Information Security Policy

Version: 1.02
Date: 6/28/2019

Revision History

Version	Date	Author	Description
1.00	1/21/2017	Dan Kinsman	Initial Document
1.01	3/8/2018	Dan Kinsman	4.2 Reporting a Data Breach – Notification is to CIO
1.02	6/25/2019	Stacy Slocum	Annual Review – minor updates to wording and punctuation. Inclusion of GDPR as area of regulation.

Table of Contents

1. Rationale / Purpose

St. John Fisher College "**SJFC**" creates, collects, maintains, uses, and transmits confidential information, including Personally Identifiable Information "**PII**" relating to individuals associated with the College, including, but not limited to, applicants, students, parents, alumni, employees and vendors. SJFC is committed to protecting the confidentiality, integrity, and availability of this information against inappropriate access and use. To that end, an Information Security Program was established to partner with the SJFC community to provide ongoing proactive security policies, procedures and education to promote a general culture of security awareness. The Information Security Program is further defined in the documents referenced in section 6.

This policy, associated procedures and standards provide direction for information security in accordance with SJFC requirements, relevant laws and regulations. St. John Fisher College information security practices are designed to promote and encourage appropriate use of information assets. They are not intended to prevent, prohibit, or inhibit the sanctioned use of information assets as required to meet the College's mission.

This Policy is adopted by the College to help all College community members understand the definition of confidential information, their obligations, and individual responsibilities. The College will make available appropriate training and education to further assist the College community in complying with the Policy.

2. Scope and Definitions

2.1. Scope

This Policy applies to all members of the St. John Fisher College community, including employees (both faculty and staff), student workers, and other individuals such as service contractors, vendors and consultants, who have a relationship with the College and whose responsibilities give them access to Confidential Information as defined in section 2.2.1. This Policy also applies to the access, use, storage, transmittal and destruction of confidential information belonging to any individual, regardless of the media in which it occurs, including both paper and electronic formats.

2.2. Information Security Categories

Data is classified according to the type of information and its impact so that the appropriate safeguards can be applied. The three types of data are Confidential, Internal Use Only, and Public. Each of the three types, or levels, has accompanying sets of protection measures. Confidential has the tightest security controls to protect the most

sensitive, high-risk confidential data. Internal Use Only has measures to protect College's enterprise-specific data. (Refer to the "Data Protection Policy and Data Classification Standard"

2.2.1. Data Classification Types

(a) ***Confidential Information*** – This is information that must be rigorously protected and is any information protected by the following laws, rules or regulations:

(i) Family Educational Rights and Privacy Act (**FERPA** – Student Records);

(ii) Health Insurance Portability and Accountability Act (HIPAA – Health Records), **PHI**;

(iii) Payment Card Industry Data Security Standard (PCI DSS – Credit Card Information), **PCI**;

(iv) Graham Leach Bliley Act (**GLBA** – Personal and Financial Information);

(v) European Union General Data Protection Act (GDPR – Data on EU residents)

(vi) Employee confidential information;

(vii) New York State Social Security Number Protection Act;

(viii) New York State Information Security Breach and Notification Act.

Confidential Information also includes:

(ix) Any information requiring confidentiality pursuant to a contract requirement;

(x) Personally Identifiable Information, ("**PII**." The term "PII," refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important to recognize that non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to identify an individual.)

(xi) Data likely to cause significant harm to an individual, group, or SJFC if disclosed.

- Examples of Confidential Information include, but are not limited to, the following:

- Employee salary, benefit and other HR information
- Personal cell phone numbers
- Unpublished College financial statements and development plans
- Non-public personal and financial information about applicants, students, alumni, corporations and donors
- Information regarding College information and facilities security systems

(b) ***Internal Use Only Information*** – This is information that is intended for use only within the College, but does not meet the definition of Confidential Information. Examples include but are not limited to):

(i) Information that is not to be released without authorization.

(ii) Information that requires protections according to SJFC policy or standards.

(iii) Data that may cause harm to an individual, group, or SJFC if disclosed.

(iv) Examples: College identified student directory information as defined in FERPA, Project Plans, Budgets, Meeting minutes, etc.

(c) ***Public Information*** - This type of information can be communicated without restrictions, and is intended for general public use. This data will not cause harm to any individual, group, or SJFC if made public.

Examples include faculty blogs, marketing material, policies, college plan, personnel directory, maps, course catalog, public web page, press releases, schedules of classes.

3. Policy Statement

Members of the College community will employ reasonable, practical and appropriate administrative, technical, physical and procedural safeguards to protect the confidentiality, integrity, and availability of all Confidential Information and Internal Use Only Information. In recent years, state and federal regulations have mandated specific protections for different types of information, including PII, PHI, PCI and Student Records. The New York State Information Security Breach and Notification Act and the breach and notification acts of other states define PII, provide guidelines governing PII and outline action to take in case of a data breach.

4. Data Breach

4.1. Definition.

Data Breach refers to an unauthorized acquisition of data that compromises the security, confidentiality, or integrity of Confidential Information or Internal Use Only Information, as defined in section 2.2.1. Good faith acquisition of Confidential Information by an employee or agent of the College for bona fide purposes of the College and in compliance with any applicable College Policies is not a breach of the security of the system, provided the Confidential Information is not used or subject to unauthorized disclosure.

4.2. Reporting a Data Breach.

- If it becomes known or suspected that College Confidential Information of Internal Use Only Information may have been acquired or used by an unauthorized person or for an unauthorized purpose, the matter should be immediately reported to the Chief Information Officer.

- Under New York law section 899-aa of the General Business Law, SJFC must notify affected New York residents and state officials as soon as practicable if a resident's "personal information" has been acquired or used by an unauthorized person or used for an unauthorized purpose. Reportable security breaches of this kind may include unauthorized access to a system that stores confidential information, or the loss or theft of a system or a physical record that contains SJFC confidential information; or cases where computers and/or devices, personal or college provided (tablets, smartphones, laptops that contain SJFC information) have been hacked, lost, stolen or passwords have been compromised.

- Possible breaches must be reported as soon as possible after becoming aware of the possible breach to the Chief Information Officer. Reporting should not be delayed in order to collect more information, to determine if a breach has actually occurred, or to determine what specific Confidential Information was actually involved.

5. Information Security Awareness Training

All full and part time college employees shall participate in an Information Security Awareness Training Session annually. The primary delivery method is assigned online training available through the College's portal. If requested at the department level, a 1-hour live session is available. The online session will also be provided to all new hire employees.

6. Related Policies and Information

- St. John Fisher College Information Security Program
- St. John Fisher College Email Policy
- St. John Fisher College FERPA Policy
- St. John Fisher College Data Protection and Data Classification Standard
- HIPAA Privacy Rules
- St. John Fisher College Employee Handbook
- St. John Fisher College Mobile Device Management Policy

7. Policy Changes

Policies and procedures are subject to review and may be modified at any time. Policies and procedures will be formally reviewed regularly by the Office of Information Technology (OIT) or in conjunction with significant system upgrades, whichever occurs sooner. Final approval for significant changes will come from Senior Staff.

Approval Date: May 5, 2017
Effective Date: May 5, 2017

Approval Authority: President's Cabinet