**Title:** **Data Security Policy**
**Code:** **1-100-200**
**Date:** **6-5-2018 rev**
**Approved:** **WPL**

---

INTRODUCTION

The purpose of this policy is to outline essential roles and responsibilities within the University community for creating and maintaining an environment that safeguards data from threats to personal, professional and institutional interests and to establish a comprehensive data security program in compliance with applicable law. This policy is also designed to establish processes for ensuring the security and confidentiality of BC's Confidential and Strictly Confidential information and to establish administrative, technical, and physical safeguards to protect against unauthorized access or use of this information.

SCOPE

This policy applies to all Boston College faculty and staff, whether full- or part-time, paid or unpaid, temporary or permanent, as well as to all other members of the University community. This policy applies to all information collected, stored or used by or on behalf of any operational unit, department and person within the community in connection with University operations. In the event that any particular information at Boston College is governed by more specific requirements under other University policies or procedures (such as the policy concerning Student Education Records), the more specific requirements shall take precedence over this policy to the extent there is any conflict.

DEFINITIONS

***Information Resource.*** An Information Resource is a discrete body of information created, collected and stored in connection with the operation and management of the University and used by members of the University having authorized access as a primary source. Information Resources include electronic databases, and data associated with an application, as well as physical files. Information derived from an Information Resource by authorized users is not an Information Resource, although such information shall be subject to this policy.

***Information System.*** An Information System is an integrated set of components for collecting, storing, processing, and providing information (e.g. application). An Information System may contain one or more Information Resources or have one or more sponsors and/or classifications. If an Information System has multiple Information Resources or multiple Sponsors, making classification difficult, then a Data Security Directive or a Computer System Security Requirement may be required to clarify the handling of data therein.

***Sponsors.*** Sponsors are those members of the University community that have primary responsibility for maintaining any particular Information Resource. Sponsors may be designated by a Vice President or Dean in connection with their administrative responsibilities (as in the case of the University Registrar with respect to student academic records), or by the actual sponsorship, collection, development, or storage of information (as in the case of individual faculty members with respect to their own research data, or student grades).

***Data Security Officers.*** Data Security Officers are those members of the University community, designated by their University Vice President or Dean, who provide administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific Information Resources in consultation with the relevant Sponsors.

***Data Security Administrator –*** Data Security Administrators are those members of the University community designated by their Data Security Officers or their respective University Vice President or Dean. They assist Data Security Officers as needed with information security training of the department; monitoring, detecting, and removing personally identifiable information (PII) from computers; classifying and marking Information Resources in coordination with Sponsors; and assisting with other security related activities as needed.

***Users***. Users include virtually all members of the Boston College community to the extent they have authorized access to University Information Resources and Information Systems, and may include students, faculty, staff, contractors, consultants and temporary employees and volunteers.

***Data Security Committee***. The Data Security Committee shall be chaired by the Executive Vice President and shall include the following Vice Presidents or their representatives: the Provost, the Financial Vice President and Treasurer, the Vice President for Information Technology, the Vice President for Human Resources, and the General Counsel.

***Computer System Security Requirements***. Computer System Security Requirements shall mean a written set of technical standards and related procedures and protocols designed to protect against risks to the security and integrity of data that is processed, stored, transmitted, or disposed of through the use of University information systems, and shall include computer system security requirements that meet or exceed the requirements of regulations promulgated under Chapter 93H of Massachusetts General Laws. The Computer System Security Requirements shall be set forth as an exhibit hereto. The Computer System Security Requirements establish minimum standards and may not reflect all the technical standards and protocols in effect at the University at any given time.

***Data Security Directives***. Data Security Directives shall be issued from time to time by the Data Security Committee to provide clarification of this policy, or to supplement this policy through more detailed procedures or specifications, or through action plans or timetables to aid in the implementation of specific security measures. All Data Security Directives issued by the Committee shall be deemed incorporated herein.

***Specific Security Procedures***. Specific Security Procedures are procedures promulgated by a University Vice President or Dean to address particular security needs of specific Information Resources sponsored within their area of responsibility, not otherwise addressed by this policy, or any Data Security Directives.

***Data Security Working Group***. The Data Security Working Group shall be chaired by the Director of Computer Policy and Security, and shall consist of those Data Security Officers as may be assigned to the group from time to time by the Data Security Committee.

***Security Breach***. A Security Breach is any event that causes or is likely to cause information to be accessed or used by an unauthorized person and shall include any incident in which the University is required to make a notification under applicable law, including chapter 93H of the Massachusetts General Laws.

DATA CLASSIFICATION

1. All information covered by this policy is to be classified among one of four categories, according to the level of security required. In descending order of sensitivity, these categories (or "security classifications") are "*Strictly Confidential,*" "*Confidential*," "*Internal Use Only*," and "*Public*."

    - *Strictly Confidential* information includes any information that Boston College has a contractual, legal, or regulatory obligation to safeguard in the most stringent manner. Strictly Confidential information must be given the highest level of protection against unauthorized access, modification, or destruction. Unauthorized access to Strictly Confidential information may result in a significant invasion of privacy or may expose members of the University community to significant financial risk.

      Without limiting the generality of the foregoing, Strictly Confidential information shall include

"personal information" as defined by Massachusetts General Laws Chapter 93H ("Massachusetts PI"). Massachusetts PI means a Massachusetts resident's first name or first initial and last name in combination with any one or more of the following: (a) social security number; (b) driver's license number or state issued identification number; (c) financial account number, or credit card or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to the resident's financial account (e.g. student financial aid data). Additionally, Strictly Confidential information includes "customer information," defined by the safeguards rule under the Gramm-Leach-Bliley Act to mean any information containing personally identifiable information that the University obtains in the process of offering a financial product or service.

Strictly Confidential information includes medical/health information pertaining to members of the University community and data collected in the course of research on human subjects. Strictly Confidential information also includes HIPAA-protected information, export-controlled information, and other sensitive information that the information sponsor or responsible Vice President has determined must remain on a secure BC server.

- *Confidential* information includes sensitive personal and institutional information. Unauthorized access or modification to personal Confidential information may adversely affect individuals. Unauthorized access or modification to institutional Confidential information may result in direct, materially negative impacts on the finances, operations, or reputation of Boston College.
  - Examples of *personal* Confidential information include
    - Information protected under privacy laws (including, without limitation, the Family Educational Rights and Privacy Act)
    - Information concerning the pay and benefits of University employees
    - Employee performance appraisals for current, former and prospective employees
    - Donor addresses and gift data
    - Medical insurance waivers and credits
  - Examples of *Institutional* Confidential information may include
    - University financial and planning information[1]
    - Legally privileged information
    - Invention disclosures
    - Other information concerning pending patent applications
    - NCAA certification
    - Regulatory reporting
    - Online course evaluations

- *Internal Use Only* information includes information that is less sensitive than Confidential or Strictly Confidential information, but that, if exposed to unauthorized parties, may have an indirect or possible adverse impact on personal interests, or on the finances, operations, or reputation of Boston College. Examples of this type of data from an institutional perspective include internal memos meant for limited circulation, or draft documents subject to internal comment prior to public release.

- *Public* information is information that is generally available to the public, or that, if it were to become available to the public, would have no material adverse effect on individual members of the University community or upon the finances, operations, or reputation of Boston College.

2. All Information Resources, whether physical documents, electronic databases, or other collections of information, are to be assigned to a security classification level according to the most sensitive content contained therein.

3. Where practicable, all data is to be explicitly classified, such that Users of any particular data derived from an

[1] Some sponsors have classified University financial information as Strictly Confidential.

Information Resource are aware of its classification.

4. In the event information is not explicitly classified, it is to be treated as follows: (1) Any data which includes any personal information concerning a member of the University community (including any health information, financial information, , social security numbers or other personal identification information) shall be treated as Strictly Confidential information, and (2) Any data which includes academic evaluations or other academic records shall be treated as Confidential information. Other information is to be treated as Internal Use Only, unless such information appears in form accessible to the public (i.e., on a public website or a widely distributed publication) or is created for a public purpose.

5. The Data Security Committee may from time to time provide clarifications relating to the security classifications, and may, through issuance of Data Security Directives establish more detailed requirements concerning the classification of Information Resources, Information Systems, or specific data.

ROLE OF THE DATA SECURITY WORKING GROUP

1. The University has established the Data Security Working Group to aid in the development of procedures and guidelines concerning the collection, storage, and use of data by the University community, and to assist the Data Security Committee in the implementation of this policy.

2. In consultation with the Office of the General Counsel and the Director of Internal Audit, the Data Security Working Group shall:

    - Monitor federal, state and local legislation concerning privacy and data security.

    - Stay abreast of evolving best practices in data security and privacy in higher education, and assess whether any changes should be made to the Computer System Security Requirements.

    - Establish data privacy and security training and awareness programs for the University community and periodically assess whether these programs are effective.

    - Periodically reassess this policy to determine if amendments are indicated or if Data Security Directives should be proposed to the Data Security Committee.

    - Discuss any material violations of this policy and Security Breaches, the University's actions in response, and recommend any further actions or changes in practice or policy to the Data Security Committee.

ROLE OF THE DATA SECURITY COMMITTEE

1. The University has established the Data Security Committee to formulate University-wide procedures and guidelines concerning the collection, storage, use and safekeeping of data, to update as necessary this policy, and to direct the responsive actions in the event of any material violation of this policy or any Security Breach.

2. Any issues concerning sponsorship, classification or handling of data will be resolved by the Data Security Committee. The Data Security Committee is the ultimate arbiter of a data classification issue.

3. The Data Security Committee shall from time to time consult with representatives of the Data Security Working Group to review the implementation of this policy and compliance with the Computer System Security Requirements and Data Security Directives.

4. The Data Security Committee shall periodically review identifiable risks to the security, confidentiality, and integrity of data, and shall review this policy and the scope of Computer System Security Requirements at least

annually to assess its effectiveness and determine whether any changes are warranted. The Data Security Committee is authorized to:

- Issue Data Security Directives.
- Promulgate amendments to this policy, including the Computer System Security Requirements.
- Take actions to ensure compliance with this policy, which may include, without limitation, the commissioning of internal audits and investigations.
- Take actions in response to violations of this policy or any Security Breach.

ROLE OF THE DIRECTOR OF COMPUTR POLICY AND SECURITY

1. The Director of Computer Policy and Security shall, with input from the Data Security Working Group, identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of University data. This identification and risk assessment shall include adopting means for detecting security system failures and monitoring the effectiveness of the Computer System Security Requirements.

2. The Director shall, in conjunction with the Data Security Working Group, oversee the implementation of the Computer System Security Requirements and recommend changes to address risks, failures, or changes to business practices to the Data Security Committee.

3. The Director shall work with other University administrators to investigate any violation of this policy and any incident in which the security or integrity of University data may have been compromised, including taking the steps set forth below in response to a security breach.

4. The Director shall work with other University administrators to develop and review training materials to be used for employee training under this policy.

SECURITY RESPONSIBILITIES

1. It is the policy of the University that all Strictly Confidential, Confidential, and other sensitive information be safeguarded from unauthorized access, use, modification or destruction. All members of the University community share in the responsibility for protecting the confidentiality and security of data. This section of the policy assigns specific duties to each of the roles of Vice President and Deans, Sponsors, Data Security Officers, Users, and the Vice President for Human Resources. However, it is likely that an individual will have responsibilities reflecting multiple roles with respect to certain information.

*2. Vice Presidents and Deans.* University Vice Presidents and Deans (including the University President, and the University Provost and Dean of Faculties in connection with their immediate staff) are responsible for promoting the institutional awareness of this policy and for ensuring overall compliance with it by their staff. In particular, Vice Presidents and Deans are responsible for:

Ensuring that all staff have the training and support necessary to protect data in accordance with this policy, all Data Security Directives, and any Specific Security Procedures applicable to such data.

- Designating and managing the efforts of one or more Sponsors and Data Security Officers for all Information Resources maintained in their area of responsibility.
- Approving access authorization of all Users of Information Resources maintained in their area of responsibility having a data classification of Strictly Confidential

- Promulgating Specific Security Procedures.

- Ensuring that Strictly Confidential, Confidential and Internal Use Only data sponsored within their area of responsibility are not provided or accessible to, or created or maintained by University vendors or other third-parties without (i) assistance from the Director of Computer Policy and Security and the Director of Internal Audit, verifying that the third party has the capability of adequately protecting such data; (ii) review and approval of the relevant contract and the underlying terms and specifications by the Director of Computer Policy and Security and the Office of the General Counsel; and (iii) unless approved otherwise by the Office of the General Counsel, verifying that the third party has executed the University's standard form of Privacy and Security Addendum.

2. *Sponsors*. A Sponsor has primary responsibility for overseeing the collection, storage, use and security of a particular Information Resource. In cases where a Sponsor is not identified for any Information Resource, the cognizant Vice President or Dean shall be deemed the Sponsor. A Sponsor is responsible for the following specific tasks associated with the security of the information:

- Ensuring that the Information Resource is assigned a security classification and that such data is marked where appropriate.

- Identifying authorized Users of the Information Resource, whether by individual identification of by job title, and obtaining approval for such access from their Vice President or Dean.

- Proposing to their Vice President or Dean Specific Security Procedures for the handling of data under their sponsorship, consistent with this policy and other applicable University policies and procedures.

4 *Data Security Officers*. A Data Security Officer works with Information Technology and other appropriate University functions under the direction of a Vice President or Dean and in consultation with a Sponsor, to support the implementation and monitoring of security measures associated with the management of Information Resources. Data Security Officers shall be responsible for:

- Ensuring adequate security technology is applied to Information Resources in keeping with their classification and to comply with this policy and all Data Security Directives, and Specific Security Procedures.

- Monitoring for indicators of loss of integrity.

- Promptly reporting to the Director of Computer Policy and Security any incidents of data being accessed or compromised by unauthorized Users, and any violations of this policy, Data Security Directives or Specific Security Procedures.

- Monitoring for risks to data security and reporting any known or reasonably foreseeable risks to the Data Security Working Group

- Appointing and supervising Data Security Administrators for their area as needed.

5. *Users.* Users are responsible for complying with all security-related procedures pertaining to any Information Resource to which they have authorized access or any information derived therefrom that they possess. Specifically, a *User* is responsible for:

- Becoming familiar with and complying with all relevant University policies, including, without limitation, this policy, and all Data Security Directives contemplated hereby, the policy on Professional Standards and Business Conduct, and other policies related to data protection, technology use and privacy rights (including the University Student Education Records).

- Providing appropriate physical security for information technology equipment, storage media, and physical data. Such equipment and files shall not be left unattended without being locked or otherwise protected such that unauthorized Users cannot obtain physical access to the data or the device(s) storing the data.

- Ensuring that Strictly Confidential, Confidential, or Internal Use Only information is not distributed or accessible to unauthorized persons. Users must not share their authorization passwords under any circumstances. Users must avail themselves of any security measures, such as encryption technology, security updates or patches, provided by Data Security Officers. Users must log off from all applications, computers and networks, and physically secure printed material, when not in use.

- To the extent possible, making sure that any Massachusetts PI accessed by the User is stored only on secure servers maintained by the University and not on local machines, unsecure servers, or portable devices.

- Boston College Strictly Confidential, Confidential, or Internal Use Only data, when removed from the campus or when accessed from off-campus, is subject to the same rules as would apply were the data on campus. Sponsors and Users will comply with this Policy and all relevant Data Security Directives irrespective of where the Boston College data might be located, including, for example, on home devices, mobile devices, on the Internet, or other third-party service providers.

- When access to information is no longer required by a User, dispose of it in a manner to insure against unauthorized interception of any Strictly Confidential, Confidential, or Internal Use Only information. Generally, paper-based duplicate copies of Strictly Confidential documents should be properly destroyed. Electronic data taken from Strictly Confidential and Confidential databases should also be properly destroyed.

- Immediately notifying his or her cognizant Data Security Officer of any incident that may cause a security breach or violation of this policy.

6. *Vice President for Human Resources.* The Vice President for Human Resources shall be responsible for:

- Working with the Data Security Working Group to educate incoming employees (including temporary and contract employees) regarding their obligations under this policy and to provide on-going employee training regarding data security;

- Ensuring that terminated employees no longer have access to University systems that permit access to Strictly Confidential, Confidential, or Internal Use Only information; and

- Carrying out any disciplinary measures against an employee taken in response to a violation of this policy as required by the Data Security Committee.

SECURITY BREACH RESPONSE

As provided above, Users and Data Security Officers must report any known Security Breach or any incident that is likely to cause a Security Breach. These incidents include thefts of computer devises, viruses, worms, or computer "attacks" that may lead to unauthorized access to non-Public information.

Immediately upon becoming aware of a likely Security Breach, the Director of Computer Policy and Security shall notify the Office of the General Counsel and the Director of Internal Audit. ITS Security and Internal Audit shall conduct an investigation commensurate with the nature of the breach. The General Counsel shall determine what, if any, actions the University is required to take to comply with applicable law, including whether any notification is required under Massachusetts law. The General Counsel shall work with other administrators as appropriate to ensure that any notifications and other legally required responses are made in a timely manner. If the event involves a criminal matter, the Boston College Police Department shall be notified and shall coordinate its response with the Office of the General Counsel.

ITS Security and Internal Audit shall investigate and review the incident with the department(s) directly affected by the incident, the appropriate Data Security Officer(s). Internal Audit, in conjunction with the Director of Computer Policy and Security, shall prepare a formal report that will be distributed to the Data Security Committee and appropriate department members immediately after the investigation is finalized.

Quarterly, the Directors of Computer Policy and Security and Internal Audit will present a summary of data security investigations and/or relevant data security updates to the Data Security Committee, who shall conduct a post-incident review of events and determine, what, if any changes should be made to University practices or policies to help prevent similar incidents. The Committee shall document the University's actions in response to a Security Breach and its post-incident review in the minutes of the meeting in which the breach is discussed.

## ENFORCEMENT SANCTIONS

The University reserves the right to monitor network traffic, perform random audits, and to take other steps to insure the integrity of its information and compliance with this policy. Violations of this policy may lead to appropriate disciplinary action, which may include temporary or permanent restrictions on access to certain information or networks. Willful or repeated violations of this policy may result in dismissal from the University.

Approved: William P. Leahy, S.J.
Date: as of 6/5/2018

# Boston College Computer System Security Requirements

The University maintains a computer security system that provides at a minimum to the extent technically feasible:

1. Secure user authentication protocols including:
    a) control of user IDs and other identifiers;
    b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
    c) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;
    d) restricting access to active Users and active User accounts only; and
    e) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system.
2. Secure access control measures that:
    a) restrict access to records and files containing Strictly Confidential and Confidential information to those who need such information to perform their job duties; and
    b) assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls.
3. Encryption of all transmitted records and files containing Massachusetts PI that will travel across public networks, and encryption of all data containing Massachusetts PI to be transmitted wirelessly.
4. Reasonable monitoring of systems, for unauthorized use of or access to Massachusetts PI.
5. Encryption of all Massachusetts PI stored on laptops or other portable devices.
6. For files containing Massachusetts PI on a system that is connected to the Internet, reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the Massachusetts PI.
7. Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.
8. Education and training of employees on the proper use of the computer security system and the importance of data security.