Springfield College

Information Security Policy

February 18, 2021

Purpose:

This document is designed to provide Springfield College ("College") with a Written Information Security Program ("WISP") in accordance with Massachusetts regulation 201 CMR 17.00 and other legal requirements which govern/regulate the protection of personal and/or financial information whether in electronic or physical format.

Table of Contents

1.0 Policy Statement

In compliance with Massachusetts 201 CMR 17.00, Springfield College ("College") has adopted this Information Security Policy ("ISP"). This policy serves the same purpose as a WISP. The ISP reflects the comprehensive College guidelines intended to ensure the safeguarding of all "Protected Data" collected by the institution in compliance with applicable laws and regulations pertaining to the protection of "Personal Information" and "Nonpublic Financial Information," as those terms are defined below.

2.0 Definitions

Data – For the purposes of this document, data refers to information stored, accessed or collected at, for, or on the College's behalf, about members of the College community.

Protected Data – Protected data is any non-public information, in whole or in part, to which access must be controlled and as such requires restrictions regarding storage, transit and other means of data usage.

Nonpublic Financial Information ("NFI") – Financial information pertaining to a Massachusetts resident which would permit access to a resident's financial account which is not lawfully obtained from publicly available information or federal/state/local government records lawfully made available to the general public.

Personal Information ("PI" also known as "PII" or Personal Identifiable Information) – As defined by Massachusetts 201 CMR 17.00 – a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following elements related to such resident that would permit access to a resident's financial account which is not lawfully obtained from publicly available information or federal/state/local government records lawfully made available to the general public:

a) Social Security Number
b) Driver's License Number or State Issued Identification Card Number
c) Financial Account Number, or Credit/Debit Card Number with or without any required security code, access code, personal identification number or password
d) Passport number, alien registration number or other government-issued identification number.
e) Date of Birth

3.0 Overview

The College's ISP was implemented in compliance with the Commonwealth of Massachusetts regulation "Standards for the Protection of Personal Information of Residents of the Commonwealth" [201 CMR. 17.00], the Federal Trade Commission [16 CFR Part 314], and obligations under the financial customer information security provisions of the Gramm-Leach-Bliley Act [15 USC 6801(b) and 6805(b)(2)]. These require the College to take measures designed to safeguard personal information to include personal financial information. Also, the College must enable a process of notice concerning security breaches of protected information to an affected individual and an individual's appropriate state agencies.

Springfield College is committed to safeguarding all protected data in both physical and electronic formats. The stored information is required for academic, business, fund raising, and employment purposes. These safeguards are defined/supported by adoption of a number of College policies and procedures designed to protect this information. The ISP is a companion document and should be read in conjunction with other policies identified and listed in Section 9 of this document.

This document includes:

- Establishment of a comprehensive information security program for the College supported by policies and procedures designed to safeguard protected data maintained by the institution in all formats;
- Defining employee responsibilities in safeguarding protected data relative to its classification level;
- Defining administrative, technical and physical safeguard expectations designed to enable a secure operational and technical environment in safeguarding protected data; and
- Defining auditing procedures to ensure the College remains perpetually compliant with all federal and state regulations governing protection of protected data.

4.0 Scope

The ISP applies to all employees, regardless of position and/or length or type of employment classification, as well as vendors of the College. This includes full- or part-time, including faculty, adjuncts, visiting scholars, graduate assistants, teaching fellows, professional and support staff, administrative staff, union staff, contract and temporary or project employees, hired consultants, interns, and student employees, all seasonal employees as well as to all other members of the College who may have access to protected data in the performance of their duties. Data covered by the ISP includes any information stored, accessed and/or collected in any location on the College's behalf. The ISP is not intended to replace or supersede any active College policy which more narrowly defines safeguard requirements of information. Where such a policy exists and conflicts with the ISP, the conflicting policy will take precedence in all areas that more strictly control access to data.

4.1 Data Classification

This ISP defines data into three distinctive categories based on security level(s) required to ensure the protection of data and adherence to federal and state law and/or College policies and procedures governing data access and protection. The classification of data will determine where the data can be stored, how it can be used and to whom it can be shared (See Appendix A). The data categories include Confidential, Restricted, and Public Information.

Confidential Information – refers to any data where unauthorized access, use, alteration or disclosure of said data could result in a significant level of risk to the College or its patrons. Confidential information elicits the highest level of security to ensure data privacy and prevent unauthorized access, use, alteration or disclosure. It is protected data.

Confidential Information includes data protected by the following federal and/or state regulations:

- Massachusetts regulation 201 CMR 17.00;
- Privacy of Consumer Financial Information 16 CFR 313;

- Graham, Leach, Bliley Act 1999 (GLBA);
- Health Insurance Portability and Accountability Act of 1996 (HIPAA); and
- Federal Trade Commission Red Flag Rules.

Restricted Information – refers to all other personal and institutional data where loss of said data could harm an individual's right to privacy or negatively impact the finances, operations, and/or reputation of the College. Any non-public data not explicitly designated as Confidential should be treated as Restricted Information. It is protected data.

Restricted Information includes data protected by the Family Educational Rights and Privacy Act of 1974 (FERPA), which pertains to the release of and access to personally identifiable information and academic information from student education records without the consent of a parent or eligible student. Additionally, the College also considers employee financial information and employee FERPA type legal/disciplinary information as Restricted Information. Restricted Information includes, but is not limited to:

- Donor information;
- Research data on human subjects;
- Intellectual property (proprietary research, patents, etc.);
- College financial and investment records; or
- Employee employment information.

Restricted Information access should be limited to individuals employed by or enrolled/matriculated at the College who have legitimate reasons for accessing said data as governed by FERPA, other applicable federal and state regulations, or approved College policies. A reasonable level of security should be maintained for this classification to ensure privacy and integrity from exposure to non-authorized parties.

Both Confidential and Restricted Information will be referred to jointly as Protected Data.

Public Information (Unrestricted) – includes any information where no restriction to its distribution exists and where the loss or public use of said information would not constitute harm to the College or members of the College community. Any information not classified as Confidential or Restricted is considered Public. It is not protected data.

5.0 Responsibilities

The Information Security Officer ("ISO") and Security Team is in charge of maintaining, updating, and implementing this policy. The College's Chief Information Officer ("CIO") has overall responsibility for this policy. The ISO and Security Team, in coordination with the CIO, are responsible to ensure:

a) Implementation of the ISP;
b) Coordination of employee ISP training;
c) Annual auditing and testing of ISP safeguards;
d) Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic data;
e) Securing and/or evaluating the security of all 3rd party service providers to ensure ISP compliance.

Every member of the College community has a role in ensuring proper data safeguards and processes are met, maintained and aligned to the protection of Confidential and Restricted Information generated by and/or on behalf of the College. No protected data should be shared with anyone who does not have a legitimate academic and/or business reason that has been approved by their respective division Vice President. As such, all data at the College is assigned according to the constituency reflective of the academic/business operation the data represents/resides.

Every member of the College community should strive to minimize the collection, handling, storage and use of protected data whenever possible.

Information Technology Services ("ITS") provides security for all data stored centrally on College servers and administrative systems. ITS is responsible for safeguarding said data in accordance with the ISP. For distributed data, whether on campus departmental servers or in the cloud, applicable department heads are responsible for ensuring operational data safeguards in collaboration with the ISO and CIO.

ITS is the sole proprietor of user account credentials for College users as it relates to network access, e-mail accounts, authentication and authorization.

In the areas of network access, single sign-on, and central ERP credentials, ITS interfaces with the Human Resources Information System to automatically enable/disable accounts for employees based upon employment status as listed in the Human Resources ("HR") database. In the case where ERP credentials are also enabled, the ITS team reacts to an automated notification from the HR department noting employment status changes resulting in access being enabled/disabled in concert with HR status changes.

In instances where departments contract with an individual or vendor warranting access to College data through credentialed profiles without going through Human Resources, the Department Head/Chair is required to coordinate with the CIO in regard to access requirements including length and degree of access needed. The CIO is then tasked with the responsibility to coordinate the access request with the various College departments to determine where the request is to be approved. It may require multiple approvals. If approved, the Department Head/Chair is required to provide the CIO with written notification when access is to be terminated.

6.0 Identification, Assessment & Mitigation of Risks to College Information

The College recognizes that both internal and external risks exist related to the security and integrity of College information. This is further complicated by the fact that the College has both resident and cloud-based repositories where information resides that include protected data. Additionally, not all software used by the College has sufficient security capabilities to allow nuanced access to data.

To mitigate internal risks, the College preforms the following actions:

- Employee training will be provided detailing the provisions and expectations of the policy.
- Annually, and upon updates to the policy, ITS will remind employees to review the ISP and encourage refresher training.
- Employment job descriptions and/or contracts should be amended to denote expectation of employee adherence to the ISP with non-compliance resulting in appropriate disciplinary action.
- College collection of protected data will be limited to that which is required to facilitate legitimate academic/business purposes.
- When reasonably possible, access to protected data will be limited to persons requiring a need to know to accomplish assigned academic/business responsibilities.
- Electronic access to protected data will be facilitated with stringent password credential strategies and where possible will include blocking access after multiple failed authentication attempts, require periodic password changes every 180 days and require strong passwords.
- Access to electronic protected data is limited to employees using unique assigned security credentials, and where possible, subject to inactivity timeout parameters designed to protect the information.
- Employees are required to never share their unique assigned security credentials with any other employee. The sole exception to this statement is when credential information is required by the College ITS staff to resolve a technical problem. However, the credentials will be set to require the owner to reset their password immediately after problem resolution.
- Terminated employee access will be suspended in sync with the HRIS termination date; and all physical and digital access to protected data will be blocked, and all physical documents and/or electronic devices where such information is stored will be returned.
- Employees are required to report any ISP discrepancies and/or suspicious activity which could compromise protected data.
- Employees are required to report all unauthorized exposure/use of protected data.
- Whenever an incident occurs requiring notification under M.G.L. c. 93H §3, an immediate mandatory post-incident review is required to list incident specifics and actions taken to ensure current data security standards are secure.
- Each department handling protected data must develop reasonable safeguards of physical records and its daily management to ensure access to these records are restricted to include storage of said records and data in locked facilities, secure areas, or locked containers. At a minimum:
    - Employees are prohibited from keeping unsupervised open files containing protected data at their desk.
    - All protected data must be protected from office visitors and unauthorized access.
    - All protected data is to be secured at the end of each business day in a manner consist with ISP rules.

    - All ISP security measures should be reviewed annually or in concert with material academic/business practice changes.
- Physical and/or electronic records containing protected data shall be disposed of in a manner compliant with M.G.L. c. 93I.

To mitigate external risks, the College anticipates:

- Proactive network security safeguards including updated firewall protection/strategies, current operating system security patch management, and current virtual service patching on all systems containing protected data.
- The ISO performs regular internal and external network security audits to all server and computer system logs to discover to the extent reasonably feasible possible electronic security breaches, and to monitor the system for possible unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of protected data.
- Installation of current anti-virus and malware protection on all College owned computers and servers.
- To the extent possible, enterprise level encryption is to be employed on all devices storing protected data and any media used to transmit said information. All computers, tablets and phones purchased with College funds and deployed after January 1, 2021, will have their internal hard drives encrypted. When feasible, existing unencrypted College purchased computing devices will be encrypted regardless of whether the employee has access to protected data. Exceptions will require written approval by the CIO upon the recommendation of the ISO.
- The removal of protected data from campus is strongly discouraged. In rare cases where it is necessary to do so, the user must take all reasonable precautions to safeguard the data. Under no circumstances are documents, electronic devices, or digital media containing protected data to be left unattended in any unsecured location.
- When there is a legitimate need to provide records containing protected data to a third party, electronic records shall be password-protected and/or encrypted, and paper records shall be marked confidential and securely sealed.
- The College will employ secure authentication protocols to include:
    1. Protocols for controlling security authentication credentials;
    2. Rigid password protocols whereby patrons must adhere to specific password lengths and complexity strategies designed to ensure reasonable data protection; and
    3. Centralized control of data security passwords.

7.0 Reporting Attempted or Actual Breach of Security

Any situation where potential or actual unauthorized access to, or disclosure of protected data might/has occurred is to be reported to the CIO and/or ISO immediately. Additionally, incidents where the misuse, alteration, destruction and other activity affecting protected data might/has occurred should also be reported to the CIO immediately with any supporting information to assist investigations. Upon notice, and if a reasonable suspicion established, the CIO and/or ISO will immediately alert the Internal Auditor, Vice President and General Counsel, and Director of Human Resources to initiate an incident/breach inquiry following the College's Incident/Breach Protocol in determining the scope and depth of the compromise of protected data and the related required actions to initiate. This protocol states that all investigative notes will be forwarded to the Internal Auditor for review in concert with the Vice President and General Counsel for legal compliance actions. Records of each investigation will be retained as directed by Massachusetts legal regulations or five years, whichever is longer.

Springfield College uses the Commonwealth of Massachusetts definition of Breach of Security by default, but is aware that other state definitions would need to be consulted in the situation where a breach of security exists involving victims from other states. For clarity, the Massachusetts definition for Breach of Security is as follows:

> *"Breach of Security, the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure."*

8.0 Enforcement

Any employee or student who willfully accesses, discloses, misuses, alters, destroys, and/or otherwise compromises College systems and/or Confidential/Restricted Information will be subject to disciplinary actions, to potentially include employment termination and/or expulsion from school. Likewise, any employee or student failing to comply with this ISP may be exposed to the same penalties. All disciplinary actions will be conducted by either the Office of Human Resources in the case of employees or by the Office of Student Affairs relating to students.

9.0 Policies Cross-Referenced

The Springfield College Information Security Program is supported and/or enhanced by the following College policies:

- **Acceptable Use Policy**
- **Data Classification - Storage Matrix (Appendix A)**
- **HIPAA Policy**
- **Policy Pertaining to Confidentiality of Students Records /Annual Notice to Students Regarding Education Records (in Student Handbook)**

10.0 Effective Date

Original Final Draft Revision Date – June 11, 2020

11.0 Review Date & Responsible Party

Expected Review Date – Annually until replaced

Responsible convening authority is the CIO in concert with ISO with expectation of reporting to the President's Cabinet annually.

Approved by: President and President's Leadership Team

Approval Date: February 23, 2021

Revisions: February 18, 2021 – *Added "Date of Birth" as Personal Information in Section 2*

APPENDIX A: DATA CLASSIFICATION - STORAGE

		Protected Data					
Storage	Public	Confidential / Private	FERPA	HIPAA / PHI	Other Restricted Data	SSN	PCI (Credit Card)
ITS Managed Storage	YES	YES	YES	YES	YES	APPROVAL NEEDED	NO
Brightspace / Moodle	YES	YES	YES	NO	YES	APPROVAL NEEDED	NO
SC GoogleApps	YES	YES	YES	NO	NO	APPROVAL NEEDED	NO
SC Office365	YES	YES	YES	NO	NO	APPROVAL NEEDED	NO
Local (C:,D:) drive (Mac, Windows)	YES	APPROVAL NEEDED	APPROVAL NEEDED	APPROVAL NEEDED	APPROVAL NEEDED	APPROVAL NEEDED	NO
Portable media (CD, Flash drive, external drive, etc)	YES	NO*	NO*	NO*	NO*	NO*	NO

APPROVAL NEEDED: NOT PERMITTED TO STORE DATA WITHOUT PRIOR APPROVAL FROM ITS Information Security Officer / Presidents Leadership Team / Internal Auditor

*Exceptions may be granted when legitimate business needs require and no other reasonable solution is available. The Information Security Officer will evaluate the situation and provide a documented procedure/solution that balances business needs and acceptable risk.

The Data Classification Matrix is regularly updated to reflect current business needs. The version above is current as of the last review of the ISP. Please review the most current version here: https://docs.google.com/spreadsheets/d/1lLJ-h4iUBD6PSVcY1L1xEszEk3X0wroQQhyI2QABIPs/edit?usp=sharing