

SPRINGFIELD COLLEGE

Information Security Policy - DRAFT

I. Purpose:

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)]. Concerning 201 CMR 27.00, this policy serves the same purpose as a WISP (Written Information Security Plan). These require the College to take measures designed to safeguard personal information, including personal financial information. Also, the College must enable a process of notice regarding security breaches of protected information to an affected individual and an individual's appropriate state agencies.

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 regarding the protection of "Personal Information" and "Nonpublic Financial Information," as those terms are defined below.

II. 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. The ISP covers any information or data 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 that 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.

III. Defined Terms:

- A. Data. For the purposes of this document data is a synonym for information, and includes all facts or figures, or collection of knowledge created, owned, received, stored, or managed by Springfield College. This includes all data that the College is legally or contractually obligated to secure, administrative data, academic data, and data gathered through College-administered surveys primarily used for organizational reporting and decision-making purposes.

- B. CUI. Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies. For this policy, it is synonymous with Protected Data. (Specific handling, protection, and processing guidelines can be found in NIST Special Publication 800-171 latest publication)
- C. Public. Public refers to people as a whole without restriction.
- D. 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.
- E. Privileged Access. Privileged Access is access to Protected Data beyond what is automatically granted to user based on their general role at the institution (faculty, staff, student, etc.).
- F. Nonpublic Financial Information (“NFI”). Financial information about a Massachusetts 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.
- G. 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 another government-issued identification number.
 - e. Date of Birth

IV. Overview:

Springfield College is committed to safeguarding all protected data in both physical and electronic formats. The stored information is required for academic, business, fundraising, and employment purposes. These safeguards are defined/supported by the adoption of several 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 X](#) of this document.

This document includes:

- Establishment of a comprehensive information security program for the College supported by policies, plans, 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 the protection of protected data.

V. Data Classification:

This ISP defines data into four distinct categories based on the 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 data classification 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 Restricted, Confidential, Internal-only, and Public Information. Information containing data from multiple categories will assume the most stringent category and follow the appropriate protective measures.

- A. **Restricted information** – any data that, if compromised or accessed without authorization, could lead to criminal charges and massive legal fines or cause irreparable damage to the College or its patrons. Restricted information requires the highest level of security to ensure data privacy and prevent unauthorized access, use, alteration or disclosure. Any non-public data not clearly described by the definitions of Confidential or Internal-Only Information should be treated as Restricted Information. It is protected data.

Restricted 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.

- B. **Confidential information** – refers to all other personal and institutional data where the loss of said data could harm an individual's right to privacy or negatively impact the finances, operations, and/or reputation of the College. It is protected data.

Confidential 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, employee FERPA-like information, and legal/disciplinary information as Confidential Information. Confidential 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.

Confidential 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.

- C. **Protected Data** – both Confidential and Restricted Information will be referred to jointly as Protected Data. For the purposes of NIST SP 800-171 compliance, Protected Data is synonymous with CUI.
- D. **Internal-only Information** – refers to data that is strictly intended for internal college community members who are granted access. This might include internal-only emails or other communications, business plans, etc. Access to this information should be limited to the intended recipient(s) and those with a business-related need to know.
- E. **Public Information (Unrestricted)** – includes any data where no restriction to its distribution exists and where the loss or public use of said information would not harm the College or members of the College community. Any information not classified as Confidential, Restricted or Internal-only is considered Public. It is never protected data.

VI. Responsibilities:

The Chief Information Security Officer ("CISO") and Security Team maintain, update, and implement this policy. The College's Chief Information Officer ("CIO") is responsible for this policy. The CISO and Security Team, in coordination with the CIO, are responsible for ensuring:

- a) Implementation of the ISP;
- b) Coordination of employee ISP training;

- c) Annual auditing and testing of ISP safeguards;
- d) Administrative actions, 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 Restricted and Confidential 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 their respective division Vice President has approved. All data access at the College is assigned according to the constituency reflective of the academic/business operation the data represents/resides.

Every college community member 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 or in the cloud, department heads and Data Stewards (see Data Governance Policy for definition) are responsible for ensuring operational data safeguards in collaboration with the CISO and CIO.

ITS exclusively manages user account credentials for College network access, email accounts, authentication, and authorization.

In the areas of network access, single sign-on, and role-based ERP credentials, ITS interfaces with the ERP System to automatically enable/disable accounts for users based upon role(s) at the college.

When privileged access is needed, the supervisor must submit a written request. This request must be approved by both the Data Steward and ITS and undergo an auditable review at least annually. The person receiving privileged access must have entered into an NDA or similar agreement with the college and completed FERPA training within the previous 12 months before access will be granted.

For Privileged Access credentials, the ITS team responds to automated notification from the ERP System regarding status changes, typically tied to changes in HR status, resulting in access being

either enabled, disabled, or modified. As an additional safeguard, in coordination with the Data Steward, ITS adjusts Privileged Access based on audit outcomes as required.

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 regarding access requirements, including length and degree of access needed. The CIO is then tasked with coordinating 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 must provide the CIO with a written notification when access is to be terminated.

When feasible, ITS will retain at least one user account on all College systems, with the highest level of access, to facilitate audits and support. ITS is responsible for installing and configuring all applications on college servers. Vendors may install applications on college servers only when contracted for this purpose and with an exception approved by the CIO.

I. Identification, Assessment & Mitigation of Risks to College Information:

The College recognizes that 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 the information resides that include protected data. Additionally, not all software the College uses has sufficient security capabilities to allow nuanced access to data.

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

- New employees will be expected to review this policy on their first day.
- Minimally, annual cyber security training will provide to all employees.
- Upon update to this policy, ITS will remind employees to review the ISP.
- All Information Technology Services employees are required to read and sign the current version of the Information Security Policy (ISP) within 15 days of publishing. Signed documents will be kept in personnel files.
- Employment job descriptions and/or contracts should be amended to denote the 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.

- When possible based on technological capabilities, the College will enforce the following stringent authentication measures on all accounts to safeguard data:
 1. **Credential Management Protocols:** Ensure standardized and secure procedures for controlling and managing authentication credentials.
 2. **Password Policy:** All users must comply with the stipulated password requirements to enhance data security. These are:
 - Minimum length of 15 characters.
 - Must include at least one of each: uppercase letter, lowercase letter, number, and special character.
 - Passwords cannot be any of the last 10 passwords used.
 - Passwords must be changed every 90 days if not protected by MFA.
 - Accounts will be automatically locked after six consecutive failed login attempts.
 3. **Multi-Factor Authentication (MFA):** MFA is mandatory where dictated by law, during server access, and is recommended for all employees wherever it's technically feasible. Beginning October 30, 2023, MFA will be progressively mandated for users accessing protected data and those in key roles. The goal is to have all employees with Privileged Access using MFA by September 30, 2024.
 4. **Centralized Password Management:** Central repository and oversight for data security passwords to ensure consistent application of security practices.
- 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.
- 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 must report any ISP discrepancies and/or suspicious activity that could compromise protected data.
- Employees are required to report all unauthorized exposure/use of protected data.
- Whenever an incident requires notification under MGL c. 93H §3, an immediate mandatory post-incident review is necessary to list incident

specifics and actions taken to ensure that current data security standards are secure.

- Each department handling protected data must develop reasonable safeguards of physical records and its daily management to ensure restricted access to these records, including 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 desks.
 - 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 consistent 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 MGL c. 93I.

To mitigate external risks, in addition to those to mitigate internal 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 CISO 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 compromises of protected data.
- The College will conduct regular automated penetration tests of IT systems, network infrastructure, and network-attached devices to validate cyber defenses and identify areas for remediation.
- 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 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 CISO.

- The removal of protected data from campus is strongly discouraged. In rare cases where it is necessary, 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.
- All software utilized by the College is subject to a cybersecurity evaluation. The College will require all Software as a Service and hosted on-campus application vendors to complete a Higher Education Community Vendor Assessment Toolkit (HECVAT) questionnaire. This is to ensure that the necessary information, data, and cybersecurity policies are in place to safeguard sensitive institutional information and constituents' PII. If a vendor declines to fill out the questionnaire, alternative documentation may be considered at the discretion of both the CIO and CISO. A cybersecurity re-evaluation will occur every two years or at the renewal of a multi-year contract.

VII. 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 CISO 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 reasonable suspicion is established, the CIO and/or CISO will immediately alert the Office of the President, Legal 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 necessary related actions to initiate. This protocol states that all investigative notes will be forwarded to the Legal Counsel for legal compliance actions. Records of each investigation will be retained as directed by Massachusetts legal regulations or for five years, whichever is longer.

Springfield College uses the Commonwealth of Massachusetts definition of Breach of Security by default. Still, it 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."

VIII. Enforcement:

Any employee or student who willfully illegitimately 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. Any ITS employee found violating this policy is subject to immediate dismissal. 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.

IX. Contacts:

Send questions regarding this policy and reports of policy violations to:
Chief Information Officer (CIO), 413-748-3532 or
Chief Information Security Officer (CISO), 413-748-3925

X. Related Policies and References:

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

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

Approved by: President and Cabinet
Date Adopted: June 11, 2020

Date Effective: June 11, 2020
Last Revision: October 4, 2024
Last Reviewed: April 14, 2025

Revision History:

- June 11, 2020 - Adopted
- February 18, 2021 – *Added “Date of Birth” as Personal Information in Section 2*
- October 14, 2022 – *Put policy in standard College format. Merged first paragraph of overview with purpose statement to reduce redundancy. Swapped the definitions of Restricted and Confidential Information to be consistent with government classification language. Added an Internal-only information classification. Added a definition of public. Added a definition of CUI. Updated the definition of data. Added the requirement for MFA and regular penetration testing, and removed all exceptions for password sharing to Section 6. Minor grammar and language clarification changes.*
- October 14, 2023 – *Added definition for Protected Access. Added process around requesting and maintaining Protected Access. Added details about authentication. Added reference and link to the Data Governance Policy.*
- August 8, 2024 – *Removed references to “Internal Auditor.” Changed “General Counsel” to “Legal Counsel.” Added requirement of ITS to have a privileged user account on all systems. Added IT responsibility for installing software on college servers, not vendors. Added requirement for employees to review policy on first day. Clarified the MFA requirement for Privileged Access. Added requirement for ITS to provide annual cybersecurity training. Added re-evaluation requirement for the software cybersecurity evaluation. Added requirement for ITS employees to sign the current version of this policy. Added the Office of the President into the breach response notifications. Added that ITS employees in violation of this policy are subject to immediate dismissal.*

APPENDIX A: DATA CLASSIFICATION - STORAGE

			Protected Data					
			Confidential Information			Restricted Information		
Storage	Public Information	Internal-only Information	FERPA	HIPAA / PHI – MOVE Restricted	Other Confidential Information	SSN	PCI (Credit Card)	Other Restricted Information
ITS Managed Storage	YES	YES	YES	YES	YES	APPROVAL NEEDED	NO	YES
Brightspace	YES	YES	YES	NO	YES	NO	NO	YES
SC GoogleApps	YES	YES	YES	NO	YES	APPROVAL NEEDED	NO	NO
SC Office365	YES	YES	YES	NO	YES	APPROVAL NEEDED	NO	NO
Local (C:,D:) drive (Mac, Windows)	YES	YES	APPROVAL NEEDED	APPROVAL NEEDED	APPROVAL NEEDED	APPROVAL NEEDED	NO	APPROVAL NEEDED
Portable media (CD, Flash drive, external drive, etc)	YES	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/1ILJ-h4iUBD6PSVcY1L1xEszEk3X0wroQQhyI2QABIPs/edit?usp=sharing>