Terms of Use

[1] Applicable content from Policy 5201 was combined with Policy 5200, creating one new policy. Policy 5201 is retired.

Users are required to adhere to the following Appropriate Use standards whenever they access or interact with the University's Information Technology Resources and Institutional Information:

a. **Access Controls & Authentication:** Access to restricted resources is granted through authentication credentials and controls provided as a privilege tied to a user's role. The university reserves the right to revoke credentials to safeguard resources.

b. **User Responsibility & Security Awareness:** Users are responsible for maintaining the integrity, security, and confidentiality of university resources and data. They must follow instructions from resource administrators and take proactive measures to prevent unauthorized access, such as recognizing phishing attempts, malware risks, and social engineering threats.

c. **Prohibited Activities:** Circumventing security controls, accessing unauthorized systems or data, sharing credentials, or granting unauthorized access to others is strictly prohibited. Users must only access resources and data within the scope of their roles and responsibilities, ensuring compliance with all related policies and procedures.

By accessing the University's Information Technology Resources and Institutional Information, users agree to adhere to these Terms of Use, which define acceptable behavior, security practices, and user responsibilities. These Terms of Use are subject to updates to reflect changes in legal, regulatory, and cybersecurity requirements. Additionally, users must comply with all applicable federal, state, and local laws, including those governing intellectual property, communications, privacy, and the appropriate use of government resources.

2.3 Device and Endpoint Management and Security

All university-owned devices must meet or exceed the security procedures and standards outlined at https://computers.usu.edu. This includes requirements for device configuration, software updates, and endpoint security controls to protect against unauthorized access, malware, and other threats. Access controls must be implemented on all devices to ensure only authorized individuals can access university- owned or -managed data and resources. Employees are responsible for collaborating with their assigned IT staff to ensure their devices meet these security standards.

The use of personal devices to access university data or conduct university business must be limited to ensure the security, privacy, and integrity of institutional information. Employees are encouraged to utilize university-provided devices and services whenever possible. If personal devices must be used, they must comply with the university procedure, as documented on the Device Management Website.

2.4 Data Classification and System Criticality Classification

USU data must be inventoried and classified according to a system that assesses the potential impact of unauthorized access, use, or alteration. This classification framework helps manage risks associated with various types of Institutional Information and supports critical functions such as compliance, information management, vendor oversight, and incident response. Each classification level considers potential impacts on individuals and the university, as well as legal, regulatory, and contractual obligations. While all individuals handling Institutional Information should be aware of its classification and associated safeguards, trustees and stewards must ensure that their teams implement and adhere to appropriate security measures. For more details, refer to the USU Data Classification and System Criticality Classification.

2.5 Security Incident Management

A security incident is any unauthorized access, acquisition, disclosure, loss of access, or destruction of Institutional Information. The significance of a breach is determined by its potential to cause substantial harm or disruption to university resources, stakeholders, affected individuals, or services. This assessment considers various risk factors, including the type and volume of data involved, the number of individuals affected, and the nature of the incident. All users must report Information Security Incidents according to the procedures and timelines outlined at https://infosec.usu.edu. Timely reporting helps mitigate damage, ensures compliance with regulatory requirements, and assists in the swift recovery and investigation of security incidents.

2.6 Vendor Management

Vendors or third-party contractors may access the University's Information Technology Resources or Institutional Information only if an appropriate agreement is established, ensuring compliance with applicable information security and privacy regulations and standards, based on the type of Institutional Information involved. Please consult the University Vendor Management Plan before initiating a contractual process to understand and address the applicable compliance controls.

2.7 Information Privacy

USU is committed to protecting the privacy of Personal Data in compliance with applicable laws, regulations, and standards. Users must handle Personal Data in accordance with the information outlined in the University Privacy Policy and the USU Privacy Website. This includes safeguarding personal information and promoting its confidential, lawful, transparent, and responsible use of Personal Data.

2.8 Artificial Intelligence (AI) Use and Compliance

USU recognizes the growing significance of Artificial Intelligence (AI) in education, research, and operations. The use of AI tools must align with university policies, security guidelines, and ethical standards.

a. **Data Security & Privacy:** Users are responsible for ensuring that sensitive, restricted, or confidential data (including FERPA, HIPAA, Personal Data, and proprietary university information) is not uploaded or processed in AI tools unless the university has an established privacy agreement with the provider. Uploading such data to third-party AI tools without a university-approved privacy agreement may result in security breaches, compliance violations, and legal or institutional liability. Users must understand these restrictions and exercise caution when using AI tools.

b. **Integrity and Accountability:** AI-generated content must be reviewed for accuracy, bias, and compliance with copyright regulations before use in coursework, research, or administrative communications.

c. **Responsible Use:** AI should supplement human decision-making but must not replace critical thinking, academic rigor, or professional judgment.

d. **Institutional Guidance:** Faculty, staff, and students should refer to USU's AI Guidance for official procedures, best practices, and available AI tools.

2.9 Enforcement and Sanctions

Failure to comply with USU's Information Security policies, including but not limited to unauthorized access, data misuse, or failure to report security incidents, may result in disciplinary action. Potential sanctions include loss of access to university IT resources, termination of employment or academic privileges, and, where applicable, legal action. Violations will be investigated in accordance with university procedures, and actions will be determined based on the severity of the infraction.

Disciplinary actions will be enforced in alignment with the following policies:

- USU Policy 3001: Setting Expectations and Managing Performance
- USU Policy 4006: Academic Due Process—Sanctions and Hearing Procedures for Faculty
- Article VI of the Student Code: Governing Procedures for Students

5200.3 RESPONSIBILITIES

The successful implementation and adherence to USU's information security policies require the involvement of various stakeholders across the institution. The following roles outline the responsibilities of specific parties to ensure compliance and protect university assets.

3.1 President's Cabinet, Deans, and Department Heads

The President's Cabinet, Deans, and Department Heads are accountable for fostering a culture of compliance, providing the necessary resources to support information security initiatives, and ensuring that their departments and divisions comply with relevant security policies, procedures, and standards. Additionally, they must promote security awareness and support the enforcement of university-wide security measures.

3.2 Chief Information Security Officer (CISO)

The CISO is responsible for developing, maintaining, and overseeing USU's overarching information security program. The CISO ensures that security standards, procedures, and best practices are documented, updated, and made accessible to support compliance with laws, policies, and evolving security needs. This role includes overseeing the implementation of enterprise security controls and leading responses to security incidents. Additionally, responsibilities include coordinating the assessment of emerging threats and vulnerabilities to drive continuous improvement in security practices and procedures across the university. Collaboration with university departments is a key aspect of this role, ensuring the delivery of effective training and awareness programs related to information security.

3.3 Information Technology and IT Staff

The Information Technology department, along with all campus IT staff, holds primary responsibility for implementing and enforcing technical security controls on university systems. IT staff includes members of the USU Information Technology Department as well as any other USU employees tasked with these responsibilities. Collectively, they are accountable for ensuring robust access control, comprehensive device management, proactive engagement, and timely incident response. This includes the consistent application of security patches, configurations, reporting, and updates in accordance with established university procedures to protect the university's information assets and infrastructure.

Additionally, IT staff manage IT resources, systems, and services that store, process, or transmit Institutional Information. They ensure system security through proper configuration, maintenance, and adherence to best practices, policies, and procedures. By providing technical expertise and supporting the systems under their care, IT staff play a critical role in preserving data integrity, enforcing security standards, and protecting university-owned assets.

3.4 Data Management Roles

3.4.1 Data Trustees are responsible for appointing Data Stewards to manage specific data sets or operational responsibilities, ensuring that data governance is effectively delegated and maintained. They establish and approve governance practices designed to protect and preserve Institutional Information while ensuring alignment with organizational goals and regulatory requirements. Additionally, Data Trustees guide the development of data strategies, ensuring compliance with policies and mitigating risks associated with data management. They also make high-level decisions regarding system procurement, creation, and lifecycle governance to support the organization's overall mission.

3.4.2 Data Stewards Data Stewards are responsible for collaborating with Data Trustees to ensure that operational practices align with data governance strategies, institutional goals, and organizational policies. They inventory, classify, and categorize Institutional Information to maintain an accurate understanding of the data landscape. Additionally, they manage user access permissions based on roles and responsibilities, ensuring compliance with relevant policies, regulations, and contracts. Data

Stewards implement and enforce policies, procedures, and best practices to promote secure and effective data management. They also oversee and approve the lifecycle of Institutional Data, including its collection, transfer, integration, and use, with a focus on maintaining integrity when data is shared across units or with third parties.

3.5 Researchers and Research Administrators

Researchers must comply with university policies, state and federal regulations, and contract and award terms to protect research data, including by working under the proper cybersecurity controls, adhering to export control laws and securing controlled technologies. They are responsible for classifying and safeguarding research data in accordance with university procedures to protect sensitive research, intellectual property, and federally funded projects. Research Administrators assist researchers in fulfilling compliance requirements, working with the Office of Research to secure research data and report any information security incidents. For further guidance on research data security, and export controls, researchers can consult USU's Office of Research.

3.6 Faculty, Staff, and Students

All faculty, staff, and students are responsible for adhering to the information security procedures outlined in https://infosec.usu.edu. This includes following the security protocols for device usage, data protection, and reporting any security incidents. Users are required to comply with data classification procedures and ensure that any confidential or sensitive data they handle is protected in accordance with university standards. Each user is expected to complete any required information security awareness training and to follow best practices for securing their accounts, passwords, and devices.

3.7 Contractors and Vendors

Contractors and vendors with access to university systems or data must comply with the university's information security policies and contractual obligations regarding data protection. Contractors must follow the security protocols outlined in their agreements, including limited use, confidentiality, access controls, data handling procedures, incident reporting, and disposal or return of data. When engaging or planning to procure University Systems through third-party vendors, all units and departments must follow the USU Vendor Management Process.

3.8 Users (General Responsibility)

Users include university employees, faculty, students, agents, contractors, consultants, temporary staff, volunteers, visiting scholars, guests, and affiliated personnel through third-party contractors who are granted access to University Systems, Institutional Information, or resources to fulfill their academic, professional, or contractual responsibilities, or for any other authorized purpose.

Users are responsible for protecting Personal Data and Institutional Information on any devices they use and for ensuring that personal and sensitive information is handled securely. They must safeguard their user-controlled equipment, accounts, and credentials to prevent misuse or compromise.

Users are required to report any information security incidents promptly and follow the procedures outlined at https://infosec.usu.edu. Furthermore, users must adhere to the university's acceptable use policies as outlined in the Terms of Use, as well as any service and access policies established by their units, departments, or USU. Finally, they must comply with all applicable laws, regulations, and university policies governing the use of institutional systems and data.

5200.4 REFERENCES

This policy and its associated procedures are designed to comply with and implement the requirements of the 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. The framework established by this policy is based on current best practices, including the CIS Controls, the NIST Cybersecurity

Framework, and other relevant standards and guidelines. These are intended to secure university information systems, protect personal data, and ensure compliance with applicable legal and regulatory standards.

- Utah System of Higher Education Policy R345, Information Technology Resource Security.
- Protection of Personal Information Act, Utah Code 13-44-101 et seq.
- Center for Internet Security – Critical Security Controls (CIS Controls)
- NIST Cybersecurity Framework

5200.5 RELATED USU POLICIES

- Information Technology Policies (5200-5208)
- Policy 1010: Contract Signature Authority and Delegation
- Policy 2202: Privacy and Security of Protected Health Information under HIPAA
- Policy 4102: Research
- Policy 4103: Protection of Human Participants in Research
- Policy 4106: Intellectual Property
- Policy 4107: Research Data
- Policy 4109: Export Controls

5200.6 DEFINITIONS

- **Artificial Intelligence (AI)**. A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.
- **Capacity of Resource.** Some Resources have a limit that can be exceeded by certain uses, either causing the Resource to underperform or exceed service or license capacity.
- **CIS Controls.** A set of best practices developed by the Center for Internet Security to safeguard systems and data from cyber threats.
- **Chief Information Security Officer (CISO).** A role responsible for developing, maintaining, and overseeing the organization's information security program. The CISO ensures that security standards, procedures, and best practices are documented, updated, and made accessible to support compliance with laws, policies, and evolving security needs.
- **Compromise.** Loss of exclusive, authorized control of an IT Resource to an unauthorized person or unauthorized software, resulting in the exploitation, control, and/or use of the IT Resource beyond USU's purpose or intent for that IT Resource.
- **Credentials.** UserID/PIN, username/passcode or other secrets or keys used to gain access to a restricted Resource.
- **Data Asset Inventory.** A comprehensive list of data assets owned or managed by an organization, used for classification and protection purposes.
- **Data Stewards.** Management-level officials (e.g., Controller, Registrar, Directors, Managers, Principal Investigators) who have operational responsibility for specific data or services that may contain sensitive information. They coordinate with Data Trustees, classify data, authorize access, and enforce applicable policies and practices.
- **Data Trustees.** USU Administrative Officers (President, Provost, Vice Presidents, Deans, etc.) with oversight of data in their divisions. Responsibilities include appointing stewards, implementing protective practices, approving data transfers and usage, and designing workflows to reduce risk.
- **Device.** Any electronic equipment, such as laptops, desktops, smartphones, or tablets, used to access, store, or process organizational data.
- **Endpoint Security.** Measures implemented to protect devices such as laptops, desktops, and mobile devices connected to an organization's network from threats like unauthorized access and malware.
- **Export Control Regulations.** U.S. laws that restrict the export of certain sensitive technologies, information, and software, particularly those related to defense and national security.
- **Incident Management Plan.** The process of reporting any event that compromises the security

of information systems, including data breaches and unauthorized access.

- **Institutional Data.** Refer to Institutional Information.
- **Institutional Information.** Information collected, created, maintained, shared with, or generally managed by Utah State University (USU) in support of academic, research, administrative, or operational functions. This includes data in all formats and media and encompasses both personal and non-personal data.
- **Information Technology (IT).** Refers to the systems, services, personnel, and resources involved in managing the university's computing, networking, and digital infrastructure.
- **Information Technology Resources.** Any service, data, or device provided by or on behalf of the University, including networks, infrastructure, devices, applications, and storage.
- **NIST Cybersecurity Framework.** A set of standards, guidelines, and practices developed by the National Institute of Standards and Technology to help organizations manage and reduce cybersecurity risks.
- **Personal Data.** Also known as Personally Identifiable Information (PII), this includes any information that can be used to identify an individual. This includes both Direct Identifiers (e.g., name, ID number) and Indirect Identifiers (e.g., ZIP code, gender, age) that can reveal an individual's identity when combined.
- **Privilege.** While access is generally granted to everyone in a relevant role, the University retains the right to revoke that access to protect the Resource from misuse or overuse.
- **Research Administrators.** University staff who manage compliance requirements related to sponsored research and regulatory areas. They coordinate with institutional offices and the CISO to secure research data and report incidents.
- **Resource.** Refer to Information Technology Resources.
- **Resource Owners.** Individuals directed to establish and communicate procedures and access controls specific to the Resource they manage, aligning with policy objectives.
- **Resource Users.** Individuals who use a Resource and are responsible for complying with policies and procedures associated with that Resource.
- **Restricted Resources.** Resources available only to individuals in particular roles, unlike public resources such as the USU homepage.
- **Role.** A category of user who is given access to a particular restricted Resource; may range from general (e.g., student) to specific (e.g., advisor).
- **System Administrators or Support.** IT professionals responsible for managing systems and services that store, process, or transmit sensitive data. They ensure technical security, system preservation, and compliance with best practices and policies.
- **Terms of Use.** A document outlining acceptable behavior, responsibilities, and practices that users must agree to in order to access and use organizational resources.
- **Third-party.** Any external entity that interacts with the institution but is not directly part of it, including vendors, collaborators, and government agencies.
- **University Systems.** Any software, hardware, network, or cloud-based system used to gather, process, transmit, or store data in support of university operations.
- **User.** Any individual or organization granted access to University Systems, including students, faculty, staff, contractors, volunteers, and affiliated personnel. Users are expected to comply with policies, report incidents, and follow university security guidelines.
- **Vendor Management Plan.** A structured approach to managing third-party vendors and service providers to ensure they meet operational, security, and compliance requirements. It includes evaluation, contracting, monitoring, and risk management processes.

Additional definitions of key terms related to USU's Information Security Program may be found in the Glossary section on the USU Information Security Program website.

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

- Information Security Program: https://infosec.usu.edu
- Device/Endpoint Management: https://computers.usu.edu
- Data Asset Inventory: https://datacensus.usu.edu
- Research Data: https://research.usu.edu/compliance/
- Artificial Intelligence: https://ai.usu.edu
- Data Management and Storage
- Equipment Management Procedures and Forms

Guidance

- Center for Internet Security CIS Critical Security Controls (USHE 2022 selected core cybersecurity framework):
- NIST Cybersecurity Framework
- Guidance For Implementing National Security Presidential Memorandum 33 (Nspm-33) On National Security Strategy for United States Government-Supported Research and Development
- Cybersecurity Maturity Model Certification (CMMC) Program
    - https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity- model-certification-cmmc-program
    - https://www.defense.gov/News/Releases/Release/Article/3932947/cybersecurity-maturity-model- certification-program-final-rule-published/
- 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
    - Chief Information Security Officer, Allen Hill
    - Service Desk, (435) 797-HELP
- Office of Legal Affairs
- Office of Research
- Internal Audit Services
- List of Data Trustees, Data Stewards, and Support Technicians (under development)

POLICY HISTORY

Original issue date: 2022/03/23

Last revision date: 2025/11/07

Next scheduled review date: 2026/05/01

Previous revision dates: 2022/03/23; 2025/06/20