Southern Reformed College & Seminary

Information Security Policy

Policy Title	Information Security Policy
Responsible	Registrar
Executive	President's Office
Last Update	November 9, 2017

I. Policy Statement

The purpose of this policy is to provide a security framework that will ensure the protection of Seminary Information from unauthorized access, loss or damage while supporting the open, information-sharing needs of our academic culture. Seminary Information may be verbal, digital, and/or hardcopy, individually-controlled or shared, stand-alone or networked, used for administration, research, teaching, or other purposes.

Failure to comply with this policy may subject you to a disciplinary action.

II. Who Is Affected by This Policy

The Information Security Policy applies to all seminary faculty and staff, as well as to students acting on behalf of Southern Reformed College & Seminary through service on seminary bodies such as task forces, councils and committees (for example, the Faculty-Student Committee on Discipline). This policy also applies to all other individuals and entities granted use of Seminary Information, including, but not limited to, contractors, temporary employees, and volunteers.

III. Definitions

Authorization – the function of establishing an individual's privilege levels to access and/or handle information.

Availability – ensuring that information is ready and suitable for use.

Confidentiality – ensuring that information is kept in strict privacy.

Integrity – ensuring the accuracy, completeness, and consistency of information.

Unauthorized access – looking up, reviewing, copying, modifying, deleting, analyzing, or handling information without proper authorization and legitimate business need.

Seminary Information – information that Southern Reformed collects, possesses, or has access to, regardless of its source. This includes information contained in hard copy documents or other media, communicated over voice or data networks, or exchanged in conversation.

IV. Policy

Southern Reformed appropriately secures its information from unauthorized access, loss or damage while supporting the open, information-sharing needs of our academic culture.

A. Classification Levels

All Seminary Information is classified into one of four levels based on its sensitivity and the risks associated with disclosure. The classification level determines the security protections that must be used for the information.

When combining information, the classification level of the resulting information must be re-evaluated independently of the source information's classification to manage risks.

The classifications levels are:

1. Restricted

The following Seminary Information is classified as Restricted:

- Social security number
- Bank account number
- Driver's license number
- State identity card number
- Credit card number
- Protected health information (as defined by HIPAA)

State and Federal laws require that unauthorized access to certain Restricted information must be reported to the appropriate agency or agencies. **All reporting of this nature to external parties must be done by or in consultation with the Office of the President.**

Sharing of Restricted information within the seminary may be permissible if necessary to meet the seminary's legitimate business needs. Except as otherwise

required by law (or for purposes of sharing between law enforcement entities), no Restricted information may be disclosed to parties outside the seminary, including contractors, without the proposed recipient's prior written agreement (i) to take appropriate measures to safeguard the confidentiality of the Restricted information; (ii) not to disclose the Restricted information to any other party for any purpose absent the seminary's prior written consent or a valid court order or subpoena; and (iii) to notify the seminary in advance of any disclosure pursuant to a court order or subpoena unless the order or subpoena explicitly prohibits such notification. In addition, the proposed recipient must abide by the requirements of this policy. Any sharing of Restricted information within the seminary must comply with seminary's policies.

2. Confidential

Seminary Information is classified as Confidential if it falls outside the Restricted classification, but is not intended to be shared freely within or outside the seminary due to its sensitive nature and/or contractual or legal obligations. Examples of Confidential Information include all non-Restricted information contained in personnel files, misconduct and law enforcement investigation records, internal financial data, donor records, and education records (as defined by FERPA).

Sharing of Confidential information may be permissible if necessary to meet the Seminary's legitimate business needs. Unless disclosure is required by law (or for purposes of sharing between law enforcement entities), when disclosing Confidential information to parties outside the seminary, the proposed recipient must agree (i) to take appropriate measures to safeguard the confidentiality of the information:(ii) not to disclose the information to any other party for any purpose absent the Seminary's prior written consent or a valid court order or subpoena; and (iii) to notify the Seminary in advance of any disclosure pursuant to a court order or subpoena unless the order or subpoena explicitly prohibits such notification. In addition, the proposed recipient must abide by the requirements of this policy. Any sharing of Confidential information within the Seminary must comply with Seminary.

3. Unrestricted Within Southern Reformed (UWSR)

Seminary Information is classified as Unrestricted Within Southern Reformed (UWSR) if it falls outside the Restricted and Confidential classifications, but is not intended to be freely shared outside the Seminary.

The presumption is that UWSR information will remain within Southern Reformed. However, this information may be shared outside of Southern Reformed if necessary to meet the seminary's legitimate business needs, and the proposed recipient agrees not to re-disclose the information without the Seminary's consent.

4. Publicly Available

Seminary Information is classified as Publicly Available if it is intended to be made available to anyone inside and outside of Southern Reformed.

B. Protection, Handling, and Classification of Information

1. Based on its classification, Seminary Information must be appropriately protected from unauthorized access, loss and damage.

2. Handling of Seminary Information from any source other than Southern Reformed may require compliance with both this policy and the requirements of the individual or entity that created, provided or controls the information. If you have concerns about your ability to comply, consult the relevant senior executive.

3. When deemed appropriate, the level of classification may be increased or additional security requirements imposed beyond what is required by the Information Security Policy.

V. Responsibilities

All Southern Reformed faculty, staff, students (when acting on behalf of the Seminary through service on Seminary bodies), and others granted use of Seminary Information are expected to:

- Understand the information classification levels defined in the Information Security Policy.
- As appropriate, classify the information for which one is responsible accordingly.
- Access information only as needed to meet legitimate business needs.
- Not divulge, copy, release, sell, loan, alter or destroy any Seminary Information without a valid business purpose and/or authorization.
- Protect the confidentiality, integrity and availability of Seminary Information in a manner consistent with the information's classification level and type.
- Handle information in accordance with any other applicable Seminary standard or policy.
- Safeguard any physical key, ID card, computer account, or network account that allows one to access Seminary Information.
- Discard media containing Southern Reformed information in a manner consistent with the information’s classification level, type, and any applicable Seminary retention requirement. This includes information contained in any hard copy document (such as a memo or report) or in any electronic, magnetic or optical storage medium (such as a memory stick, CD, hard disk, magnetic tape, or disk).

- Contact the Office of the Registrar prior to disclosing information generated by that Office or prior to responding to any litigation or law enforcement subpoenas, court orders, and other information requests from private litigants and government agencies.
- Contact the appropriate Seminary office prior to responding to requests for information from regulatory agencies, inspectors, examiners, and/or auditors.

VI. Policy Review

At a minimum, the Information Security Policy will be reviewed every 24 months.

PRIVACY PLEDGE

I acknowledge that I have received a copy of the Information Security Policy. Furthermore, I have understood and agree with the Policy and will fully comply with its stipulations. As staff at SRCS, I have access to confidential information and use of data the seminary community generally perceives as personal and private. I understand that access to this confidential information and data carries with it responsibility to guard against unauthorized use and to abide by the Information Security Policy. To treat information as confidential means not to divulge it to anyone who is not authorized by the seminary, or to cause it to be accessible by anyone who is not authorized by the seminary. Anything not specifically named as "public information" is considered confidential. I agree to fulfill my responsibilities in accordance with the following guidelines:

1. I agree to not permit unauthorized individual to access to the confidential data, either electronically or hard copy.
2. I agree to not store confidential information on non-seminary storage unit either electronically or hard copy.
3. I agree to return or delete all confidential documents and files that might be in my personal email accounts or locations outside the seminary property.

Name Position

Signed Date