Title: Data Security Policy
Code: I-100-200
Date: 11-6-08rev
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.

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 particular information at Boston College is governed by more specific requirements under other University policies or procedures (such as the policy concerning Student Educational 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 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.

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.

Users. Users include virtually all members of the Boston College community to the extent they have authorized access to University Information Resources, 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 and the Vice President for Human Resources.

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 Information Technology 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.

DATA CLASSIFICATION

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

- *Confidential* information includes sensitive personal and institutional information, and must be given the highest level of protection against unauthorized access, modification or destruction. Unauthorized access to personal Confidential information may result in a significant invasion of privacy, or may expose members of the University community to significant financial risk. 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, and the Gramm-Leach-Bliley Act), information concerning the pay and benefits of University employees, personal identification information or medical/health information pertaining to members of the University community, and data collected in the course of research on human subjects. Institutional Confidential information may include University financial and planning information, legally privileged information, invention disclosures and other information concerning pending patent applications.

- *Internal Use Only* information includes information that is less sensitive than 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 Information Resource are aware of its classification.

4. In the event information is not explicitly classified, it is to be treated as follows: Any data which includes any personal information concerning a member of the University community (including any health information, financial information, academic evaluations, social security numbers or other personal identification information) shall be treated as Confidential. 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 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.
- Establish data privacy and security training and awareness programs for the University community.
- Periodically reassess this policy to determine if amendments are indicated or if Data Security Directives should be proposed to the Data Security Committee.
- Review material violations of this policy and material security breaches, and recommend response actions 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 response actions in the event of any material violations of this policy or material security breaches.

2. 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 Data Security Directives.

3. The Data Security Committee is authorized to:

- Issue Data Security Directives.
- Promulgate amendments to this policy.
- 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 Data Security Directives.

SECURITY RESPONSIBILITIES

1. It is the policy of the University that all confidential and other sensitive information be safeguarded from unauthorized access, use, modification and destruction. All members of the University community share in the responsibility for protecting the security of data. This section of the policy assigns specific duties to each of the four roles of Vice President and Deans, Sponsors, Data Security Officers and Users. 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 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 Confidential.
- Promulgating Specific Security Procedures.
- Ensuring that Confidential or 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 review and approval of the relevant contract and the underlying terms and specifications by the Director of Information Technology Policy & Security, and the Office of the University General Counsel.

3. *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 Information Technology Policy and Security any incidents of data being accessed or compromised by unauthorized users, and any violations of this policy, any Data Security Directives or Specific Security Procedures.

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 of which they have possession. 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 Policy, and the University Gramm-Leach-Bliley Policy).
- 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 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.
- Users who wish to access Boston College Confidential or Internal Use Only data remotely must protect, and use the data subject to the same rules as would apply were they on campus or any Data Security Directives promulgated with respect to any remote access technologies.
- When access to Confidential or Internal Use Only data is no longer required by a User, any information extracted or copied from Information Resources must be disposed of in a manner to insure against unauthorized interception. Generally, paper-based duplicate copies of Confidential documents should be properly shredded, and electronic data taken from Confidential databases should be destroyed.

ENFORCEMENT AND 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.

Update: October 10, 2008; May 15, 2007; November 6, 2008