SEWANEE
THE UNIVERSITY OF THE SOUTH

INFORMATION SECURITY POLICY

1.0 PURPOSE

The purpose of this policy is to assist the University in its efforts to fulfill its fiduciary responsibilities relating to the protection of information assets and comply with regulatory and contractual requirements involving information security and privacy. This policy addresses key controls in areas needed to provide for the confidentiality, integrity, and availability of the University's information assets. The policy strives to clearly establish the University of the South's role in protecting its information assets, and communicate minimum expectations for meeting these requirements.

In addition, the University has business reasons to collect or handle confidential personally identifiable information (PII) such as Social Security numbers, visa permit numbers, bank account numbers, driver's license numbers, and credit card numbers. The University has a legal and ethical obligation to ensure this data is secured in a manner that minimizes the risk of unauthorized use or disclosure. This data must be protected by University policies, physical measures, and appropriate computer security procedures

2.0 SCOPE

The scope of this policy includes all information assets governed by the University. This includes all users and service providers who have access to or utilize assets of the University, including data at rest, in transit, or in process, and shall be subject to these requirements. This policy applies to all information assets and information technology (IT) resources operated by the University; all information assets and IT resources provided by the University through contracts, subject to the provisions and restrictions of the contracts; and all authenticated users of the University information assets and IT resources. This policy and any associated guidelines are subject to change at the discretion of the University.

3.0 DEFINITIONS

Term	Definition
Cardholder data	At a minimum, cardholder data consists of the full primary account number (PAN). Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date, and/or service code.
Centralized authentication	User information (usernames and passwords) are gathered into a single central repository, and software products direct user authentication to this central repository. This allows for the easy disabling of system access when a user is no longer affiliated with the University.
Chief Information Officer (CIO)	Role held by the Associate Provost for Library and Information Technology Services is known as the CIO. The CIO is a member of the vice-chancellor's cabinet and is responsible for all aspects of Library and Information Technology Services for the University.

Center for Internet Security (CIS)	Center for Internet Security is a community-driven nonprofit, responsible for the CIS controls, and globally recognized best practices for securing IT systems and data.
Confidential Data	Data for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to the University if disclosed or modified. This data may be protected by FERPA, HIPAA, or other laws or standards such as PCI DSS. This term is often used interchangeably with sensitive data.
Customer	As per the Federal Trade Commission's Red Flag Rules, a customer is a person that has a covered account with a financial institution or creditor. For the University, this includes various stakeholders including students, parents, and employees.
Data Custodians	A data custodian is an employee of the University who has administrative and/or operational responsibility over institutional data. Data custodians for the University's educational records are identified in the Education Records and FERPA policy of the University.
Domain Keys Identified Mail (DKIM)	Domain Keys Identified Mail is an email authentication technique that allows the receiver to check that an email was indeed sent and authorized by an organization.
Enterprise Resource Planning System (ERP)	Enterprise Resource Planning (ERP) refers to a type of software that organizations use to manage day-to-day business activities such as accounting, accounts payable, purchasing, payroll, personnel, student records, financial aid, admissions, etc.
FERPA	Acronym for Family Educational Rights and Privacy Act of 1974. The Family Educational Rights and Privacy Act of 1974 is a United States federal law governing access to educational information and records by public entities such as potential employers, publicly funded educational institutions, and foreign governments.
HIPAA	Acronym for Health Insurance Portability and Accountability Act of 1996 (HIPAA). The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that requires the creation of national standards to protect confidential patient health information from being disclosed without the patient's consent or knowledge.
Information Technology (IT)	Information Technology is part of the Library and Information Technology Services division of the University. IT is charged with establishing, monitoring, and maintaining information technology systems and services. IT includes the Technology, Access & Support department and the Strategic Digital Infrastructure department.

Information Technology (IT) Resources	Includes all the University owned, licensed, or managed hardware and software, email domains and related services, and any use of the University's network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.
Internal Use Data	Data that may not be confidential but that the data owner feels should be protected to prevent unauthorized disclosure. Examples might include meeting notes, agendas, or budget documents.
Known bad reputation	Email reputations are a score that is set by Internet Service Providers based on the history of emails sent by the individual user or the organization. Most email providers check databases of known bad senders to block potentially bad emails.
LITS	Library and Information Technology Services is a division of the University that encompasses the library and information technology functions of the University.
Media	Media is defined as any printed or handwritten paper, received faxes, floppy disks, backup tapes, computer hard drive, etc.
Multi-Factor Authentication	Authentication that requires more than one method before authorizing access. These methods should be different types, such as something you have, something you know, and something you are.
National Institute of Standards and Technology (NIST)	The National Institute of Standards and Technology is part of the U.S. Department of Commerce, and it provides standards for controls and best practices in information technology.
PCI DSS	Acronym for the Payment Card Industry Data Security Standards. It sets the operational and technical requirements for organizations accepting or processing payment transactions, and for software developers and manufacturers of applications and devices used in those transactions.
PII	Personally Identifiable Information. This includes, but is not limited to, Banner ID, Social Security numbers, bank account numbers, driver's license numbers, and credit card numbers.
Penetration Testing	A penetration test, also known as a pen test or ethical hacking, is an authorized simulated cyberattack on a computer system, performed to evaluate the system's security.
Private Cloud	A pool of resources at a hosting provider in which the University houses servers that are maintained and configured by staff in the SDI department.
Privileged	A login credential to a server, firewall, or other system which provides access beyond what a normal user has. Privileged accounts are also

	commonly called administrative accounts, and they are used for configuring the system, creating accounts, or granting access.
Public Use Data	Data that may be freely shared and distributed. Examples include the University's external website and data made publicly available by Institutional Research.
Red Flag	A red flag is a pattern, practice, or specific activity that indicates the possible existence of identity theft.
Software As a Service (SAAS)	Software as a Service is software that is provided by a vendor on software not owned or controlled by the University. The University has access to use the software via a subscription service.
SDI	Strategic Digital Infrastructure is a department within the Library and Information Technology Services division of the University.
SDI Procedures Manual	A collection of written procedures for key functions performed by the SDI staff. The procedures help ensure the continued functioning of the department during an employee's absence.
Secure Shell (SSH)	Secure Shell or Secure Socket Shell is a network protocol that gives users and system administrators a secure channel over an unsecure network.
Sensitive Information	Any data, electronic or physical copy, for which the compromise of confidentiality, integrity, and/or availability could have a material adverse effect on the University's interests, the conduct of University programs, or the privacy to which individuals are entitled. Examples of such data would include that data protected by the Family Education Rights and Privacy Act (FERPA), Gramm-Leach-Bliley Act (GLBA), European Union's General Data Protection Regulation (EU GDPR), or other laws governing the use of data or data that has been deemed by the University as requiring protective measures.
Sensitive Personally Identifiable Information	Sensitive personally identifiable information (PII) includes Social Security Number, visa permit number, driver's license, financial information, credit card information, and medical records.
Service Provider	Business entity that is not a payment brand directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. This also includes companies that provide services that control or could impact the security of cardholder data.
Single Sign On (SSO)	Single Sign-on (SSO) is an authentication methodology that allows a user to log in with a single ID to several systems without providing a password for each system they access.
Sender Policy Framework (SPF)	Sender Policy Framework is an email authentication method designed to detect fraudulent sender addresses during the delivery of the email.

Stakeholder	A stakeholder is a person with an affiliation with the University. This includes students, faculty, staff, alumni, retirees, community members, contractors, volunteers, and others.
TAS	Technology, Access & Support is a department within the Library and Information Technology Services division of the University.
Transport Layer Security (TLS/SSL)	Transport layer security is a cryptographic protocol designed to provide communications security over a computer network. It is used in https to secure web browser traffic and is widely used in applications such as email, instant messaging, and voice over IP. It is sometimes referenced as secure sockets layer protocol (SSL) which is an older protocol.
Virtual Private Network (VPN)	Virtual Private Network provides a way for University stakeholders to access University IT resources that aren't available outside of the University's firewall from outside the University's firewall.

4.0 Provisions for Information Security Standards

The University's Security Program is framed by the National Institute of Standards and Technology (NIST) and controls implemented based on the Center for Internet Security Controls priorities. The University has also developed appropriate control standards and procedures required to support this policy. Standards are written and maintained by the Directors of Strategic Digital Infrastructure (SDI), and Technology Access & Support (TAS) and subject to the approval of the Associate Provost for Library and Information Technology Services (hereafter referred to as the CIO) based on industry-recognized security standards.

4.1 Inventory and Control of University IT Assets

- The Library and Information Technology Services (LITS) division maintains an inventory of all University equipment with the potential to store, process, or transmit data. The directors of the SDI and TAS departments are responsible for overseeing and maintaining this inventory.
- Per the University purchasing policy, all purchases of computers, software, and technology equipment must be coordinated with the appropriate LITS department.
- Equipment assigned to University employees must be returned to the SDI or TAS department when an employee leaves the University as per the University's staff and faculty handbooks.
- Any equipment checked out through the IT HelpDesk must be returned by the due date.

4.2 Inventory and Control of University Software

- The Library and Information Technology Services division maintains an inventory of all software containing University data. The directors of SDI and TAS are responsible for overseeing and maintaining this inventory.
- Per the University purchasing policy, all software purchases must be coordinated with the appropriate LITS department.
- Per the University's staff and faculty handbooks, all software, applications, or mobile apps licensed to the University, must be removed from personal devices before an employee's last day of service.

4.3 DATA SECURITY

- Items in this section supplement the University's Education Records and FERPA policy.
- Access
    - Access to information on any media type, both paper and digital, must be limited to only those personnel with a business need to know and with only the least privilege needed.
- Classification
    - Data and media containing data must always be labeled to indicate sensitivity level
        - **Confidential** data might include information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to the University if disclosed or modified. Confidential data includes cardholder data.
        - **Internal Use** data might include information that the data owner feels should be protected to prevent unauthorized disclosure;
        - **Public** data is information that may be freely disseminated.
- Handling of data
    - Data should only be used for authorized business purposes, and all usage must comply with applicable state, federal and international laws, as well as the University's policies governing the appropriate use of technology.
- Protection of Cardholder data
    - In addition to protections outlined in the Acceptable Use Policy, additional protections are required for cardholder data which includes credit and debit cards.
    - All Access to sensitive cardholder data should be controlled and authorized.
    - Any job functions that require access to cardholder data should be clearly defined.
    - Procedures for handling cardholder data have been defined and must be followed.
- Mobile devices
    - Internal use or confidential information can only be stored on University-owned laptops when there is a business need and should be removed when the business need no longer exists.
    - University-owned laptops must be encrypted. End users must not circumvent this encryption.
- Personal devices
    - The University recognizes and allows employees to connect personally owned mobile devices to the University's resources to access and synchronize email data, contacts, and calendar information. All usage must comply with state and federal laws, as well as the University's policies governing the appropriate use of technology.
    - Internal use or confidential University data should never be downloaded or stored on personally owned devices.
    - Employees using personal mobile devices are required to delete any University applications or data stored on their device immediately upon termination of employment (voluntary or involuntary).
- Identity Theft Detection and Prevention
    - As required, the University has an Identity Theft Detection and Prevention Program, which is commonly referred to as the "Red Flag Rules."

    - The CIO will appoint a Program Administrator to be responsible for developing, implementing and updating the University's Identity Theft Detection and Prevention Program. The Program Administrator will also ensure appropriate training is conducted for the program.
    - A data security incident that results in unauthorized access to a customer's account record or a notice that a customer has provided information related to a covered account to someone fraudulently claiming to represent the University or to a fraudulent website may heighten the risk of identity theft and should be considered Red Flags.
    - The detection of a Red Flag by an employee shall be reported to their appropriate administrator and IT-SECURITY@sewanee.edu. Based on the type of red flag, the appropriate administrator, the CIO, and the Director of SDI, together with the employee, will determine the appropriate response.
- Removable media
    - Data stored on removable media must be encrypted.
    - If media is no longer needed, it must be properly sanitized or destroyed before disposal or release for reuse.
- Transport
    - Sensitive data must be encrypted in transit using standard security protocols such as TLS/SSL or SSH.

4.4 SECURE CONFIGURATION

- Baseline Configuration Standards
    - Standards are written and maintained by the Directors of SDI and TAS and are subject to the approval of the CIO.
    - All workstations, servers, software, system components, etc. owned by the University will be configured using defined baseline security configuration standards and must have up-to-date system security patches installed to protect the asset from known vulnerabilities.
    - Information systems that process, transmit, or store cardholder data must also be configured in accordance with the applicable standard for that class of device or system.
- Upgrades and patches
    - University systems must run vendor supported versions.
    - Upgrades and patches should be applied as soon as feasible as per the defined standards.
    - Systems which are running an unsupported version that can't be patched or upgraded to a supported version must be removed from the University's network.
    - The director of SDI or TAS may submit exception recommendations to the CIO for approval. Any approved exceptions are to be documented. Exceptions should only be granted for short term periods and have a defined plan to migrate to a supported version of the same or similar system.
- Mobile devices
    - All University-owned mobile end-user devices should be encrypted and meet the defined security standards of the University.

4.5 Account Management

- The SDI department of LITS is responsible for maintaining the inventory of enterprise-wide University accounts.
- The Director of SDI is responsible for the oversight and approval of the enterprise account maintenance process.
- University stakeholders must adhere to the University's defined security standard for accounts which includes such items as password complexity, multi-factor authentication, and periodic password resets.
- Accounts that remain dormant for 45 days or more are subject to suspension.
- Enterprise applications must be configured to utilize single sign-on or centralized authentication when feasible.
- Separate accounts not used for general computing activities must be used for privileged system administration when feasible.

4.6 Access Control Management

- Access to the University's systems is only given to authorized users based on their role and granted based on a least privilege needed principle.
- Access to University data and its resident information systems will be restricted to those users that have a legitimate business need and appropriate approvals for access to such information.
- All University systems should be configured to use single-sign-on if possible, and, if not, must meet the University standards for passwords and multi-factor authentication.
- Defined data custodians will be responsible for approving security to systems as it relates to their areas of oversight. For example, in the University's Enterprise Resource Planning System:
    - Director of Advancement Services - Donor and Alumni records
    - Assistant Treasurer - Finance
    - Director of Human Resources - Human Resources, Payroll
    - Financial Aid Director - Financial Aid Records
    - Registrar - Non-financial Student Records
    - Director of Strategic Digital Infrastructure - Administrative system functionality or cross-functional area records
- Managers are obligated to notify IT when new employees are hired, existing employees change roles, and employees leave the institution either through processes defined by Human Resources (HR) or by contacting IT directly when HR doesn't have a defined process. IT will use defined procedures to grant and terminate access per these notifications.
- Access will also be terminated upon an employee, retiree, student, or alum's death. Access to any personal files may be requested through the CIO or Director of SDI and would be granted after an appropriate administrator approves. For staff, it is the immediate supervisor, and for faculty or students, it is the Dean of the College or Dean of the School of Theology. The Vice-Chancellor, Provost, General Counsel, or other members of the VC's cabinet may also provide approval as needed.

4.7 Vulnerability Management

- To mitigate potential vulnerabilities, University systems will also be proactively patched and upgraded to minimize risk.

- Wherever possible, systems must have automatic updates enabled for operating system updates and patches released from their respective vendors.
- Security patches should be installed within one month of release from the vendor following the defined change control process.
- The Strategic Digital Infrastructure department is responsible for conducting periodic vulnerability assessments and scans and utilizes the services of third parties. Weakness or vulnerabilities identified will be mitigated in priority order.
- All University stakeholders will be required to assist SDI or TAS personnel with mitigating risks if a vulnerability is identified in a system for which the stakeholder is responsible.

4.8 Audit and Monitoring

- Audit Logs
    - The University has defined procedures to create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity on University systems.
    - The SDI department of LITS is responsible for managing audit logs of students it maintains as per the defined standards.
- Monitoring
    - As per defined, approved standards, the SDI department employs various measures to protect the security and availability of the University's information resources. While the University does not routinely monitor individual usage, it does monitor the normal operation and maintenance of the University's computing and networking resources, including backup, logging of activity, the monitoring of general and individual usage patterns, and other such activities that are necessary for information security and the rendition of service. Users should be aware that their uses of University computers and network resources are not private.
    - Any monitoring will be conducted at the direction of and approval from either the CIO or the Director of SDI.

4.9 Email and Web Browser Protections

- Only approved email clients and web browsers should be used. The TAS department is responsible for maintaining an inventory of approved clients and browsers.
- Email clients and web browsers should be kept up to date with the latest security patches and updates applied in a timely manner.
- Email protections
    - Users or departments wanting to send email from a third party system with a university address must work with the SDI department to utilize email verification tools such as the Sender Policy Framework (SPF) or the DomainKeys Identified Mail (DKIM) standards.
    - The University reserves the right to implement restrictions in email, such as blocking senders with a known bad reputation or blocking risky attachment types.
    - The University also reserves the right to monitor and inspect email to look for issues as needed to protect the confidentiality, integrity, and availability of the University's resources.

4.10 Malware Defenses

- University-owned equipment is configured with malware and virus defense software as per the University's standards.
- End users must not disable or otherwise circumvent the automated updates, firewalls, anti-virus, or anti-malware.
- Exceptions to this policy must be approved by the Director of SDI, the Director of TAS, or the CIO.

4.11 Backup and Recovery

- Backups
    - Accurate and timely backups of the operating system, system, and user files of the file and enterprise application servers of the University which are housed in the data center or in the private cloud administered by the SDI department shall be conducted routinely by the SDI department. Backup of software as a service (SAAS) applications are the responsibility of the hosting entity.
    - Backup of individual University-issued computers is the responsibility of the computer user.
- Recovery of backup data
    - Any restores of data from backups are to be approved by the CIO or the Director of Strategic Digital Infrastructure.
- Disaster Recovery
    - The IT departments have defined an IT Recovery Manual to outline recovery procedures from varying levels of disaster. This manual must be reviewed and updated annually by the departments and approved by the CIO.

4.12 Network Infrastructure Management

- All network device configurations must adhere to the University's required standards before being placed on the network as specified in the University configuration standards.
- Network devices will be checked periodically against the configuration standards, and all discrepancies will be evaluated and remediated by SDI staff.
- Personal devices
    - Personally owned devices can only be connected to the University's network through the wireless network and should never be attached to the wired network of the University.
- Remote Access
    - Only authorized users will be permitted to remotely connect to University information systems, networks, and data repositories to conduct University-related business.
    - The CIO or the Director of SDI will be responsible for evaluating and approving any requests.
    - Users granted permission to access systems remotely must adhere to the standards and procedures defined by the Director of SDI.
- Changes to the University network will be managed and executed according to a change management process identified in the SDI procedures manual.

4.13 Network Monitoring and Defense

- The University's network is designed as per the defined standard to minimize access to internal or confidential information.
- The University reserves the right to review, monitor, and/or capture any content residing on or transmitted over its computers or network at its sole discretion without prior notification or approval of the individual user. It should be emphasized that University stakeholders should have no expectation of privacy when using or communicating through the University's electronic services.
- Any monitoring will be conducted at the direction of and approval from either the CIO or the Director of SDI.

4.14 Awareness and Training (AT)

- All employees of the University are required to participate in security awareness training within thirty days of starting employment and thereafter on an annual basis. This also applies to volunteers and grant-funded affiliates.
- Additional training beyond the general training will also be required for some departments and some job duties. Examples of such departments include IT, the Wellness Center, Financial Aid, and the Treasurer's Office. Examples of job duties include those handling credit cards, such as cashiers.
- Students are encouraged to participate in security awareness training during their first semester at the University and thereafter on an annual basis.
- Students working for the University in any capacity (whether paid or unpaid) are required to participate in security awareness training as any other employee in the department.

4.15 Service Provider Management

- The SDI department is responsible for maintaining an inventory of all suppliers and third-party partners of information systems, components, and services.
- As per the purchasing policy, any department of the University proposing a contract or relationship with an outside vendor that involves University data or information shall work with IT staff to define appropriate access and contract language as per defined standards.

4.16 Application Software Security

- Application Security Administration
    - Each application software system will have a defined security administrator.
    - Security will be defined using a least privilege approach based on a business need to know.
    - The SDI department is responsible for maintaining an inventory of the defined security administrators for all University systems.
- Change Management
    - Changes to information systems shall be managed and executed according to a change management process as identified in the SDI and TAS procedures manuals.
    - The control process will ensure that changes proposed are reviewed, authorized, tested, implemented, and released in a controlled manner; and that the status of each proposed change is monitored.

4.17 Cyber Incident Response

- Cyber Incident Response Procedures
    - The University has established cyber incident handling procedures which define preparation, detection, analysis, containment, recovery, and user response activities. These procedures will be reviewed annually and updated as needed by the directors of SDI and TAS. These procedures will be submitted to the CIO for approval.
- User Responsibilities
    - Any University constituent who discovers a suspected or known cyber security incident or data breach must notify IT immediately by emailing IT-security@sewanee.edu as soon as possible. This includes an observed or suspected security weakness in the University's systems or services.
    - Users must also provide prompt notice to the University's helpdesk upon becoming aware of, or having reason to believe that University information (including email) has, or may have been, lost or compromised as the result of
        - A third party gaining unauthorized access to data stored on their devices; or
        - Inadvertent forwarding or sharing data with unintended recipients; or
        - The theft or loss of their device

4.18 Penetration Testing

To protect the University's assets, the University reserves the right to conduct periodic penetration tests of the University's network and systems. Information obtained in these tests will be used to mitigate risk for the University and its users.
University stakeholders are responsible for working with the LITS departments to mitigate any risks detected.

5.0 Consequences

The University may suspend or block access to any individual account or device when it appears necessary to do so to protect the integrity, security, or functionality of the University and its information technology resources.

Any employee who violates this policy may be subject to disciplinary action, up to and including termination of employment. Any student who violates this policy may be subject to disciplinary action, up to and including suspension from the University.

6.0 Privacy

The University and any contracted vendors must make every reasonable effort to respect a user's privacy. However, stakeholders do not acquire a right of privacy for communications transmitted or stored on University resources.

In addition, in response to a judicial order or any other action required by law or permitted by official organization policy or as otherwise considered reasonably necessary to protect or promote the legitimate interests of the organization, the Director of SDI, or an employee authorized by the CIO, may access, review, monitor and/or disclose computer files associated with an individual's account.

7.0 Exceptions

Exceptions to the policy may be granted by the Chief Information Officer, or his or her designee as designated in this policy.

8.0 Disclaimer

The University disclaims any responsibility for and does not warrant information and materials residing on non-university systems or available over publicly accessible networks. Such materials do not necessarily reflect the attitudes, opinions, or values of the University.

9.0 Related Policies

- Acceptable Use Policy
- Education Records and FERPA Policy
- Purchasing Policy

10.0 Responsibilities

All University stakeholders are responsible for understanding and abiding by this policy. The Library Information Technology Services Division, particularly the CIO, the SDI and TAS departments is responsible for maintaining this policy.

11.0 Policy Authority

This policy is maintained by the Associate Provost for Library and Information Technology Services for The University

12.0 Revision History

Version	Date	Author	Revisions
1.0	September 21, 2022	Various	Initial Policy