# 2.3.020
# Information Security Policy

Date of last board of trustees review: February 15, 2023

The originator of this policy is the Office of Information Technology. Questions regarding this policy may be directed to the originator by calling 801-957-4042.

## 1. Policy

Salt Lake Community College keeps personal information about its students, employees, and others, as well as proprietary institutional data essential to its mission and effective operation. This policy sets requirements for all employees, students, and college administrative units to comply with applicable laws and provide necessary security standards to protect the privacy rights of college community members and ensure the integrity of college information assets, systems, and resources.

## 2. References

A. Family Educational Rights and Privacy Act of 1974 (FERPA), 20 U.S.C. § 1232g.

B. 45 C.F.R. 164: Health Insurance Portability and Accountability Act (HIPAA): Security and Privacy.

C. 16 C.F.R. 313: Graham-Leach-Bliley Act.

D. Utah System of Higher Education Information Technology Resource Security R 345.

# 2.3.020
# Information Security Procedure

Date of last executive cabinet review: November 5, 2022

The originator of this procedure is the Office of Information Technology. Questions regarding this procedure may be directed to the originator by calling 801-957-4042.

## 3. Definitions

A. Audit Log: a chronological sequence of audit records that provide documentary evidence of a sequence of activities from the execution of a business process or system function.

B. Authentication Credentials: user identification (ID) and personal identification number (PIN), username and password, or other secrets or keys used to gain access to a restricted resource.

C. College Entity: any administrative unit of the college including school, department, or division.

D. Computer Asset: any college-owned information asset or IT resource that is a part of college business processes.

E. Computer Resource: any electronic hardware or software that makes the storage or use of information possible.

F. Electronic Resource: any resource used for electronic communication, including but not limited to the internet, e-mail, and social media.

G. Encryption: information altered using a code or mathematical algorithm to make it unintelligible to unauthorized persons.

H. Firewall: a device or program that controls network traffic flow between networks or hosts that employ disparate security policies.

I. Information Asset: data or knowledge stored in any electronic manner and recognized as having value for the purpose of enabling the college to perform its business functions.

J. Information Security Incident: an event or weakness that jeopardizes the confidentiality, integrity, and availability of the college's information assets, IT resources, and information systems.

K. Information Systems: an application or group of servers used for electronic storing, processing, or transmitting any college data or information asset.

L. IT Resource: Any computer resource used to perform college business operations including, but not limited to, the creation, access, storage, processing, and transmission of information assets. (i.e., server, workstation, mobile device, networking device, web camera, etc.).

M. IT Technician: a college employee who uses industry best practices to develop, administer, manage, and monitor computer resources and assets that support the college's IT infrastructure and ensure compliant IT system security.

N. Office of Information Technology ("OIT"): College department responsible for all management of college computer assets and security of information assets.

O. Remote Access: access to information assets from any location outside of the college's network or physical boundaries.

P. Restricted Resource: a resource available only to individuals in particular roles within the college community who handle critical data.

Q. User (Authorized User): Any person, including students, staff, faculty, permanent and temporary employees, contractors, vendors, research collaborators, and third-party agents, who accesses any college electronic resources, information systems, or IT resources.

R. Vulnerability: an asset weakness that can be exploited to allow unauthorized access and cause harm to the asset.

## 4. Procedures

A. General

1. User Responsibilities

a. All college entities and users must:

(1) implement reasonable practices to identify and protect information assets, information systems, and IT resources;

(2) maintain an inventory of all IT resources that store, process, and transmit information assets;

(3) follow the Risk Management department's contract review process, including information security evaluation of a third-party vendor's information resources;

(4) only install properly licensed and approved software on IT resources;

(5) follow the security controls, access restrictions, data handling procedures, and security plans for each work area;

(6) take reasonable precautions to reduce the risk of loss of college resources on personal electronic resources.

b. Users who use a cloud computing service must follow all security controls, access restrictions, data handling procedures, and security plans as all other college computer systems.

B. Enforcement

1. If any user violates this policy, other information technology policy, or department rule, the College's Information Security Office (ISO) may:

   a. discontinue user service or revoke user access; and

   b. contact Employee Relations and the user's supervisor about the policy violation which may result in corrective action.

C. Authentication Credentials

1. Only authorized users may physically, electronically, or otherwise access computer assets.

2. Users must:

   a. create strong credentials;

   b. protect credentials from use by others;

   c. never share credentials with others;

   d. provide authentication credentials to access any computer resource that stores, processes, or transmits any college information asset; and

   e. use multi-factor authentication credentials for initial access to all IT resources and after a period of inactivity.

3. Users with restricted resource access authorization must use additional authentication credentials.

4. OIT limits each user's resource access to the lowest privilege principle necessary for the user's job function.

5. OIT monitors and audits access to college resources to prevent unauthorized access through the access requirements on the Credentials Rule Requirements webpage.

6. OIT may revoke credentials from users who violate access control requirements.

D. Security Controls

1. General

   a. All users must:

      (1) use OIT approved functioning and up-to-date antivirus and anti-malware programs on resources;

      (2) install all relevant security patches;

(3) enable resources' firewalls prior to accessing the internet;

(4) store personally identifiable information only on college-approved and encrypted resources; and

(5) follow reasonable security measures to prevent resource theft.

2. Physical and Facility Security

   a. OIT assesses resources and information systems risk and imposes safeguard requirements in the Physical and Facility Security Rule.

   b. OIT must align physical and facility safety requirements with current Center for Internet Security industry standards.

3. Digital Security

   a. OIT imposes baseline security settings for IT resources and information systems based on the OIT malware risk assessment per the IT Resource and Information Security System Security and Vulnerabulity Management Rule.

   b. Users managing any college computer assets must:

      (1) protect any computer assets under their management from compromise;

      (2) configure the computer assets to reduce vulnerabilities to a minimum;

      (3) periodically:

         (a) verify audit and activity logs;

         (b) examine performance data; and

         (c) check for evidence of unauthorized access, the presence of viruses or other malicious code;

      (4) cooperate with ISO by:

         (a) providing support for review of administrative activities; and

         (b) performing penetration testing and real-time intrusion detection.

4. Remote Access

   Users with remote access privileges to the college's network are required to maintain access and security levels equivalent to the users' on-site connection per the Remote Access Rule.

5. Security Incident Response and Handling

   a. Users must immediately report any suspected resource theft to the college's Department of Public Safety and OIT.

   b. Users must report any suspect college resource loss to their supervisor and OIT

within 24 hours.

c. Users must immediately report any suspected or actual information security incident to the college's Information Security Officer.

d. ISO will consult with the Office of Risk Management if any suspected or actual breach involving personal or financial information occurs.

e. If unauthorized release of private information occurs, the college will comply with reporting and disclosure requirements as required by law or industry standards in addition to the procedures set forth in the Information Security Incident Response Management Rule.

E. Change Management

OIT must authorize, test, document, and approve all changes to computer assets that store, process, transmit, or maintain critical data before implementation per the Change Management Requirements Rule.

F. Data Classification, Handling, and Encryption

1. The Office of Institutional Effectiveness and the Data Governance Council (DGC) establishes and maintains data classifications in the Data Governance Policy.

2. OIT establishes and regularly reviews data handling and encryption requirements outlined in DGC's Data Classification Guidelines.

3. IT Technicians must establish, document, implement, and manage data handling and management procedures for the IT Resources and Information Systems they administer.

G. Critical Data and Personally Identifiable Information

1. Users must not knowingly keep personally identifiable information on resources, including, but not limited to:

a. social security numbers;

b. financial information such as credit card numbers;

c. protected health information such as medical records; and

d. other types of personally identifiable information as set forth in USHE Information Technology Resource Security Rule 345.

2. Users must use established departmental procedures to transmit, exchange, or destroy personally identifiable information on computer resources when the information is no longer needed to conduct college business.

3. Only authorized users who have legitimate business may collect or access critical data.

4. Authorized users who access critical data must:

a. sign a confidentiality agreement before OIT grants access; and

b. complete confidentiality training.

H. Log Management and Monitoring

OIT configures all college computer assets to record and monitor information security incidents, events, and weaknesses in audit logs per the requirements forth in the Log Management and Monitoring Rule.

I. Backup and Recovery

OIT establishes routine backup procedures which provide for timely restoration and recoverability of information assets per the Data Classification and Encryption Rule and the Backup and Recovery Rule.

J. Business Continuity and Disaster Recovery Planning

1. The OIT must develop and periodically review, test, and update:

   a. a formal, documented, business-continuity and disaster recovery plan that incorporates information security requirements; and

   b. formal, documented procedures to facilitate the implementation of the contingency plans.

   c. OIT must base information security requirements on business impact analysis that addresses purpose, scope, roles, responsibilities, management commitment, coordination among college administrative units and entities, escalation procedures and compliance, per the requirements in the set forth in the Business Continuity and Disaster Recovery Rule.

K. Information Security Awareness Training

1. All college employees must annually complete information security awareness training.

2. College employees with significant Information System security roles must complete additional security training.

3. OIT will not issue initial restricted resource authorization until employees have completes the initial additional training.

4. The Information Security Director must develop and employ the Information Security Awareness Training to identify information system vulnerabilities and address threats to the information system and ensure it is current and compliant with:

   a. legal requirements;

   b. security industry standards and best practices regarding practices;

   c. data management techniques; and

d. emerging technologies.