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, is revealed only to law enforcement agencies of the same jurisdiction, and Campus Safety does not have access to education records maintained by Southern.
- 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 Restricted Information.**	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.
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	• 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	• 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 • Certain University contact information not designated by the individual as "private" • Information in the public domain

	Restricted Information	Confidential Information	Unrestricted Information
	(PHI) • Passport and visa numbers	• 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	• 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 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.	Encryption of Confidential information is strongly recommended. Level of required protection of 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.	No encryption is required for Unrestricted information. Care should still be taken to protect the integrity of Unrestricted information.

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.

[Adapted from Stanford University - Data Classification, Access, Transmittal, and Storage Policy]