College of Southern Idaho Campus Procedures and Guidelines

2025-2026

COLLEGE OF SOUTHERN IDAHO CAMPUS PRACTICES AND PROCEDURES

This document outlines the College of Southern Idaho's practices and procedures related to campus technology. In instances where practices and procedures are directly connected to the College of Southern Idaho Employment Policies and Operational Policies, as approved by the College of Southern Idaho Board of Trustees, the appropriate Policy is identified. In these instances, the practices and procedures outlined in this document are intended to add clarity and additional information related to the specific Policy. In instances where practices and procedures are not directly linked to a policy, the information in this document is intended to provide information regarding the accepted practices and procedures of the College. Employees of the College of Southern Idaho are expected to follow all College policies, practices, and procedures. Nothing in this document should be construed to run contrary to the Board approved Employment Policies and Operational Policies, as those policies supersede language in this document.

Final decisions on practices and procedures are always the purview of the President.

Updates to these procedures can be made as needed by the identified department responsible. Changes should be (1) initiated through standard reporting lines (2) brought to Cabinet for awareness (3) updated (with revision date) on the official posted copy at www.csi.edu

Finalized: April 2026

Office of Information Technology Practices and Procedures

Responsible Departments: Office of Information Technology
Contact Information: Chief Information Officer

Introduction – Purpose, Authority, and Governance Structure
Section 1 – Acceptable Use of Institutional Technology
Section 2 – Official College Communications
Section 3 – Institutional Social Media Governance
Section 4 – Information Governance and Data Protection
Section 5 – Technology Procurement and Application Governance
Section 6 – Artificial Intelligence Governance
Section 7 – Cybersecurity Awareness and Training
Section 8 – Enterprise Architecture and System Standards
Section 9 – Technology Asset Lifecycle and Inventory Management
Section 10 – Identity and Account Governance
Section 11 – Records Retention and Public Records
Section 12 – Review and Document Maintenance
Section 13 – Exceptions and Administrative Authority

Introduction

1. Purpose

The Office of Information Technology (OIT) provides enterprise technology services that support the academic, administrative, and operational functions of the College of Southern Idaho. These practices and procedures establish expectations for the governance, acquisition, management, integration, protection, and appropriate use of institutional technology resources.

These practices and procedures are intended to promote responsible use of institutional technology, ensure operational continuity, support regulatory compliance, and maintain a secure, reliable, and integrated technology environment.

2. Authority

These practices and procedures are issued under the authority granted to the Chief Information Officer by the College of Southern Idaho Board of Trustees in the Information Technology Policy Statement (Effective June 2023).

Pursuant to that Board-approved policy, the Office of Information Technology is responsible for ensuring that the College maintains secure, reliable, and compliant information technology services; supports academic and administrative operations; and implements industry best practices in technology governance and system management.

Under this delegated authority, the Chief Information Officer establishes and maintains the operational standards, practices, and procedures necessary to manage institutional technology systems, safeguard institutional data, and support regulatory and legal compliance requirements.

3. Governance Structure

The Chief Information Officer is responsible for oversight and coordination of the College's enterprise technology environment, including infrastructure, enterprise systems, institutional data platforms, and cloud-based services.

Enterprise technology standards and institution-wide technology initiatives are established by OIT, with advisory input and endorsement from the Technology Council. The Technology Council serves as a cross-functional advisory body providing institutional guidance regarding enterprise technology priorities, standards, and long-term planning.

These practices and procedures apply to all employees, students, contractors, and third-party users who access, manage, or utilize College-owned or College-managed technology resources.

Section 1 – Acceptable Use of Institutional Technology

1.1 Purpose

The College of Southern Idaho provides technology resources to support instruction, public service, and administrative operations. These resources are institutional assets and must be used in a responsible, ethical, and lawful manner.

All users of College technology resources are subject to these practices and procedures.

1.2 Definitions

For purposes of this section:

Technology Resources include all College-owned, leased, managed, or contracted systems and services, including networks, servers, computers, mobile devices, enterprise systems, email systems, cloud platforms, software applications, collaboration tools, learning management systems, and data storage environments.

Institutional Data includes any data created, received, maintained, transmitted, or stored in the course of College business, regardless of format or storage location.

Authorized User means any employee, student, contractor, volunteer, or third party granted access to College technology resources.

Credential includes usernames, passwords, authentication tokens, multi-factor authentication devices, and any mechanism used to verify identity for system access.

1.3 Scope

These practices apply to:

- All College-owned devices
- All College-managed systems and platforms
- Personal devices used to access institutional systems
- All institutional data, regardless of storage platform

1.4 Institutional Ownership and Monitoring

Technology resources and institutional data are the property of the College.

Users should not expect personal privacy when using College technology resources. The College reserves the right to access, review, preserve, and disclose institutional data when necessary to:

- Maintain operational continuity
- Protect institutional assets
- Comply with public records laws
- Respond to lawful requests
- Investigate suspected violations
- Maintain system integrity

Monitoring may include review of network activity, system logs, institutional email, and stored data.

1.5 General Responsibilities of Authorized Users

Authorized users are expected to:

- Use technology resources for legitimate academic and institutional purposes
- Protect institutional data according to its classification
- Safeguard credentials and authentication mechanisms
- Comply with copyright, intellectual property, and licensing requirements
- Respect the privacy and rights of others
- Follow established technology procurement and approval processes
- Report suspected misuse or system concerns to the Office of Information Technology

1.6 Credential Protection

Users are responsible for maintaining the confidentiality of their credentials.

Users may not:

- Share login credentials

- Use another individual's credentials
- Attempt to bypass authentication controls
- Access systems or data without

1.7 Cloud Services and External Platforms

Institutional data may only be stored, transmitted, or processed within systems approved by the Office of Information Technology.

Departments and individuals may not independently adopt external software platforms, cloud services, collaboration tools, or applications for institutional business without prior review and approval.

1.8 Generative Artificial Intelligence

The use of generative artificial intelligence tools must comply with institutional standards regarding data privacy, intellectual property, and academic integrity.

Institutional data classified as Restricted or High-Risk may not be entered into external artificial intelligence platforms unless formally reviewed and approved.

1.9 Prohibited Activities

The following activities are prohibited:

- Unauthorized access to systems, accounts, or data
- Installation of unapproved software on College-owned devices
- Introduction of malicious or disruptive software
- Disruption or degradation of network services
- Harassment, discrimination, or intimidation using institutional systems
- Transmission or storage of unlawful content
- Use of College resources for personal financial gain
- Operation of private commercial enterprises using institutional systems
- Political or religious advocacy unrelated to official College business
- Misrepresentation of the College

1.10 Personal and Incidental Use

Limited incidental personal use is permitted if it:

- Does not interfere with work or academic responsibilities
- Does not consume excessive institutional resources
- Does not create institutional liability
- Does not violate law or College standards

1.11 Compliance and Enforcement

Failure to comply with these practices and procedures may result in:

- Additional corrective measures as necessary to protect institutional systems and compliance obligations
- Administrative review
- Disciplinary action consistent with applicable employee procedures
- Additional corrective measures

The Office of Information Technology may take immediate action to protect institutional systems and data when misuse, non-compliance, or risk to the institution is identified.

Section 2 – Official College Communications (Email, SMS, Institutional Messaging Governance)

2.1 Purpose

The College of Southern Idaho designates specific communication platforms as official institutional communication channels to ensure consistency, legal compliance, operational integrity, cybersecurity protection, and appropriate record retention.

This section establishes governance standards for the use of College-issued email accounts, approved messaging platforms, and institutional SMS systems.

2.2 Scope

This section applies to:

- All employees
- Emeritus faculty and staff
- Contractors and volunteers issued College accounts
- Any user authorized to communicate on behalf of the College

It applies to:

- CSI-issued email accounts
- Institutionally approved messaging systems
- Mass notification systems
- Official SMS platforms
- Any communication system designated by OIT as an institutional channel

2.3 Official Email as Institutional Record

All CSI-issued email accounts are official institutional communication tools.

All email communications created, received, stored, or transmitted through CSI email systems are considered institutional records and may be subject to disclosure under the Idaho Public Records Act and other applicable public records laws.

Email accounts are the property of the College. The College reserves the right to access, review, preserve, and disclose email content when necessary to:

- Comply with legal or regulatory requirements
- Respond to public records requests
- Support institutional investigations
- Maintain operational continuity

Users should not expect personal privacy when using CSI email systems.

Once the College receives notice of a public records request, legal hold, audit, or investigation, employees must not delete, alter, or destroy emails that may be responsive. This obligation applies regardless of storage location.

2.4 Acceptable Use of College Email

CSI email accounts must be used primarily for official College business.

Limited incidental personal use is permitted only if it:

- Does not interfere with job responsibilities
- Does not create institutional liability
- Does not conflict with College standards
- Does not involve personal commercial activity

The following are prohibited:

- Auto-forwarding CSI email to external personal accounts without OIT approval
- Use of CSI email for private commercial ventures
- Political or religious advocacy unrelated to official College business
- Distribution of Restricted, High-Risk, or Moderate-Risk data without authorization
- Sharing login credentials
- Circumventing authentication controls

2.5 Email Security Requirements

To maintain the integrity of institutional systems, users must:

- Maintain strong authentication credentials in accordance with institutional standards
- Utilize multi-factor authentication where required
- Safeguard login credentials
- Report phishing emails, suspicious links, or compromised accounts to

OIT immediately

Authentication standards are governed under Section 10 – Identity and Account Governance.

2.6 SMS and Text Messaging Governance

Institutional business conducted via SMS or text messaging must utilize College-approved messaging platforms when:

- Communicating in an official capacity
- Issuing institutional notifications
- Sending mass communications
- Handling data classified as Moderate-Risk or higher

SMS communications conducted through institutional systems are considered public records and subject to retention requirements.

2.7 Mass Communication and Official Notices

All mass institutional communications must utilize designated College systems to ensure:

- Accessibility compliance (Title II ADA)
- Consistent branding and messaging
- Proper record retention
- Security and authentication integrity

Departments may not deploy independent mass-email or messaging systems without OIT review and approval.

2.8 Monitoring and Auditing

The Office of Information Technology may conduct monitoring and periodic review of institutional communication systems to:

- Identify misuse
- Detect security threats
- Ensure compliance with institutional standards

Monitoring authority aligns with Section 1 – Acceptable Use of Institutional Technology and related operational procedures.

2.9 Account Deactivation

Upon separation of employment, access to institutional communication systems will be modified or deactivated according to established account lifecycle procedures.

Access to former employee email accounts may be retained temporarily when required for operational continuity, legal hold, or public records compliance.

2.10 Compliance and Enforcement

Failure to comply with official communication standards may result in:

- Restriction or suspension of access to institutional communication systems
- Administrative review
- Disciplinary action consistent with applicable employee procedures, including termination for repeated violations
- Additional corrective measures as necessary to protect institutional records and compliance obligations

The Office of Information Technology may take immediate action to preserve institutional records, ensure regulatory compliance, or protect system integrity.

Section 3 – Institutional Social Media Governance

3.1 Purpose

The College of Southern Idaho recognizes social media platforms as official communication channels when used to represent the institution, its departments, programs, or initiatives.

This section establishes governance standards for the creation, management, and use of institutional social media accounts and provides guidance for employee personal use of social media when affiliated with the College.

3.2 Scope

This section applies to:

- All official institutional social media accounts
- All employees managing or contributing to institutional social media content
- Employee personal social media use when identifying affiliation with the College
- Use of College-owned devices or networks to access social media platforms

For purposes of this section, social media platforms include, but are not limited to:

- Professional or social networking sites (e.g., Facebook, LinkedIn)
- Message boards or online forums (e.g., X/Twitter, Reddit)
- Photo and video sharing platforms (e.g., YouTube, Instagram, Snapchat, TikTok)

3.3 Official Institutional Accounts

Any social media account representing the College, a department, program, or institutional initiative must:

- Be approved through appropriate institutional channels
- Be coordinated with the Office of Marketing and Communication
- Comply with institutional branding standards
- Use institutionally managed credentials
- Maintain continuity of access during personnel transitions

Official institutional social media accounts are considered institutional communication platforms and are subject to public records requirements and applicable retention standards as outlined in Section 11 of this document.

Access credentials for official accounts shall not be tied solely to a single individual's personal email address.

3.4 Content Standards

Content published through official institutional accounts must:

- Comply with applicable federal and state law
- Adhere to Title II ADA digital accessibility requirements
- Protect institutional data in accordance with Section 4 – Information Governance and Data Protection
- Be reviewed for accuracy and appropriateness prior to publication

Artificial intelligence tools used to generate social media content must comply with Section 6 – Artificial Intelligence Governance. Human review is required prior to publication of AI-generated content on official accounts.

3.5 Institutional Data and Confidential Information

Employees shall not post or disclose Restricted, High-Risk, or Moderate-Risk institutional information on social media platforms unless expressly authorized and compliant with institutional standards.

This includes, but is not limited to:

- FERPA-protected student information
- Personnel records
- Financial information
- Authentication credentials
- Nonpublic institutional data

3.6 Personal Use of Social Media

This subsection applies to employees using social media for personal use.

Employees should avoid creating confusion regarding whether a personal social media account is officially connected to the College.

If an employee identifies themselves as affiliated with the College, they must ensure that:

- Views expressed are clearly personal
- The account cannot reasonably be construed as representing the official position of the College
- They are not acting in their official capacity as a College employee

Employees may consider including a disclaimer such as:

"While I am an employee at CSI, comments made on this account are my own and do not reflect the official views of the College."

Personal use of social media must not:

- Interfere with or disrupt assigned duties
- Disclose Restricted, High-Risk, or Moderate-Risk institutional information
- Create institutional liability
- Misrepresent the College

Personal social media accounts must be associated with a personal email address rather than an official CSI email account, except where platforms are institutionally approved or contractually linked.

Use of social media on College-owned devices or networks eliminates any expectation of personal privacy and may subject activity to disclosure under applicable public records laws.

While employees retain rights of personal expression, such expression does not relieve employees of responsibility for conduct that materially interferes with institutional operations, compliance obligations, or professional responsibilities.

3.7 Crisis and Official Statements

Employees may not independently issue statements on behalf of the College regarding emergencies, legal matters, or institutional crises unless authorized to do so.

Official institutional messaging shall be coordinated through designated communication channels.

3.8 Monitoring and Oversight

The College may review publicly available content associated with official institutional accounts to ensure compliance with communication, branding, accessibility, and regulatory standards.

The Office of Information Technology may coordinate with the Office of Marketing and Communication to ensure credential continuity, system integrity, and risk mitigation.

3.9 Compliance and Enforcement

Failure to comply with institutional social media governance standards may result in:

- Restriction or suspension of access to institutional communication systems
- Administrative review
- Disciplinary action consistent with applicable employee procedures
- Additional corrective measures as necessary to protect institutional records and compliance obligations

Section 4 – Information Governance and Data Protection

4.1 Purpose

The College of Southern Idaho maintains a structured framework for information governance to ensure that institutional data is classified, protected, accessed, retained, and disposed of in accordance with applicable federal and state law, regulatory mandates, and institutional standards.

Pursuant to the Board-approved Information Technology Policy Statement (Effective June 2023), the Office of Information Technology is responsible for supporting electronic data governance, regulatory compliance, and the secure management of institutional systems.

4.2 Scope

This section applies to:

- All institutional data, regardless of format or storage location
- All employees, students, contractors, and third parties with access to College systems
- All College-owned or College-managed systems, including cloud environments

This section applies whether data is stored:

- On-premises systems
- Microsoft 365 environments
- Azure environments
- Enterprise systems such as SIS, ERP, HR Payroll, CRM, LMS
- Approved third-party or cloud-based applications

4.3 Data Classification

The College classifies institutional information into four categories:

- Restricted Information
- High-Risk Information
- Moderate-Risk Information
- Low-Risk Information

Classification determines the level of protection, access control, storage limitations, and transmission safeguards required.

Restricted Information
Disclosure could cause severe harm to individuals or the College, including criminal or civil liability.

Examples include:

- Credit card numbers
- Certain security system information
- Data subject to stringent regulatory controls

High-Risk Information
Disclosure could cause significant harm or regulatory violation.

Examples include:

- Social Security numbers
- Direct deposit information
- Employee personal information
- User credentials
- Financial account numbers

Moderate-Risk Information
Disclosure could cause limited harm or contractual exposure.

Examples include:

- FERPA-protected student records
- Employee personnel records
- Donor or volunteer information
- Nonpublic financial information

Low-Risk Information
Information approved for public release.

Examples include:

- Course catalogs
- Public website content
- Directory information

- Published intellectual property

4.4 Data Ownership and Stewardship

Each institutional data set shall have a designated Data Owner responsible for:

- Determining appropriate access
- Authorizing use and disclosure
- Ensuring compliance with applicable regulatory requirements

The Office of Information Technology serves as the technical steward of institutional systems and enforces access controls and technical safeguards as authorized by Data Owners.

4.5 Personally Identifiable Information (PII)

Personally Identifiable Information (PII) includes any information that can identify or be linked to an individual.

Examples include:

- Social Security numbers
- Date of birth
- Driver's license numbers
- Financial account numbers
- Biometric data
- Home address or phone number
- Information that may grant access to financial, health, or academic records

PII must be handled in accordance with its assigned classification level and applicable federal and state requirements, including FERPA and other regulatory mandates.

4.6 Data Protection Requirements

All users are responsible for protecting institutional data according to its classification.

At minimum:

- Restricted and High-Risk Information must be stored only within approved institutional systems
- Sensitive data must not be transmitted through unapproved platforms
- Encryption shall be used where required by institutional standards
- Access shall be limited to individuals with a legitimate business need

Operational encryption standards and technical safeguards are established and maintained by the Office of Information Technology.

4.7 Access Logging and Monitoring

Institutional systems that store Restricted, High-Risk, or Moderate-Risk Information must maintain appropriate access logging and monitoring capabilities.

User access activity may be logged and reviewed to:

- Detect unauthorized access
- Support regulatory compliance
- Investigate suspected misuse
- Maintain non-repudiation of system activity

Operational logging standards and review procedures are established and maintained by the Office of Information Technology.

4.8 Data Retention and Destruction

Under the authority granted to the Chief Information Officer pursuant to the Board-approved Information Technology Policy Statement (June 2023), the Office of Information Technology establishes and maintains operational procedures governing system-based retention controls and secure destruction standards.

Institutional data shall be retained in accordance with approved College retention schedules and applicable federal and state law.

Upon expiration of required retention periods, data shall be securely destroyed using recognized industry standards and established operational procedures.

Data destruction activities shall be suspended when data is subject to:

- Legal hold
- Litigation
- Audit
- Regulatory investigation
- Public records request

4.9 Information Privacy and Disclosure

The College will maintain the confidentiality of personal and institutional information to the extent permitted by public records laws.

Disclosure of personal or sensitive information shall occur only:

- To authorized personnel with a legitimate institutional need
- As required by law
- In response to valid legal or regulatory requests
- In accordance with institutional disclosure standards

The College may consult legal counsel prior to releasing sensitive information when appropriate.

4.10 Compliance and Enforcement

Failure to comply with information governance and data protection standards may result in:

- Restriction or suspension of access to institutional systems
- Administrative review
- Disciplinary action consistent with applicable employee procedures
- Additional corrective measures

The Office of Information Technology may take immediate action to mitigate risk, protect institutional data, or preserve evidence in cases involving suspected misuse or regulatory exposure.

Section 5 – Technology Procurement and Application Governance

5.1 Purpose

The College of Southern Idaho maintains centralized governance over technology acquisition to ensure compliance with regulatory requirements, fiscal accountability standards, accessibility mandates, and institutional architecture.

All technology-related purchases must align with College standards prior to acquisition or contract execution.

5.2 Scope

This section applies to all departments, faculty, staff, and affiliated entities using:

- Institutional funds
- Grant funds
- Foundation funds
- Procurement cards
- External funding sources

Technology-related purchases include, but are not limited to:

- Computers and mobile devices
- Software licenses and subscriptions
- Cloud-based services (SaaS, PaaS, IaaS)
- Artificial intelligence platforms
- Servers and storage systems

- Networking equipment
- Audiovisual systems
- IT consulting or professional services
- Any system connecting to CSI's network

5.3 Required Review and Approval

All technology-related purchases must be reviewed and approved by the Office of Information Technology prior to purchase or contract execution.

Enterprise-impacting systems or institution-wide platforms shall be reviewed in consultation with the Technology Council.

The Business Office shall not process technology-related purchases without documented OIT approval.

5.4 Review Criteria

OIT review shall assess:

Cybersecurity Compliance
Alignment with institutional security standards and risk management practices.

GASB Compliance
Proper asset classification, capitalization, and tracking in accordance with Governmental Accounting Standards Board requirements.

ADA Title II Compliance
Accessibility compliance for digital platforms and technology systems.

System Compatibility and Architecture
Interoperability with existing institutional systems and identity infrastructure.

Data Governance
Appropriate handling of institutional data and compliance with classification standards.

Total Cost of Ownership (TCO)
Long-term costs including licensing, maintenance, staffing, training, and support.

5.5 Application Lifecycle Management

All enterprise applications must:

- Have a designated institutional sponsor
- Undergo review prior to deployment
- Comply with institutional data standards
- Follow formal retirement procedures when decommissioned

Operational procedures governing application approval and retirement are maintained by OIT.

5.6 Exceptions

Exceptions may be granted by the Chief Information Officer or designee in consultation with appropriate institutional stakeholders.

Emergency procurements required to mitigate institutional risk may proceed under conditional approval but must undergo post-purchase review.

5.7 Enforcement

Technology purchased without required review:

- May not be supported by OIT
- May be denied network access
- May require removal or replacement
- May result in administrative review
- May result in disciplinary action consistent with applicable employee procedures.

Section 6 – Artificial Intelligence Governance

6.1 Purpose

The College of Southern Idaho recognizes that artificial intelligence (AI), including generative AI technologies, presents both operational opportunities and institutional risk.

This section establishes governance standards for the responsible use, procurement, and oversight of AI-enabled systems in support of academic, administrative, and operational functions.

Pursuant to the authority granted to the Chief Information Officer under the Board-approved Information Technology Policy Statement (June 2023), the Office of Information Technology establishes requirements to ensure AI technologies are implemented in a manner consistent with institutional data protection, regulatory compliance, and enterprise risk management standards.

6.2 Scope

This section applies to:

- All employees
- All AI-enabled software platforms
- All generative AI tools used in the course of institutional business
- AI systems procured, integrated, or deployed for College operations

This includes both institutionally licensed AI platforms and publicly accessible AI tools used for work-related purposes.

6.3 Definitions

Artificial Intelligence (AI) – Systems capable of performing tasks that typically require human intelligence, including analysis, prediction, classification, and decision support.

Generative AI – Systems capable of producing text, images, audio, video, code, or other content based on user prompts, including large language models and similar content-generation technologies.

Institutional Data – Data owned, controlled, or maintained by the College as defined in Section 4 – Information Governance and Data Protection.

6.4 Use of Generative AI Tools

Employees may utilize generative AI tools to support institutional work activities provided such use complies with established data protection, privacy, and procurement standards.

Employees shall not input Restricted or High-Risk institutional data into publicly accessible generative AI platforms unless the platform has undergone institutional review and approval pursuant to Section 5 – Technology Procurement and Application Governance.

Moderate-Risk data may only be used in AI platforms when such platforms meet institutional security and compliance requirements.

AI-generated content must be reviewed and validated for:

- Accuracy
- Bias and appropriateness
- Accessibility compliance
- Regulatory compliance
- Institutional alignment

Use of generative AI does not transfer responsibility for content accuracy or compliance from the employee to the AI system.

6.5 Procurement and Enterprise AI Implementation

Departments may not independently procure AI-enabled software, subscriptions, or integrations without review and approval pursuant to Section 5 – Technology Procurement and Application Governance.

Enterprise AI implementations must be evaluated for:

- Data security controls

- Vendor data retention practices
- Accessibility compliance (Title II ADA)
- System interoperability
- Cost and contractual obligations

The Office of Information Technology retains authority to approve, restrict, or deny AI platform deployment when institutional risk warrants.

6.6 Academic and Instructional Use

Faculty retain discretion regarding instructional use of AI tools in accordance with academic standards and course objectives.

However, all instructional use must comply with institutional data protection requirements and applicable regulatory obligations.

AI use in grading, evaluation, or academic decision-making must include appropriate human oversight.

6.7 Data Protection and Privacy

AI use must comply with the information governance standards outlined in Section 4 – Information Governance and Data Protection.

Employees shall not:

- Upload or expose FERPA-protected student information
- Disclose personnel records
- Share financial, authentication, or restricted institutional data
- Circumvent established access controls

AI platforms that store, process, or retain institutional data may be subject to security review and contractual requirements.

6.8 Public Records and Retention

AI-generated content created or used in the course of institutional business may constitute institutional records and is subject to retention and disclosure requirements under Section 11 – Records Retention and Public Records.

Employees must preserve AI-generated materials when subject to legal hold, audit, or public records request.

6.9 Risk Monitoring and Oversight

The Office of Information Technology may monitor AI platform usage patterns, assess emerging AI risks, and issue guidance regarding approved or restricted tools.

Institutional AI guidance may evolve as regulatory, legal, and technological conditions change.

6.10 Compliance and Enforcement

Failure to comply with artificial intelligence governance standards may result in:

- Restriction or suspension of access to institutional systems
- Administrative review
- Disciplinary action consistent with applicable employee procedures
- Additional corrective measures as necessary to protect institutional systems and compliance obligations

Section 7 – Cybersecurity Awareness and Training

7.1 Purpose

The College of Southern Idaho requires ongoing cybersecurity awareness and training to reduce institutional risk, support regulatory compliance, and promote responsible use of technology resources.

Pursuant to the Board-approved Information Technology Policy Statement (June 2023), the Office of Information Technology is responsible for maintaining a secure and resilient technology environment. Employee participation in cybersecurity awareness initiatives is a critical component of that responsibility.

7.2 Scope

This section applies to:

- All employees with access to institutional systems
- Contractors or third parties granted access to College systems, as determined appropriate

7.3 Training Requirements

All employees with access to institutional email or digital systems are required to:

- Complete assigned cybersecurity awareness training modules
- Participate in periodic phishing simulation exercises
- Comply with established timelines for completion

Training may include modules addressing:

- Phishing and social engineering awareness
- Data protection responsibilities
- Password and authentication standards
- Safe use of institutional systems
- Emerging cybersecurity risks

7.4 Phishing Simulation Exercises

The College utilizes simulated phishing exercises to evaluate employee readiness and improve awareness.

These exercises are designed to:

- Identify areas requiring additional training
- Reinforce appropriate reporting behaviors
- Reduce susceptibility to real-world phishing attacks

Employees who interact with simulated phishing messages may be assigned additional awareness training.

7.5 Reporting Responsibilities

Employees are expected to promptly report suspected phishing emails, suspicious system activity, or potential security concerns to the Office of Information Technology using approved reporting tools.

Timely reporting supports rapid risk mitigation and protects institutional systems.

7.6 Compliance Monitoring

The Office of Information Technology will monitor:

- Completion of required training modules
- Participation in awareness activities
- Organizational trends in phishing simulation results

Supervisors will be notified of employee non-compliance.

7.7 Institutional Responsibilities

The Office of Information Technology will:

- Provide regular cybersecurity awareness training
- Maintain appropriate tracking of participation
- Update training materials to address emerging risks
- Provide guidance and support to departments

7.8 Compliance and Enforcement

Failure to comply with cybersecurity awareness and training requirements may result in:

- Restriction or suspension of access to institutional systems
- Administrative review
- Disciplinary action consistent with applicable employee procedures

- Additional corrective measures as necessary to protect institutional systems and compliance obligations

Section 8 – Enterprise Architecture and System Standards

8.1 Purpose

The College of Southern Idaho maintains enterprise technology standards to ensure that institutional systems are secure, reliable, interoperable, and aligned with organizational objectives.

Pursuant to the authority granted to the Chief Information Officer under the Board-approved Information Technology Policy Statement (June 2023), the Office of Information Technology establishes and maintains enterprise architecture standards and system requirements necessary to support academic, administrative, and operational functions.

8.2 Scope

This section applies to:

- All College-owned or College-managed systems
- All enterprise applications and platforms
- All cloud-based services and hosted environments
- All devices connected to institutional infrastructure
- All systems storing or processing institutional data

8.3 Enterprise Architecture Authority

The Office of Information Technology maintains authority over:

- Enterprise system architecture
- Identity and authentication integration
- System interoperability requirements
- Infrastructure standards
- Technical configuration baselines

All institutional systems must align with established architecture standards prior to implementation or integration.

Enterprise-impacting architecture decisions may be reviewed in consultation with the Technology Council.

8.4 System Standards and Configuration

Institutional systems must adhere to established technical configuration standards to ensure stability, interoperability, and protection of institutional data.

The Office of Information Technology establishes operational standards governing:

- Secure system configuration baselines
- Endpoint configuration requirements
- Server configuration standards
- Administrative privilege controls
- Platform version management

Departments may not alter core system configurations without approval from OIT.

8.5 Encryption and Data Protection Standards

Systems storing or transmitting Restricted or High-Risk Information must implement encryption and data protection measures consistent with institutional standards.

Encryption requirements, key management practices, and related technical controls are established and maintained by the Office of Information Technology.

8.6 Logging and System Monitoring Standards

Enterprise systems that store or process Moderate-Risk, High-Risk, or Restricted Information must maintain appropriate access logging and monitoring capabilities.

Logging standards, retention parameters, and review processes are established and maintained by the Office of Information Technology to support:

- Operational integrity
- Regulatory compliance
- Investigation of suspected misuse
- System accountability

8.7 Vulnerability and Patch Management Standards

All College-managed systems and devices must comply with institutional patch management and vulnerability remediation standards.

The Office of Information Technology establishes operational procedures governing:

- Vulnerability assessment
- Patch prioritization
- Deployment schedules
- Change management coordination
- Monitoring and reporting

Employees are responsible for complying with update requirements for devices assigned to them.

8.8 Administrative Privilege Management

Administrative and elevated system privileges shall be limited to authorized personnel with a legitimate operational need.

The Office of Information Technology establishes standards governing:

- Assignment of administrative rights
- Review and approval of privileged access
- Monitoring of privileged account activity
- Revocation of privileges when no longer required

8.9 System Integration and Interoperability

All institutional systems must support integration with the College's identity infrastructure and designated systems of record when applicable.

Systems that cannot integrate appropriately with institutional authentication or data standards may be denied approval.

Integration requirements are evaluated during procurement and implementation in accordance with Section 5 of this document.

8.10 Compliance and Enforcement

Failure to comply with enterprise architecture and system standards may result in:

- Restriction or suspension of access to institutional systems
- Administrative review
- Disciplinary action consistent with applicable employee procedures
- Additional corrective measures as necessary to protect institutional systems and compliance obligations

The Office of Information Technology may take immediate action to mitigate system risk, preserve system integrity, or enforce established standards.

Section 9 – Technology Asset Lifecycle and Inventory Management

9.1 Purpose

The College of Southern Idaho maintains structured oversight of institutional technology assets to ensure accountability, fiscal responsibility, operational continuity, and compliance with applicable regulatory and accounting standards.

Pursuant to the authority granted to the Chief Information Officer under the Board-approved Information Technology Policy Statement (June 2023), the Office of Information Technology establishes standards governing acquisition, tracking, assignment, maintenance, reassignment, and disposal of institutional technology assets.

9.2 Scope

This section applies to:

- All College-owned technology equipment
- All devices purchased with institutional, grant, or external funds
- All network-connected devices
- All servers, storage systems, endpoints, and mobile devices
- Technology equipment assigned to employees

9.3 Asset Tracking and Inventory Control

The Office of Information Technology shall maintain documented methods for tracking institutional technology assets throughout their lifecycle using available institutional tools and processes.

Asset tracking shall include, at minimum:

- Device identification
- Assignment to department or employee
- Location when applicable
- Lifecycle status

Inventory tracking methods may include procurement records, assignment documentation, spreadsheets, system records, or other approved tracking mechanisms.

As institutional resources allow, the Office of Information Technology may implement centralized asset management tools to enhance inventory oversight and reporting capabilities.

Departments shall cooperate with inventory verification processes as requested by OIT.

9.4 Asset Assignment and Accountability

Technology assets assigned to employees remain the property of the College.

Employees are responsible for:

- Safeguarding assigned equipment
- Using equipment in accordance with institutional standards
- Promptly reporting loss, theft, or damage
- Returning equipment upon separation, reassignment, or request

Supervisors are responsible for coordinating recovery of assigned assets upon employee separation or role change.

9.5 Lifecycle Management

The Office of Information Technology establishes lifecycle standards governing:

- Device deployment
- Maintenance and support eligibility
- Hardware refresh considerations

- Software support status
- End-of-life determination

Devices that fall outside of established support standards may be restricted from network access or scheduled for replacement.

9.6 Surplus and Disposal

Technology equipment designated as surplus shall be processed in accordance with applicable state law and institutional procedures.

Disposal of technology equipment must ensure:

- Removal of institutional data
- Compliance with established data destruction standards
- Environmentally responsible disposal when applicable

9.7 Lost or Stolen Equipment

Employees must immediately report lost or stolen devices to the Office of Information Technology.

The Office of Information Technology may take appropriate protective measures, including:

- Disabling system access
- Removing credentials
- Coordinating with appropriate institutional offices

9.8 Network-Connected Devices

Any device connecting to institutional infrastructure must comply with established technical standards.

Unauthorized devices may be denied network access.

9.9 Compliance and Enforcement

Failure to comply with technology asset lifecycle and inventory standards may result in:

- Restriction or suspension of access to institutional systems
- Administrative review
- Disciplinary action consistent with applicable employee procedures
- Additional corrective measures as necessary to protect institutional systems and compliance obligations

The Office of Information Technology may take action necessary to secure or recover institutional assets when required to mitigate institutional risk.

Section 10 – Identity and Account Governance

10.1 Purpose

The College of Southern Idaho maintains structured governance over user identities and system access to ensure appropriate authorization, accountability, and protection of institutional systems and data.

Pursuant to the authority granted to the Chief Information Officer under the Board-approved Information Technology Policy Statement (June 2023), the Office of Information Technology establishes standards governing account provisioning, access control, authentication, monitoring, and account lifecycle management.

10.2 Scope

This section applies to:

- All employee accounts
- All privileged or administrative accounts
- All system and service accounts
- All applications and systems connected to institutional authentication services

This section applies to accounts used to access on-premises systems, cloud environments, enterprise applications, and third-party platforms integrated with College systems.

10.3 Account Provisioning

User accounts shall be provisioned based on documented business need and appropriate supervisory authorization.

Access shall be:

- Role-based where feasible
- Limited to the minimum level necessary to perform assigned duties
- Aligned with the data classification standards outlined in Section 4

The Office of Information Technology is responsible for implementing technical controls governing account creation and access assignment.

10.4 Account Modification and Deactivation

User access shall be modified or revoked promptly when:

- Employment status changes
- Job responsibilities change
- Access is no longer required
- Separation from the College occurs

Supervisors are responsible for timely notification of role changes or separation to ensure appropriate access adjustments.

The Office of Information Technology shall implement procedures to disable or remove access in accordance with established timelines.

10.5 Authentication Standards

Institutional systems shall require secure authentication mechanisms appropriate to the level of data sensitivity.

Authentication standards may include:

- Strong password requirements
- Multi-factor authentication
- Conditional access controls
- Account lockout controls

Authentication requirements are established and maintained by the Office of Information Technology.

10.6 Privileged and Administrative Access

Administrative or elevated access privileges shall be:

- Limited to authorized personnel
- Approved based on documented operational need
- Reviewed periodically
- Revoked when no longer required

Privileged account activity may be logged and monitored in accordance with institutional standards.

10.7 Credential Protection

Employees are responsible for safeguarding authentication credentials.

Employees may not:

- Share passwords or authentication tokens
- Use another individual's credentials
- Circumvent established authentication controls

Compromised credentials must be reported immediately to the Office of Information Technology.

10.8 Access Logging and Review

User access activity may be logged and reviewed to:

- Verify appropriate system use
- Detect unauthorized access
- Support regulatory compliance
- Investigate suspected misuse

Logging and monitoring standards are governed under Section 8 of this document.

10.9 Account Reviews

The Office of Information Technology may conduct periodic access reviews to validate:

- Continued business need
- Appropriate privilege levels
- Compliance with role-based access standards

Supervisors may be required to certify employee access during review cycles.

10.10 Compliance and Enforcement

Failure to comply with identity and account governance standards may result in:

- Restriction or suspension of access to institutional systems
- Administrative review
- Disciplinary action consistent with applicable employee procedures
- Additional corrective measures as necessary to protect institutional systems and compliance obligations

The Office of Information Technology may take immediate action to disable or restrict accounts when necessary to mitigate institutional risk.

Section 11 – Records Retention and Public Records

11.1 Purpose

The College of Southern Idaho maintains records retention practices to ensure compliance with applicable federal and state laws, support institutional accountability, and preserve records necessary for operational, legal, and historical purposes.

Pursuant to the authority granted to the Chief Information Officer under the Board-approved Information Technology Policy Statement (June 2023), the Office of Information Technology supports the technical implementation of records retention and public records compliance within institutional systems.

11.2 Scope

This section applies to:

- All institutional records created, received, maintained, or stored in the course of College business
- All records stored in electronic systems, cloud platforms, email systems, collaboration tools, and enterprise applications
- All employees responsible for managing institutional records

This section applies regardless of format, including digital, paper, audio, video, or other recorded media.

11.3 Records Retention Requirements

Institutional records shall be retained in accordance with:

- Approved College retention schedules
- Applicable federal and state law
- Regulatory and audit requirements

Retention requirements apply to all official records, including email, electronic documents, databases, and communications conducted through approved institutional systems.

Employees are responsible for ensuring that records under their control are maintained in accordance with established retention schedules.

11.4 Public Records Compliance

Records created or maintained in the course of College business may be subject to disclosure under applicable public records laws.

Employees shall:

- Cooperate with institutional public records request processes
- Preserve requested records when notified
- Refrain from deleting or altering records subject to request

The College may consult legal counsel when responding to public records requests involving sensitive or protected information.

11.5 Legal Hold and Preservation

When litigation, audit, investigation, or public records review is reasonably anticipated or formally initiated, the College may issue a legal hold.

Upon issuance of a legal hold:

- Relevant records must not be altered or destroyed
- Automatic deletion processes may be suspended
- Employees must preserve responsive information

The Office of Information Technology may implement technical measures necessary to enforce preservation requirements.

11.6 Electronic Records and System Retention Controls

Institutional systems may implement automated retention and archiving controls consistent with approved retention schedules.

The Office of Information Technology establishes and maintains operational procedures governing:

- Email retention configurations
- System-based archival processes
- Backup retention practices
- Secure deletion standards

System retention controls shall align with Section 4 – Information Governance and Data Protection.

11.7 Records Destruction

Upon expiration of required retention periods, records shall be destroyed in accordance with established procedures and applicable standards.

Destruction must ensure that:

- Confidential or sensitive information is rendered unrecoverable
- Destruction methods are appropriate to the medium
- Destruction activities are documented when required

Destruction may be suspended when subject to legal hold or regulatory requirement.

11.8 Compliance and Enforcement

Failure to comply with records retention and public records standards may result in:

- Restriction or suspension of access to institutional systems
- Administrative review
- Disciplinary action consistent with applicable employee procedures
- Additional corrective measures as necessary to protect institutional records and compliance obligations

The Office of Information Technology may take action necessary to preserve records, suspend deletion processes, or enforce retention controls when required to mitigate institutional risk.

Section 12 – Review and Document Maintenance

12.1 Purpose

The College of Southern Idaho maintains a structured process for reviewing and maintaining these Practices and Procedures to ensure continued alignment with institutional priorities, regulatory requirements, operational needs, and emerging technology risks.

12.2 Review Authority

Pursuant to the authority granted to the Chief Information Officer under the Board-approved Information Technology Policy Statement (June 2023), the Office of Information Technology is responsible for maintaining and updating these Practices and Procedures.

12.3 Review Cycle

These Practices and Procedures shall be reviewed at least annually by the Office of Information Technology.

Interim reviews may occur when:

- Regulatory requirements change
- Institutional risk conditions change
- Technology environments materially evolve
- Operational improvements are identified

12.4 Consultation

During review cycles, the Chief Information Officer may consult with:

- The Technology Council
- Institutional leadership
- Legal counsel
- The Business Office
- Other relevant stakeholders

Consultation ensures that updates remain aligned with institutional strategy and compliance obligations.

12.5 Revision Authority

The Chief Information Officer may issue revisions to these Practices and Procedures as necessary to:

- Address emerging risks
- Clarify governance standards
- Improve operational alignment
- Strengthen compliance posture

Material structural changes may be communicated to executive leadership as appropriate.

12.6 Operational Procedures

The Office of Information Technology maintains separate operational procedures, standards, and technical guidelines supporting the implementation of these Practices and Procedures.

Operational documents may be updated as needed to reflect evolving technology standards, provided they remain consistent with the governance framework established herein.

12.7 Document Control

The official version of these Practices and Procedures shall be maintained by the Office of Information Technology.

Departments and employees shall rely on the most current published version.

Archived versions may be retained for historical reference and audit purposes.

12.8 Compliance and Enforcement

Failure to adhere to established review and maintenance requirements may result in:

- Restriction or suspension of access to institutional systems
- Administrative review
- Disciplinary action consistent with applicable employee procedures
- Additional corrective measures as necessary to protect institutional systems and compliance obligations

The Office of Information Technology may take appropriate action to ensure continued compliance with these Practices and Procedures.

Section 13 – Exceptions and Administrative Authority

13.1 Purpose

The College of Southern Idaho recognizes that operational realities, resource constraints, or unique institutional circumstances may require limited exceptions to established technology practices and procedures.

This section establishes the authority and framework for reviewing, approving, documenting, and managing exceptions in a controlled and accountable manner.

13.2 Authority

Pursuant to the authority granted to the Chief Information Officer under the Board-approved Information Technology Policy Statement (June 2023), the Chief Information Officer may grant exceptions to specific provisions within these Practices and Procedures when appropriate.

Exception authority is administrative in nature and does not modify Board-approved policy.

13.3 Exception Criteria

Exceptions may be considered when:

- Operational necessity exists
- Regulatory requirements allow flexibility
- Risk is formally evaluated and deemed acceptable
- Budgetary or resource constraints prevent immediate compliance
- Temporary accommodations are required during transition periods

Exceptions shall not be granted when they would result in violation of federal or state law.

13.4 Documentation Requirements

Approved exceptions shall be documented and include:

- The specific provision for which the exception is granted
- The justification for the exception
- The duration of the exception
- Any compensating controls or mitigation measures

Exceptions may be time-limited and subject to periodic review.

13.5 Risk Considerations

When evaluating exception requests, the Office of Information Technology may consider:

- Impact to institutional data protection
- Operational impact
- Regulatory exposure
- Reputational risk
- Financial implications

The Chief Information Officer may require risk mitigation measures as a condition of approval.

13.6 Temporary and Emergency Exceptions

In emergency circumstances requiring immediate operational action, the Chief Information Officer or designee may authorize temporary exceptions.

Such exceptions must be documented as soon as practicable and reviewed for continued necessity.

13.7 Revocation of Exceptions

The Chief Information Officer may revoke previously granted exceptions when:

- Risk conditions change
- Mitigation measures are not implemented
- Institutional priorities require compliance
- Legal or regulatory conditions change

13.8 Compliance and Enforcement

Failure to comply with approved exception conditions may result in:

- Restriction or suspension of access to institutional systems
- Administrative review
- Disciplinary action consistent with applicable employee procedures
- Additional corrective measures as necessary to protect institutional systems and compliance obligations

This completes the full structure of the Office of Information Technology Practices and Procedures document.