Southern Adventist University

Information Security Policy

Version 1 Revised Apr 27 2015

Summary
The purpose of this policy statement is to establish the requirements necessary to prevent or minimize accidental or intentional unauthorized access or damage to Southern Adventist University information resources.

Applicability
This policy applies to all university students, faculty and staff, affiliates, third-party support contractors, and all others granted access to Southern's information resources. All users of information resources bear responsibility for the protection of those assets. Based on system and information classification categories, some categories of users have a greater burden of responsibility and accountability than others.

This policy pertains to all university information resources, whether the resources are individually or departmentally controlled, enterprise managed, stand-alone or networked. It applies to all computer and communication facilities owned, leased, operated or contracted by the university, networking devices, mobile devices, telephones, wireless devices, workstations, portable storage devices and any associated peripherals and software, whether used for administrative, research, teaching or other purposes. It applies to personal devices that are attempting to access, store or maintain university information. This policy also pertains to hard-copy documents that are classified under these guidelines.

Section headings are:

1. Responsibilities

Adherence to the principles of information security set forth in this policy requires the participation and involvement of the entire university community. In particular,

state law (Tenn. Code Ann. §§ 47-18-2105 to -2107 (2005)) mandates that the university notify individuals when there is a breach of the security of system information or written material that contains their "personally identifiable information," as defined by the law. Because of the legal requirement to protect this information, such personal information should be treated as Restricted Information. Southern employees who are aware of any attempted or actual breach are required to report the incident to the Information Systems Department for investigation and potential breach notification.

Within the framework of these principles, the responsibilities of those in key positions, as well as other members of the campus community, are as follows:

a. **Information Systems Department** is responsible for oversight, consultation about, and interpretation of this and other related information security policies, and for disseminating related information.
b. **System and Information Stewards / Owners** are responsible for the application of this and related policies to the systems, data, paper records, and other information resources under their care or control.
c. **System Administrators** - are responsible for the application of this and related policies to the systems information resources in their care. System Administrators shall comply with this *Information Security Policy* and shall coordinate such compliance with the Information Systems. Systems that store Restrictive or Confidential Information, including departmentally supported server-based applications, if not centrally managed and maintained by IS, should be managed by department System Administrators in coordination with IS.
d. **System Developers and Information Integrators** - System Developers and Information Integrators are responsible for the application of this and related policies to the systems, data, and other information resources in their care and shall coordinate with the Information Systems Department to ensure that all aspects of the development process are in compliance with the *Southern Information Security Policy*.
e. **Users** - Users of Southern's information resources are responsible for the application of this and related policies to the systems, data, paper records and other information resources in their care, including both electronic and hard-copy. In addition, users who download or store Restricted or Confidential Information should be aware of the security risks and responsibilities associated with such activities and follow applicable *Southern Information Security Policy*.
f. **Third-party Vendors and Consultants** – Employees involved with out-sourcing, shall mandate that third-party vendors and consultants implement appropriate information protection and security measures as a condition of receipt or use of university information. When receiving and using university information, third-party vendors and consultants are expected to follow the guiding principles of this policy and (1) provide for

the security of information during transmission, (2) safeguard information while in their possession and control, and (3) properly dispose of or return the information to the university at the completion of, and in compliance with, the contractual arrangement. In the event that a third-party vendor or consultant discovers any breach of the security of university information in its possession and control, the third-party vendor or consultant shall notify the university immediately upon discovery when the information was, or is reasonably believed to have been, acquired by an unauthorized person.

2. Principles of Information Security

The purpose of information security is to protect the information resources of the university from unauthorized access or damage. The underlying principles followed to achieve this objective are:

a. **Information Protection, Back-Up and Recovery** - Institutional information resources, including systems, workstations, and data and record classifications, identified by this policy, shall be operated in a manner that reasonably minimizes the threat of internal or external compromises to the security, confidentiality or integrity of university information. Users are expected to safeguard such information in compliance with legal obligations and administrative policies and procedures, including confidentiality and non-disclosure agreements. They should have plans in place to restore such information to assure the continuation of the necessary business operations of the university, in the event of a compromise to institutional information resources.
b. **Information Availability** - The information resources of the university, including the network, the hardware, the software, the facilities, the infrastructure, hard-copy documents and any other such resources, should be available to support the teaching, learning, research and administrative roles for which they are created.
c. **Information Integrity** - Information stewards should employ appropriate authentication and verification measures so that the information, used in the pursuit of teaching, learning, research and administration, can be trusted to be accurate.
d. **Information Confidentiality** - The value of information as an institutional resource increases through its widespread and appropriate use; its value diminishes through misuse, misinterpretation, or unnecessary restrictions to its access. The ability to access or modify information shall be provided as needed to users for authorized purposes, based on a minimal access model.
e. **Information Use and Disclosure** - The use of Restricted Information for identification, authentication, or any other purpose should be eliminated whenever possible. Historical records containing Restricted Information shall be appropriately maintained and destroyed in accordance with legal

and regulatory standards, and the principles set forth in this policy. Users requesting access to university information resources, or collecting such information, shall be required to limit the scope of those requests or collections to only the information necessary for their legitimate use. Users must not disclose Restricted or Confidential Information to unauthorized individuals or entities without a legitimate educational or business reason for access to the information. State and federal law and regulations and university policies provide standards for the distribution of various forms of information contained in university records.

3. Classification of Information Records

All university information, including electronic and hard copy records, is assigned to stewards, who classify it by the level of sensitivity and risk. These classifications take into account the legal protections, contractual agreements, ethical considerations and proprietary worth. Information can also be classified as a result of the application of "prudent stewardship," where a legal mandate to protect such information is lacking, but reasonable discretion may be required in its disclosure.

The classification level assigned to information guides information stewards, end users, business and technical project teams, and others who may obtain or store information, in the security protections and access authorization mechanisms appropriate for that information.

Information classification is defined in Southern's Data Classification Policy (see appendix A) as follows:

a. Restricted Information
b. Confidential Information
c. Unrestricted Information

When the appropriate level of protection is determined, that same level of protection shall be applied to all other related information in whatever format, wherever retained (e.g., servers, network segments, desktop computers, mobile devices and storage devices such as jump drives, CD or DVD, and physical storage units such as rooms/spaces, desk drawers and file cabinets).

4. Classification of Systems

University systems, both hardware and software, are classified by scope and level of support and by impact on university operations. The classification of systems takes into account legal protections, contractual agreements, ethical considerations, and strategic or proprietary worth of information maintained in such systems. The classification level assigned to systems will guide system and

data stewards, and business and technical project teams in the security protections and access authorization mechanisms appropriate for those systems. Such categorization provides the basis for planning, allocation of resources, support, and security/ access controls appropriate for those systems.
The system classifications are as follows:

a. **Applications/Servers**
    - *Enterprise Systems* - Systems with university-wide data accessibility presence across various departments or academic units. These systems, considered business-essential, require a high degree of availability. Examples include, but are not limited to, Ellucian applications.
    - *Department Systems* - Systems with a localized departmental presence, essential for conducting business processes or delivery of academic content.
    - All systems hosting server services must be registered with the Information Systems Department.

b. **Workstations and Other Access Devices** Users who access university systems and data via their workstations or other devices are responsible for exercising proper accountability and stewardship in protecting the restricted, confidential, private, personal or institutional information they access or use in the conduct of their job responsibilities. User access to university systems and information resources will be governed by the type of workstation or device used as follows:
    - *Managed Workstations and Devices* - Workstations and devices that access enterprise or business critical systems or access Restricted or Confidential Information shall adhere to configuration standards and maintenance procedures established by the Information Systems Department. Failure to meet these requirements will be grounds for denial of system or university network access.
    - *Non-Managed Workstations and Devices* - Non-Managed workstations and devices may include but are not limited to faculty and staff personal workstations, personal computers, mobile devices, etc. Non-Managed Workstations and Devices shall have no access or limited access to enterprise or business critical systems that store Restricted Information.

5. Information Storage and Disposition

Information and records, whether maintained in electronic files or on paper, must be stored and disposed of securely according to the guidelines published in Southern's Data Classification Policy.
ALL information and records subject to a litigation hold must be retained in whatever format the information is in and in whatever classifications notwithstanding other general policies on retention.

6. Violations of Policy and Misuse of Information
Violations of this policy include, but are not limited to: accessing information to which the individual has no authorization or business purpose; enabling unauthorized individuals to access information; disclosing information in a way that violates applicable restricted access or confidentiality procedures, or handling or using information contrary to any other relevant regulations or laws; inappropriately modifying or destroying information or university business records; inadequately protecting Restricted Information or Confidential Information; or ignoring the explicit requirements of information stewards for the proper management, use and protection of information resources. Violations may result in network removal, access revocation, corrective action, university disciplinary action and/or civil or criminal prosecution, if applicable. Should disciplinary action be implemented, up to and including dismissal, suspension or expulsion, such actions will be taken pursuant to applicable university policies and procedures.

In the event that a university office or department is found to have generally violated this policy (beyond actions taken by an individual employee), the vice president responsible for that area will be notified. Corrective actions and possible financial costs associated with an information security incident will be coordinated at cabinet level.

Third-party vendors and/or consultants found to have breached their respective agreements with the university may be subject to consequences, including but not limited to, the loss of third-party vendor/consultant access to university information technology resources, removal of the vendor/consultant from university facilities, termination/cancellation of the agreement, payment of damages, and criminal or civil charges based on the nature of the violation.

The university is sometimes required to transmit information by state or federal forms and formats. When using such forms and formats, university employees should transmit such information following university policy and utilize appropriate safeguarding and security measures in the transmission of that information. It is important to work with state and federal officials in striving to meet industry best practices in the transmission of information.

7. Exceptional Information Releases
In some instances the university is mandated to disclose, or authorize to release information that would normally be protected under this policy. Examples include, but are not limited to, disclosures pursuant to state or federal reporting requirements, legal process (such as subpoenas, court orders, warrants, etc.), and certain authorized releases of information about particular individuals (students, employees or customers).

Legal Process

Any employee or affiliate of the university who is served with a legal document (for example, a subpoena, summons, court order, warrant, etc.) that refers to university records or data shall notify the Senior Vice President of Financial Administration immediately and prior to the release of any requested information. The Senior Vice President of Financial Administration will review the legal document to determine the validity and enforceability of the document, and to provide guidance and assistance in properly responding.

Legal documents that are addressed to a particular person should be accepted only by that person. If an unintended recipient is served with the legal document, it should not be accepted. The process server or deliverer should be referred to the person identified on the document, by name, title or job description, or should be directed to the Senior Vice President of Financial Administration.

Requests from External Entities and Persons, including Law Enforcement and Attorneys

The university receives numerous requests for information and records maintained by the university from persons and entities that are external to the university. The release of information about a particular person may require authorization by that person. The Senior Vice President of Financial Administration is available to assist with evaluating the validity and scope of any authorization provided for the release of information, as well as providing guidance for appropriately responding to information requests pursuant to an authorization.

External law enforcement agencies sometimes request information. Before responding to these requests, the Senior Vice President of Financial Administration should be contacted to determine the authenticity of the request and the requestor. In addition, any request for information from an attorney, whether by legal process or not, should be immediately referred to the Senior Vice President of Financial Administration.

All other requests for information from outside entities or persons should be evaluated on a case-by-case basis. For identifying information or data stored in an electronic format at Southern, the Information Systems Department is available for assistance.

In the absence of the Senior Vice President of Financial Administration, all legal requests should be directed to the Senior Vice President of Academic Administration.

8. Sources of More Information

The duties and responsibilities of university employees with regards to information protection and safeguarding are defined by numerous documents, including but not limited to, state and federal laws and regulations, university policies and procedures, and industry standards and best practices. Since

information security is a growing and evolving area, the Information Systems Department, with cooperation from the Compliance Committee, will constantly monitor for new developments and maintain a listing of relevant resources on this topic.

APPENDIX A

SOUTHERN ADVENTIST UNIVERSITY

Data Classification, Access, Transmittal, and Storage Policy

Version 1 Revised Dec 17 2014

Southern Adventist University takes seriously its commitment to respect and protect the privacy of its students, alumni, faculty and staff, as well as to protect the confidentiality of information important to Southern's academic mission. For that reason, Southern has classified its information assets into the categories Unrestricted, Confidential and Restricted for the purpose of determining who is allowed to access the information and what security precautions must be taken to protect it against unauthorized access.

Southern expects all partners, consultants and vendors to abide by Southern 's information security policies. If non-public information is to be accessed or shared with these third parties, they should be bound by contract to abide by Southern's information security policies.

All new information systems that store or process Restricted Data, should be assessed by the Information Systems Department.

These guidelines are intended to reflect the minimum level of care necessary for Southern 's sensitive data. They do not relieve Southern or its employees, partners, consultants or vendors of further obligations that may be imposed by law, regulation or contract.

Definitions

- **Computing Equipment** is any Southern or non- Southern desktop or portable device or system.
- A number is **Masked** if: (i) a credit card primary account number (PAN) has no more than the first 6 and the last 4 digits intact, and (ii) all other Restricted numbers have only the last 4 intact.
- **NIST-Approved Encryption**: The National Institute of Standards and Technology (NIST), develops and promotes cryptographic standards that enable U.S. Government agencies and others to select cryptographic security functionality for protecting their data. Encryption which meets NIST-approved standards is suitable for use to protect Southern's data if the encryption keys are properly managed. In particular, secret cryptographic keys must not be stored or transmitted along with the data they protect. Cryptographic keys have the same data classification as the most sensitive data they protect.
- **Payment Card Industry Data Security Standards** are the practices used by the credit card industry to protect cardholder data. The Payment Card Industry Data Security Standards (PCI DSS) comprise an effective and appropriate security program for systems that process, store, or have access to Southern's Restricted data. The most recent version of the PCI DSS is available here.

- **Protected Health Information (PHI)** is all individually identifiable information that relates to the health or health care of an individual and is protected under federal or state law.
- A **Qualified Machine** is a computing device located in a secure Southern facility and with access control.
- **Student Records –** are those that are required to be maintained as non-public by the Family Educational Rights and Privacy Act (FERPA). Student records are any records maintained by Southern Adventist University or an agent of the Southern which is directly related to a student, except:
    - A personal record kept by a staff member, if it is kept in the personal possession of the individual who made the record, and information contained in the record has never been revealed or made available to any other person except the maker's temporary substitute.
    - An employment record of an individual whose employment is not contingent on the fact that he or she is a student, provided the record is used only in relation to the individual's employment.
    - Records maintained by Southern Adventist University's Campus Safety department if the record is maintained solely for law enforcement purposes, and is revealed only to law enforcement agencies of the same jurisdiction.
    - Records maintained by Health Service if the records are used only for treatment of a student and made available to those persons providing the treatment.
    - Alumni records which contain information about a student after he or she is no longer in attendance at Southern and the records do not relate to the person as a student.

Data Classifications

Use these criteria to determine which data classification is appropriate for a particular information or infrastructure system. A positive response to the highest category in any row is sufficient to place that system into that Classification.

	Restricted Information	Confidential Information	Unrestricted Information
Information Classification Guideline	Information is classified as "Restricted" if protection of the information is required by law/regulation or Southern is required to self-report to the government and/or provide notice to the individual if information is inappropriately accessed **If a file which would otherwise be considered to be Confidential contains any element of Restricted Information, the entire file is considered to be**	Information is classified as "Confidential" if (i) it is not considered to be Restricted and is not generally available to the public, or (ii) it is listed as Confidential in the "Classification of Common Data Elements".	Information is classified as "Unrestricted" if it is not considered to be Restricted, or Confidential.

	Restricted Information	Confidential Information	Unrestricted Information
	Restricted Information.		
Classification of Common Data Elements	• Social Security Numbers • Credit Card Numbers • Financial Account Numbers, such as checking or investment account numbers • Driver's License Numbers • Health Insurance Policy ID Numbers • Health Information, including Protected Health Information (PHI) • Passport and visa numbers	• Student Records • Unpublished Research Data • Faculty/staff employment applications, personnel files, benefits information, salary, birth date, and personal contact information • Admission applications • Donor contact information and non-public gift amounts • Privileged attorney-client communications • Non-public SAU policies and policy manuals • SAU internal memos and email, and non-public reports, budgets, plans, and financial information • Non-public contracts • University and employee ID numbers • Directory information as designated in the University catalog, for students who have chosen to exercise their right to privacy.	• Information authorized to be available on or through Southern's website • Published Research Data • Certain policy and procedure manuals designated by the owner as public • Campus maps • Job postings • Directory information as designated in the University catalog, for students who have not chosen to exercise their right to privacy. • Information in the public domain • SAU email address
Access Protocol	Access limited to those permitted under law, regulation and SAU's policies, and with a need to know.	Access limited to those with a need to know, at the discretion of the data owner or custodian.	At the discretion of the data owner, anyone may be given access to Unrestricted information. However, care should always be taken to use all University information appropriately and to respect all applicable laws. Information that is subject to copyright must only be distributed with the permission of the copyright holder.
Transmission	NIST-approved encryption is required when transmitting information through an insecure network. Third party email services are not appropriate for transmitting Restricted information. Restricted numbers may be Masked instead of encrypted.	NIST-approved encryption is strongly recommended when transmitting information through a network. Third party email services are discouraged for transmitting Confidential information.	No encryption is required for Unrestricted information.
Storage	Restricted on Computing Equipment unless approved by the SAU. If SAU approves, NIST-approved	Encryption of Confidential information is strongly recommended. Level of required protection of	No encryption is required for Unrestricted information. Care should still be taken to protect the integrity of Unrestricted information.

	Restricted Information	Confidential Information	Unrestricted Information
	encryption is required on Computing Equipment. Restricted numbers may be Masked instead of encrypted. NIST-approved encryption is also required if the information is not stored on a Qualified Machine. Third party processing or storage services are not appropriate for receiving or storing Restricted information unless approved by the SAU.	Confidential information is either pursuant to SAU policy or at the discretion of the owner or custodian of the information. If appropriate level of protection is not known, check with the data owner before storing Confidential information unencrypted. Third party processing or storage services may receive or store Confidential data if SAU has a valid contract with the vendor that includes the standard clauses specified in the Security Requirements.	

Unpublished Research and Intellectual Property Data

Published research data is considered public, and Southern is committed to openness in its research. Unpublished research data may need to be kept private. In those circumstances, unpublished research data is considered Confidential.

For purposes of data classification, a faculty member directing research is the data owner of the results of that research. As such, determining the level of protection necessary for unpublished research data is the prerogative of the faculty, taking into account any agreements such as the information security requirements of external research sponsors.

Southern members can invite other members, both within and outside the university to view Unrestricted data, co-edit documents, and use collaboration tools. It is the responsibility of each member to ensure appropriate sharing controls are used in order to protect intellectual property as well as prevent accidental or undesirable information sharing.

SAU Services

Please contact Information Systems for guidance before using a service to store, process, or transmit Restricted, or Confidential data as defined above, noting that Southern approval is needed in advance of handling Restricted data on anything other than Qualified Machines. Some of the services require additional components in order to qualify for the specified permitted data classifications.