Simmons Information Security Policy

Policy Objective and Scope

The objective of the Simmons Information Security Policy is to advise and govern faculty, staff, and students on the proper storage and release of sensitive information at Simmons and to ensure that such storage and release is compliant with Massachusetts General Laws as codified in *201 CMR 17.00: Standards for The Protection of Personal Information of Residents of the Commonwealth.*

This security policy may overlap with other Simmons Policies, as well as State and Federal security laws and standards such as HIPAA, FERPA, Red Flag Rules, and the Gramm-Leach-Bliley Act (GLBA).

For the purposes of this policy, sensitive information is an individual's name, address, or telephone number combined with any of the following:[1]

- Social security number or taxpayer ID number
- Financial account, credit or debit card number
- Financial/salary data
- Driver's license number
- Date of birth
- Medical or health information protected under state or federal law (e.g. HIPAA)
- Student data protected under state or federal law (e.g. FERPA)
- Access codes, security codes or passwords that would permit access to sensitive information

In addition, the security of other types of sensitive or confidential information is provided for in this policy. This includes, but is not limited to, information relating to any of the following:

- Current or future fundraising campaign strategies
- Donor information such as wealth, asset holdings, and giving history, internal and external to Simmons
- Planning and construction of facilities
- Information regarding Simmons current or projected financial matters, including its schools and programs
- Vendor proprietary information (e.g. information from a third-party held confidential by agreement)
- Information explicitly marked as confidential (e.g. documents prepared for the Board of Trustees)

Storage and Access of Sensitive Information

All users responsible for Simmons data must adhere to secure computing practices regarding what data may be stored where. For a full description of the policy regarding the proper storage of specific types of data, please refer to the Data Classification & Secure Storage

[1] Mass 201 CMR17.04(1)(a)

Policy.

Sensitive information will only be maintained for a length of time reasonably necessary to accomplish legitimate business purposes, or to comply with state, local, or federal regulations. Individuals and organizations are responsible for maintaining compliance with this policy, including obligations under 201 CMR 17.00 and any other applicable state, local and federal regulations.

Simmons has established the following general guidelines regarding the remote and physical access to information assets:

- Simmons Technology encrypts data on Simmons-own computer workstations, laptops, and devices.[2]
- Simmons Technology encrypts remote access to sensitive information contained in managed applications, systems, and servers.[3]
- Simmons Technology maintains data loss prevention tools that identify potentially sensitive information in Simmons managed network and cloud storage solutions.
- Simmons prohibits the use of personal cloud solutions, such as Apple iCloud, non-Simmons Google Drive, or Microsoft OneDrive for the storing of sensitive information.
- Simmons prohibits the use of non-Simmons personal computers, devices, and media for the storage or transportation of sensitive information.

Physical Access

Users are responsible for the physical security of information and computer resources which may include, but are not limited to, practices such as:[4]

- Using an activated screen saver password or lock-screen when devices are unattended.
- Positioning monitors to prevent inadvertent disclosure of information on screens
- Preventing theft by locking computer resources in secure areas or securing them with a cable lock
- Physical copies of sensitive information are to be secured in a locked desk or file cabinet.
- Implementing software/hardware solutions that aid in recovery of lost or stolen computers such as "Find My Phone".

Virus and Malware Protection

Virus and malware constitute a significant threat to sensitive information and may cause unauthorized disclosure. All Simmons computers are equipped with virus and malware protection and software, including operating systems, are kept up-to-date. Faculty and staff with Administrative Rights to Simmons computers shall not alter or disable this protection. Virus and malware protection is available free to students, faculty, and staff of the university for their personally owned computers from the Simmons Technology website. All computers, including those personally owned and attached to the campus network must have virus

[2] Mass 201 CMR17.04(1)(a)
[3] Mass 201 CMR17.04(3)
[4] Mass 201 CMR17.04(1)(b)

protection installed and software up-to-date.[5]

Permissions and Passwords

Remote access to applications and systems is granted by authentication and authorization systems managed by Technology. In most cases, access is allowed via a Simmons username and password. Faculty, staff and students must take precautions to safeguard usernames and passwords including:[6]

- Not writing usernames and passwords down or keeping them where others could gain access.
- Never using the same password for any other service, application, or website.
- Never sharing or divulging to any anyone usernames or passwords, including others at Simmons.
- Not entering passwords on computers that have potential to be compromised, such as public computers in Internet cafés or airports.

Password Guidelines

When selecting a new password, users must select passwords that are long, strong, and complex and meet these minimum requirements:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Contains at least one number character (e.g., 0-9)
- Contains at least one of these special characters:
  _ ` ^ ~ < = > | \ - ; : ! ? / . ' " ( ) [ ] { } @ $ * & # % + and space
- Have a minimum of at least 10 characters and preferably 15 characters long and is a phrase.
- Maximum 100 characters
- Not include username, student ID, first and last name
- Not included common words or sequences (e.g. password, qwerty, 123456, 111111, 999999, qazwsx, etc.)

E-mail

Sensitive information in documents exchanged and stored in email is susceptible to unauthorized access while stored on email servers, local computers both at work or home, and during transition. Users shall not transmit or store sensitive information in email. Technology is available to advise users on alternatives to storing and transmitting sensitive information by email.

Retention and Destruction of Sensitive Information

Simmons will limit the amount of sensitive information collected and used and shall collect only the amount reasonably necessary to perform an official task, a legitimate business purpose, or to comply with state, local, or federal regulations.

In some cases, government and/or other regulations may mandate the retention of data. In such cases, retention of data shall comply with these rules. Otherwise, copies of sensitive information that are made for a specific purpose must be deleted or destroyed after that

[5] Mass 201 CMR17.04(7)

[6] Mass 201 CMR17.04(1)(c)

purpose has been fulfilled. In the case of paper or other disposable media, such as CDs, floppies, or magnetic tape, destruction shall be complete and permanent. For assistance or advice, please contact the Simmons Service Desk.

If you have access to or copies of sensitive information in your possession or under your control, you are responsible for surrendering that information upon termination of your employment. Your manager, Dean, Vice President, or a member of Human Resources will work with you to assist you in this critical task prior to your last day of work. No Simmons employee – faculty or staff – shall delete information at the conclusion of employment without consulting their supervisor.

The Simmons Records Retention Policy can be found:
https://internal.simmons.edu/wp-content/uploads/2019/09/Records-Retention-Policy.pdf

Policy Compliance

All persons with access to sensitive information at Simmons are responsible for compliance with this policy. Violations of this policy are serious and may result in disciplinary action up to and including termination of employment. Any disclosures of sensitive information that is not for Simmons business purposes, shall be reported expeditiously to the Information Security Officer, Chief Information Officer, the Office of the Senior Vice President for Finance & Administration, or the university Vice President and General Counsel. Such report shall include:

- The type and scope of information disclosed (who, what, when)
- Circumstances under which the disclosure occurred (where, how)

Contractors with whom Simmons shares sensitive information or who have incidental access to sensitive information within the scope of their work shall sign a confidentiality agreement acknowledging this policy.

Update 09/28/2018
Approved 10/09/2018