Data Security Policies

Title: **Data Security Policy**
Code: **1-100-200**
Date: **12-31-10rev**
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 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 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, 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 Confidential 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 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.

  Without limiting the generality of the foregoing, 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 and Confidential information also 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.

- *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, 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. 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.

3. 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.

4. 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 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 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 (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.

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 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.

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 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 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, disposing of it in a manner to insure against unauthorized interception of any Confidential or Internal Use Only information. Generally, paper-based duplicate copies of Confidential documents should be properly shredded, and electronic data taken from Confidential databases should be 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 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 confidential 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. 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: December 31, 2010rev

BOSTON COLLEGE
Data Security Policy
http://www.bc.edu/content/dam/files/offices/policies/pdf/policies/I/1-100-200.pdf

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 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.

UNIVERSITY OF FLORIDA
Information Security
https://it.ufl.edu/policies/information-security/#unrestricted

UF

UF Information Technology UNIVERSITY of FLORIDA

LEADERSHIP SERVICES GOVERNANCE POLICIES COMMUNITY

INFORMATION SECURITY

MOBILE COMPUTING AND STORAGE DEVICES POLICY

DATA CLASSIFICATION POLICY

AUTHENTICATION MANAGEMENT POLICY

RISK MANAGEMENT POLICY

ACCOUNT MANAGEMENT POLICY

BACKUP AND RECOVERY

RELATED STANDARDS AND DOCUMENTS

REMOTE ACCESS POLICY

REMOTE ACCESS

POLICIES

- Mobile Computing and Storage Devices Policy (March 1, 2013)
The University of Florida has established a policy for the use of mobile computing and storage devices, and to specify minimum configuration requirements.
- Data Classification Policy (April 26, 2012)
All data at the University of Florida is now classified into three categories: restricted, sensitive, and open.
- Authentication Management Policy (July 11, 2013)
Authentication mechanisms such as passwords are the primary means of protecting access to computer systems and data. It is essential that these authenticators be strongly constructed and used in a manner that prevents their compromise.
- Risk Management Policy (September 15, 2015)
The University of Florida has established a process to manage risks to the University of Florida that result from threats to the confidentiality, integrity and availability of University Data and Information Systems.
- Account Management Policy (January 20, 2016)
To provide a comprehensive account management process that allows only authorized individuals access to University Data and Information Systems.
- Backup and Recovery (February 20, 2016)
The purpose of this policy is to protect University Data from loss or destruction by specifying reliable backups that are based upon the availability needs of each unit and its data.
- Remote Access Policy (December 14, 2016)
The purpose of this policy is to define how the University of Florida controls Remote Access to university information systems and networks in order to prevent unauthorized use.

UNIVERSITY OF FLORIDA
Information Security
https://it.ufl.edu/policies/information-security/#unrestricted

UF

UF Information Technology UNIVERSITY of FLORIDA

LEADERSHIP SERVICES GOVERNANCE POLICIES COMMUNITY

STANDARD

MEDIA SANITIZATION STANDARD

AUDITABLE EVENTS AND RECORD CONTENT STANDARD

AUDIT AND LOGGING POLICY

CONTROL OF ELECTRONIC MEDIA

INCIDENT RESPONSE POLICY

RELATED STANDARDS & DOCUMENTS

- Definition of Terms
- Mobile Computing and Storage Devices Standard
- FAQ – Mobile Computing and Storage Devices Policy
- Authentication Management Standard
- Password Complexity Standard
- Risk Assessment Standard
- System Security Plans Standard
- External IT Vendor Sourcing Standard
- Data Classification Guidelines
- Account Management Standard
- Remote Access Standard

PDF Downloads

- Account Management Policy
- Authentication Management Policy
- Risk Management Policy
- Account Management Standard
- Authentication Management Standard
- Password Complexity Standard
- Mobile Computing and Storage Devices Standard
- Risk Assessment Standard
- System Security Standard
- External IT Vendor Sourcing Standard

JOHNS HOPKINS UNIVERSITY
Policy on Access and Retention of Research Data and Materials
http://dms.data.jhu.edu/wp-content/uploads/sites/27/2016/08/JHUDataRetentionPolicy2008_WithAppendices.pdf

JOHNS HOPKINS UNIVERSITY
POLICY ON ACCESS AND RETENTION
OF RESEARCH DATA AND MATERIALS

January 2, 2008

INTRODUCTION

The following policy paper contains parameters for Research Data and Materials Management (hereafter to be referred to as Research Data). In recent years, the amount of scrutiny and inquiry into Research Data has increased from a variety of sources, which has prompted efforts at Johns Hopkins and elsewhere to evaluate and update their Research Data Management practices.

The purpose of this policy is to protect researchers and the university. These measures are designed to address compliance requirements for researchers while diffusing some of the burden associated with Research Data Management. At Johns Hopkins, the department, research administration, divisional and university administration and the researcher are partners in managing and protecting the Research Data produced at the university.

This policy provides an umbrella approach to Research Data Management across the university. Divisional and other policies may also apply but are not to conflict with the overarching policy. This policy has been carefully designed to serve the best interests of our researchers and the university in management of Research Data. This policy is designed to complement, not supersede, other policies of the Johns Hopkins University including (but not limited to) protection of human subjects, HIPAA, intellectual property, financial management, etc. This policy does not apply to academic issues.

1. DEFINITIONS

RESEARCH DATA AND MATERIALS: Research Data is defined as information recorded in physical form, regardless of form or the media on which it may be recorded. For the purposes of this policy, Research Data is further defined as including any records that would be used for the reconstruction and evaluation of reported or otherwise published results. Research Data also includes materials such as unmodified biological specimens, environmental samples, and equipment. Examples of Research Data and Materials include laboratory notebooks, notes of any type, photographs, films, digital images, original biological and environmental samples, protocols, numbers, graphs, charts, numerical raw experimental results, instrumental outputs from which Research Data can be derived and other deliverables under sponsored agreements.

PRIMARY RESPONSIBLE INVESTIGATOR: The individual who bears primary responsibility for technical, programmatic, fiscal, and administrative requirements of the project.

2. APPLICABILITY OF POLICY: This Policy on Access and Retention of Research Data and Materials shall apply to all Johns Hopkins University faculty, staff, postdoctoral fellows, students and any other persons, including consultants, involved in the design, conduct or reporting of research performed at or under the auspices of the University.

3. OWNERSHIP OF RESEARCH DATA: The University owns all Research Data generated by research projects conducted at or under the auspices of the Johns Hopkins University regardless of funding source, unless specific terms of sponsorship, other agreements or University policy supersede these rights.

This policy does not attempt to determine relative rights of researchers and issues surrounding collaborative efforts such as authorship.

4. RETENTION AND ARCHIVING: The Primary Responsible Investigator of a research project is responsible for selection of an appropriate method of storing and archiving Research Data, and for determining what needs to be retained in sufficient detail and for an adequate period of time to enable appropriate responses to questions about accuracy, authenticity, primacy, and compliance with laws and regulations governing the conduct of research. The Primary Responsible Investigator is responsible for educating all participants in the research project of their obligations regarding Research Data, and for protection of the University's rights and ability to meet obligations related to the Research Data. The Primary Responsible Investigator should also consult with University officials regarding the development of any contingency plans.

5. RIGHTS TO ACCESS: The Primary Responsible Investigator will have access to the Research Data generated by the project. Any other faculty, staff, student or person involved in the creation of Research Data may have the right to review that portion of the Research Data that he or she created. The University will have access to the Research Data as necessary for technology transfer, compliance and other purposes. The University also has the option to take custody of the Research Data as determined by the appropriate University official. Such option will not be invoked without cause and subsequent notification of the Primary Responsible Investigator. In some instances, a research sponsor has a legal right of access or access may be requested through the sponsoring agency under the federal Freedom of Information Act (FOIA). Such requests will be coordinated through the Office of the General Counsel and/or the appropriate Research Administration Office.

6. DESTRUCTION OR REMOVAL: Research Data must be maintained for the periods required by law, University policy and sponsored agreement terms (See Appendix V). Thereafter, Research Data must not be destroyed without prior approval of the appropriate University official. With respect to removal of the Research Data, the University recognizes the importance of Research Data to the future research and career of its faculty. Therefore, should removal of Research Data be approved, for example, because of the transfer of the investigator to another institution, the following requirements apply:

I. Researchers may receive approval to remove original Research Data. The University may retain copies.
II. Research Data generated during the Researcher's employment at the University will be maintained in accordance with Johns Hopkins policy
III. Research Data that are integral to the ongoing research of another Johns Hopkins employee or student will continue to be made available for that purpose
IV. The researcher bears full responsibility for making original Research Data available to Johns Hopkins or federal and legal entities upon request.

Others involved in the project may remove copies (but not originals) of the Research Data with permission of the Primary Responsible Investigator.

7. MAINTENANCE AND REVISION OF THE RESEARCH DATA: The Primary Responsible Investigator of the research project is the person directly responsible for maintenance of Research Data created on that project. In order to support the project's credibility and the University's rights and ability to meet obligations related to the Research Data, should any revisions to final Research Data be contemplated, the Primary Responsible Investigator must notify the appropriate offices in the University and the originator of the information. The Primary Responsible Investigator must retain the original Research Data. See also Appendix IV.

APPENDICES, WEB LINKS, AND/OR FORMS:

I. RESPONDING TO REQUESTS FOR ACCESS BY NON-HOPKINS ENTITIES UNDER FOIA (Policy and Cost Reimbursement Form)
II. TRANSFER OF RESEARCH DATA FROM JHU CUSTODIANSHIP (Optional Approval Form)
III. LINK TO UNIVERSITY POLICIES (http://jhuresearch.jhu.edu/policies.htm)
IV. APPROVED METHODS OF ARCHIVAL
V. TIME MINIMUMS FOR ARCHIVAL

APPENDIX IV

Approved Methods of Archival for Research Data

1. Requirements for the recording and storage of Research Data and material will vary by discipline. Primary Responsible Investigators should always adhere to guidance provided by funding bodies, professional guidance where available, any principles set out on the division level as well as the University's recommendation as outlined below and in records management policies endorsed by the Chief Information Officer (CIO).

2. Research Data should be stored using a method that permits a complete retrospective audit if necessary. Unless ethical/professional/local or funding body guidance requires otherwise, Research Data should be archived in a durable form and in a secure location that is immune to subsequent tampering and falsification for a minimum period of 5 years after the date of any publication upon which it is based. It is recommended good practice that evidence for research based on clinical samples or relating to public health should be retained as required by the funding agency, federal laws, or other policies of the University.

APPENDIX V

Time Minimums for Research Data Archival

Research Data	Laws, Policies and Regulations	Time Periods
Proposals not funded	Not defined, but may contain proprietary information	Not defined
Expired Grants and Contracts	- Office of Management and Budget (OMB) Circular A-110* - Grants Policy of Funding Agency	OMB - Three years after completion of the entire research project Federal - follows OMB Private – Varies--see specific policy
Clinical Trials (All relevant records)	Food and Drug Administration (FDA) Notice: "Good Clinical Practices: Consolidated Guidelines"	At least two years after the last approval of a marketing application or at least two years after formal discontinuation of clinical development of the investigational product or longer if required by contract, but in no instance less than three years after the completion of the Clinical Trial
- Patent files - Data in support of patent	U.S. Patent Law	17 years from the date of the patent application
Research Data which supported enactment of a federal, state or local law	Not defined	Indefinite

* = OMB Circular A110 Uniform Administrative Requirements for Grants and Agreements with Institutions of Higher Education, Hospitals, and Other Non-Profit Organizations"
NOTE: If a sponsored agreement exists, see specific archival requirements contained therein.

Search this site

Explore KSAS

JOHNS HOPKINS
KRIEGER SCHOOL
of ARTS & SCIENCES

The Johns Hopkins University Homewood Institutional Review Board

Home (http://homewoodirb.jhu.edu/) / Investigators (http://homewoodirb.jhu.edu/investigators/) / Data Security

Data Security

Using Personal Identifiers Security Checklist

Data Security Measures When Using Personal Identifiers

1. Avoid copying or downloading sensitive data from any administrative systems to your desktop computer, home computer, laptop, mobile device, portable storage device, etc. unless absolutely required.
2. If downloading is unavoidable:
   a. Check to see if there are unnecessary confidential data variables included in the data set, such as Social Security Numbers. If so, then delete those data variables.
   b. Ensure that if you delete private information using a “track changes” feature, that you “accept all changes” and save your document in final form, not showing your markup.
   c. When possible, use a random study ID number to identify the data from each subject, and store the code or link in a location that is physically separate from the dataset itself.
   d. Encrypt the data
   e. Password Protect the data
   f. Physically protect devices that can be easily moved such as a laptop
   g. Use remote “Kill” functionality where possible.
3. Never store your subjects’ personally identifiable information on your

laptop, portable storage device, or any other device that can be lost or stolen. Instead, use a secure server.

4. Never store unencrypted data on a portable device.
5. If backing up data is required, ensure that backups are encrypted.
6. Avoid accessing personal information from computers in hotels, business centers, or any other public access locations. Remove temporary files that are created when using the internet, such as those found in browser caches and temp files.
7. If you need to use the original data collection forms and they contain personal identifiers associated with each subject, lock the originals away and use redacted copies.
8. If you store hard copies in a file cabinet or desk drawer, you must lock that storage unit. It is also preferable to be able to lock the door of the room in which the data is stored. Since several different standard file cabinets may be opened with the same key, it is advisable to get an external security bars for each of your cabinets.
9. Do not leave sensitive data unattended on a copier, printer or fax machine.
10. Dispose of documents and disks securely; use a shredder.
11. Ensure that your computer is sanitized as part of disposal.
12. Promptly report lost or stolen devices.

Title/Topic: Security of Data
Number: 6.20
Functional Classification: Information Technology
Monitoring Unit: Information Technology Services
Initially Issued: October 3, 2006
Last Revised: May 20, 2009
Last Reviewed:

SECURITY OF DATA

PURPOSE

This Policy Statement outlines the responsibilities of all *users* in supporting and upholding the security of *data* at Louisiana State University ("LSU" or the "University") regardless of *user's* affiliation or relation with the University, and irrespective of where the *data* is located, utilized, or accessed. All members of the University community have a responsibility to protect the confidentiality, integrity, and availability of *data* from unauthorized generation, access, modification, disclosure, transmission, or destruction. Specifically, this Policy Statement establishes important guidelines and restrictions regarding any and all use of *data* at, for, or through Louisiana State University. This policy is not exhaustive of all *user* responsibilities, but is intended to outline certain specific responsibilities that each *user* acknowledges, accepts, and agrees to follow when using *data* provided at, for, by and/or through the University. Violations of this policy may lead to disciplinary action up to and including dismissal, expulsion, and/or legal action.

DEFINITIONS

For the purposes of this Policy Statement, the following definitions shall apply:

Computing resources: shall be defined as all devices (including, but not limited to, personal computers, laptops, PDAs and smart phones) owned by the University, the user or otherwise, which are part of or are used to access (1) the LSU network, peripherals, and related equipment and software; (2) *data* communications infrastructure, peripherals, and related equipment and software; (3) voice communications infrastructure, peripherals, and related equipment and software; (4) and all other associated tools, instruments, facilities, and the services that make use of any technology resources owned, operated, or controlled by the University. *Computing resources* or components thereof may be individually assigned or shared, single-user or multi-user, stand-alone or networked, and/or mobile or stationary.

Data: shall include all information that is used by or belongs to the University, or that is processed, stored, maintained, transmitted, copied on, or copied from University *computing resources*.

Data Steward(s): shall be defined as the *functional unit(s)* that is responsible for the

collection, maintenance, and integrity of the *data*.

Functional unit(s): shall include any campus, college, program, service, department, office, operating division, vendor, facility *user,* or other person, entity or defined unit of Louisiana State University that has been authorized to access or use *computing resources* or *data*.

Least privilege: shall be defined as the principle that requires each person and/or functional unit be granted the most restrictive set of privileges needed for the performance of authorized tasks.

*"***Protected information:** shall be defined as *data* that has been designated as private or confidential by law or by the University. *Protected information* includes, but is not limited to, employment records, medical records, student records, education records, personal financial records (or other personally identifiable information), research *data*, trade secrets, and classified government information. *Protected information* shall not include public records that by law must be made available to the general public. To the extent there is any uncertainty as to whether any *data* constitutes *protected information*, the *data* in question shall be treated as *protected information* until a determination is made by the University or proper legal authority.

User(s): shall be defined as any person or entity that utilizes *computing resources,* including, but not limited to, employees (faculty, staff, and student workers), students, agents, vendors, consultants, contractors, or sub-contractors of the University.

GENERAL POLICY

Louisiana State University *functional units* operating or utilizing *computing resources* are responsible for managing and maintaining the security of the *data*, *computing resources* and *protected information. Functional units* are responsible for implementing appropriate managerial, operations, physical, and technical controls for access to, use of, transmission of, and disposal of *data* in compliance with this policy. This requirement is especially important for those *computing resources* that support or host critical business functions or *protected information*.

Protected information will not be disclosed except as provided by University policy and procedures, or as required by operation of law or court order.

Any electronic *data* of the University shall be classified as public, private, or confidential according to the following categories:

- Public *data* - Public *data* is defined as *data* that any person or entity either internal or external to the University can access. The disclosure, use, or destruction of public *data* should have no adverse effects on the University nor carry any liability (examples of public *data* include readily available news and information posted on the University's website).

- Private *data* - Private *data* is any *data* that derives its value from not being publicly disclosed. It includes information that the University is under legal or contractual obligation to protect. The value of private *data* to the University and/or the custodian of such *data* would be destroyed or diminished if such *data* were improperly disclosed to others. Private *data* may be copied and distributed within the University only to authorized users. Private *data* disclosed to authorized, external users must be done in accord with a Non-Disclosure Agreement (examples of private *data* include employment *data*).
- Confidential *data* - Confidential *data* is *data* that by law is not to be publicly disclosed. This designation is used for highly sensitive information whose access is restricted to authorized employees. The recipients of confidential *data* have an obligation not to reveal the contents to any individual unless that person has a valid need and authorized permission from the appropriate authority to access the *data*, and the person revealing such confidential *data* must have specific authority to do so. Confidential *data* must not be copied without authorization from the identified custodian (examples of confidential *data* include personally identifiable information in student education records, and personally identifiable non-public information about University employees).

Please see Classification of Data for a general guide to determine which data classification is appropriate for a particular information or infrastructure system.

Although some protected information, private data, and confidential data the University maintains may ultimately be determined to be "public records" subject to public disclosure, such status as public records shall not determine how the University classifies and protects data until such a determination is made. Often public records are intermingled with confidential data and protected information, so all the information and data should be protected as confidential until it is necessary to segregate any public records.

It shall be the responsibility of the *data steward(s)* to classify the *data, with input from appropriate university administrative units and legal counsel*. However, all individuals accessing *data* are responsible for the protection of the *data* at the level determined by the *data steward(s)*, or as mandated by law. Therefore, the *data steward(s)* are responsible for communicating the level of classification to individuals granted access. Any *data* not yet classified by the *data steward(s)* shall be deemed confidential. Access to *data* items may be further restricted by law, beyond the classification systems of Louisiana State University.

All *data* access must be authorized under the *principle of least privilege,* and based on minimal need. The application of this principle limits the damage that can result from accident, error, or unauthorized use. All permissions to access confidential *data* must be approved by an authorized individual, and written or electronic record of all permissions must be maintained.

Protected information shall not be provided to external parties or *users* without approval from the *data steward.* In cases where the *data steward* is not available, approval may

be obtained by the Director or Department Head of the office in which the *data* is maintained, or by an official request from a senior executive officer of the University (i.e., President, Chancellor, Executive Vice Chancellor/Provost, or Vice Chancellor).

When an individual that has been granted access changes responsibilities or leaves employment, all of their access rights should be reevaluated and any access to *protected data* outside of the scope of their new position or status should be revoked.

Data that is critical to the mission of the University shall be located, or backed up, on centralized servers maintained by the institution, unless otherwise authorized by the *data steward* of that *data,* or Office of the Vice Chancellor for Information Technology (OVCIT).

In the interest of securing information protected under FERPA, GLBA, HIPAA, other state and federal legislation, University policies (e.g. PS-113: Social Security Number Policy), and reducing the risks to the University of fines and other penalties, all users of *computing resources* shall follow Best Practices for Confidential, Private, or Sensitive Data and Best Practices for Securing Systems.

NOTE: *Please see Data Encryption for options to secure data.*

PROCEDURES

Complaints or concerns about violations of this or other technology policies should be sent to security@lsu.edu. After verification is complete using system or other logs, and in accordance with other applicable policies and procedures, the incident will be reported to the appropriate Dean, Director, or Department Head for review and possible action.

SOURCES

PS-1 Equal Opportunity
PS-06.15 Use of Electronic Mail (E-mail)
PS-06.25 Privacy of Computing Resources
PS-10 Internal and External Communications/Advertisements
PS-30 Privacy Rights of Students (Buckley Amendment)
PS-40 Employee Records Confidentiality
PS-107 Computer Users' Responsibilities
PS-113 Social Security Number Policy
PS-114 Security of Computing Resources
LSU Code of Student Conduct
PM-36 Louisiana State University System Information Security Plan
The Louisiana Database Security Breach Notification Law (Act 499)

UMassAmherst
Information Technology

Published on *UMass Amherst Information Technology* (http://www.umass.edu/it)

University of Massachusetts Amherst Information Security Policy – DRAFT [1]

February 23, 2018

I. Introduction

Institutional information, research data, and information technology (IT) resources are critical assets necessary for the University of Massachusetts Amherst ("UMass Amherst") to fulfill its missions. To maximize the preservation and protection of these assets, and to manage the risks associated with their maintenance and use, this policy establishes information security governance structure, rules, technical standards, and procedures.

By approval of UMass Amherst's Chancellor, this policy exists in conjunction with all other institutional policy.

II. Policy Statements

Information security is the responsibility of every user of institutional information, research data, and information technology resources. All users who create, access, manage, or manipulate institutional information, research data, or information technology resources must comply with this policy's administrative, technical, and physical safeguards.

A. Governance

This policy establishes campus information security governance with the creation of roles and responsibilities.

- Information Security Program Management
  - Chancellor
  - Vice Chancellor and Chief Information Officer
  - Chief Information Security Officer
  - Vice Chancellors and Deans
- Information Categorization and Management
  - Data Stewards o Steward Delegate
  - Data Administrators
  - Subject Matter Experts
  - Data Custodians
- Information Security Program Implementation
  - Vice Chancellors and Deans
  - Department Chairs, Directors, Supervisors, etc.
  - Security Liaisons
  - Chief Technology Officer
  - Service Administrator
  - Users

Additional details regarding the specific roles in these categories are in section IV.

B. Information Incident Reporting

All users must report incidents involving unauthorized access to institutional information, research data, and information technology resources to the Chief Information Security Officer. You may also report them to your local information security liaison and to the UMass Amherst IT Security Team. For more information, see: https://www.umass.edu/it/security/incident-reporting [2]

C. Institutional Information and Research Data Categorization

Institutional information and research data will be categorized in alignment with federal regulations, contractual obligations, and information risk*. Specific technical controls adhere to each category. Data Stewards are responsible for the Categorization of institutional information and research data under their purview. Data Custodians are responsible for using the appropriate security controls associated with each data category.

For more information regarding the categorization of institutional information and research data, see: https://www.umass.edu/it/security/data-categorization [3]. For more information regarding the specific technical controls that adhere to each category, see: https://www.umass.edu/it/security/controls [4].

* The standards are adapted from the Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems (FIPS 199) available at http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf [5].

III. To Whom This Policy Applies

This policy applies to every user (including, but not limited to, all faculty, students, staff, contractors, visiting researchers, or guests and volunteers) who accesses, manages, or manipulates institutional information, research data, or information technology resources.

IV. Responsible Parties

Every person at UMass Amherst has a responsibility to protect institutional information, research data, and information technology resources that they use or are otherwise within their control. These responsibilities vary based on the functional role of the individual. Depending on those functions, some individuals may have more than one role. This section identifies roles and their corresponding responsibilities. For more information and examples, see: https://www.umass.edu/it/security/roles [6].

A. Information Security Program Management

The following roles have responsibility for University of Massachusetts Amherst information security framework, oversight, and assistance.

1. Chancellor

The Chancellor has primary responsibility for campus information security and safety. The Chancellor may delegate authority for information security to the Vice Chancellor for Information Services and Strategy and Chief Information Officer.

2. Vice Chancellor for Information Services and Strategy and Chief Information Officer (CIO)

As a delegate of the Chancellor, the Vice Chancellor for Information Services and Strategy and Chief Information Officer, will provide executive oversight to the University of Massachusetts Amherst Information Security Program.

3. Chief Information Security Officer (CISO)

The Chief Information Security Officer is the University official with the authority to harmonize campus information security. The CISO is responsible for the development, implementation, and maintenance of a comprehensive information security program.

4. Vice Chancellors and Deans

The Vice Chancellors and Deans are responsible for program management oversight for the security of institutional information, research data, and information technology resources within their areas of purview.

B. Information Categorization and Management

As noted in Section II C, institutional information and research data will be categorized in alignment with federal regulations, contractual obligations, and information risk. Specific technical controls adhere to each category. Data Stewards are responsible for the categorization of institutional information and research data under their purview and the implementation of the specific technical controls that adhere to each category. Data Custodians are responsible for following the rules set by the Data Stewards. For more information see: https://www.umass.edu/it/security/information-management [7].

1. Data Stewards

Stewards have the highest level of responsibility for overseeing the categorization of institutional information and research data, and administering the privacy, security, and regulatory compliance of data sets under their purview (e.g., education records, human resources, and financial data). In the case of research data, in additional to acting as a Data Custodian, the Principal Investigator acts as the steward in consultation with research staff.

2. Steward Delegate

A steward may designate a delegate who will act on behalf of the steward for a portion or all the information and data under their purview. The delegate should be identified in writing to the Vice Chancellor for Information Services and Strategy and CIO as well as the Chief Information Security Officer, along with how long the delegation will be in place.

3. Data Administrators

Data Administrators are those individuals who are responsible for a particular line of business or who may have special knowledge of and responsibility for the compliance requirements for certain information or datasets. They have responsibility to inform the appropriate Steward(s) of any requirements or considerations that may influence policy, and set procedures, standards, or guidelines.

4. Subject Matter Experts

Subject Matter Experts are those individuals in roles with expertise such as risk, legal, compliance, privacy, and security who have a responsibility to inform the appropriate Steward(s) of any requirements or considerations that may influence policy, and set procedures, standards, or guidelines.

5. Data Custodians

Custodians are any individuals (employees, volunteers, etc.) who access, manage, or manipulate institutional information or research data. Custodians must follow campus policy and stewardship rules for handling of institutional information and research data.

C. Information Security Program Implementation

1. Vice Chancellors and Deans

In addition to the responsibilities of Vice Chancellors and Deans as noted in Section IV A 4 above, Vice Chancellors and Dean also have responsibility oversight for the implementation of the information security program within their areas of purview.

2. Department Chairs, Directors, Supervisors, etc.

Individuals who are responsible for a portion of the campus, such as a program, center, or line of business, shall develop, as needed, more restrictive information security controls for better management of risk to the institutional information or research data for which they are responsible. Supervisors may, at their discretion, create specific forms outlining the duties of their direct reports under this policy for review, signature, or workplace performance.

3. Security Liaisons

The unit security liaison is the person or persons designated by the unit head as the primary contact for the CISO. Their primary role is to share information security training in a manner that works for their unit, to be available for incidents, and provide effective communication between the UMass Amherst IT Security Team and the college or division they represent. For more information see: https://www.umass.edu/it/security/liaisons [8].

4. Chief Technology Officer (CTO)

For central information technology resources, the Chief Technology Officer, in coordination with the CISO, draws up technology architectural outlines, issues standards, and develops uniform templates for use by central IT and the campus community. For current technical architectural outlines, standards, and templates, see: https://www.umass.edu/it/architecture [9]. (Protected by NetID)

5. Service Administrator

A Service Administrator (e.g., application administrator, system administrator, or network administrator) is the individual with principal responsibility for the installation, configuration, and ongoing maintenance of an information technology system.

6. Users

In accordance with this policy, users must be aware of the value of information. They must protect information reasonably. Users must therefore follow the requirements for:

- Information technology resources
- Institutional information
- Research data

V. Standards

The user of every device connected to the campus network or that stores or transmits institutional information and research data is responsible for adherence to security control standards.

IT administrators either in UMass IT or in specific colleges or units may do the actual installation and configuration work, but it remains the responsibility of the user of that device to have those controls installed, configured and up to date (even if that simply means that when prompted to keep a computer on for its update, the user will comply with the prompt).

Faculty, staff, and researchers who do not have or accept IT administration support are still subject to these rules and assume all responsibility for maintaining up to date controls on their devices that store or transmit institutional information and research data. This rule applies whether it is an institutionally owned device or personal, and whether it is on the campus network while physically on the campus or from a remote location.

A. Technology Standards

All information technology resources, regardless of ownership, that contain institutional information or research data must have the following foundational information security controls in place and functioning. Alternative, but equally effective, controls may be substituted in accordance with the exception process. Additional controls may be required based on the categorization of the information or data, the nature of the information technology resource, the applicable regulatory or contractual requirements, or other risk management calculations. For more information see: https://www.umass.edu/it/security/controls [4].

1. Foundational Information Security Controls

The five foundational information security controls identified at the time of this policy's publication are referenced below. For additional information, or to see a complete, updated list of foundational information security controls, see https://www.umass.edu/it/security/controls [4]

a) Patch Management

Security patches must be installed, operational and regularly updated on all information technology resources.

b) Anti-Malware

Anti-malware solutions must be installed, operational and regularly updated for applicable information technology resources.

c) Firewall

Software to block incoming connections, unless explicitly allowed, must be installed and configured on applicable information technology resources.

d) Encryption

All institutional information and research data stored on end-user devices must be encrypted.

e) Secure Disposal

All information technology resources that contain institutional information or research data must be disposed of in an authorized manner.

B. User Account Standards

The campus owns all accounts, including NetID. IT creates and provisions these accounts to users for the purposes of accessing university resources. All users have a responsibility to protect the university accounts under their care. Protection of these accounts

may vary according to the risk that they present. Accounts with enhanced privileges may have additional requirements. For additional information including account standards, and password complexity rules, see: https://www.umass.edu/it/security/access [10].

At a minimum, all accounts must adhere to the following:

1. Credential Sharing

Credentials for individual accounts must not be shared.

2. Password Complexity

UMass Amherst IT sets password complexity requirements for your NetID. It is against policy for a user to subvert those requirements. Other password protected accounts must establish passwords with equivalent or greater complexity as the NetID requirements.

VI. Terms and Definitions

Assets: Information technology resources, such as hardware and software, institutional information, research data, and intellectual property.

Availability: Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

Custodians: See "Institutional Information and Data Custodians" below.

Data Categorization: See "Institutional Information and Research Data Categorization".

Data Custodians: Any individuals (employees, volunteers, etc.) who access, manage, or manipulate institutional information or research data. Custodians must follow campus policy and stewardship rules for handling of institutional information and research data.

End-User: Anyone who consumes an information service. For more information see "User".

End-User Devices: Information Technology system operated by users; e.g. Desktop and Laptop computers, Mobile phones, tablets, etc.

Information security: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Information Security Incident: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Information Service: A collection of information technology systems through which a user can access, manipulate, or create campus assets.

Information Technology (IT) Resources: Anything that generates, stores, processes or transmits electronic information. This includes end-user devices and information technology systems.

Information Technology System: A subset of information technology resources that collectively provide an information service to end-user devices.

Institutional Information: Any information, regardless of medium, in the furtherance of the campus mission, excluding research data.

Institutional Information and Research Data Categorization: The exercise of mapping data to the appropriate security categories as identified in FIPS-199.

Integrity: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

Network: A group of information technology resources and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users.

Research Data: All recorded information, regardless of medium, and all actual samples or examples, that were created or gathered and that could serve to influence or support a research finding or conclusion. Data does not include such items as research papers cited by

the researcher, preliminary notes or manuscripts, reviews, or related communications, or items that are already the property of others. This definition is intended to characterize current research norms, not to modify them.

Service Security Plan: Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

User: A person who accesses, manages, or manipulates institutional information, research data, or information technology resources. This definition includes, but is not limited to, all faculty, students, staff, contractors, visiting researchers, or guests and volunteers.

VII. References

1. Confidentiality of Institutional Information Technology Resources Policy
   http://www.umass.edu/it/security/conf-policy [11]
2. Acceptable Use of Information Technology Resources Policy
   http://www.umass.edu/it/security/acceptable-use-policy [12]
3. Records Retention and Disposition Schedules
   http://www.umass.edu/records/record-retention-and-disposition-schedules [13]
4. Secure Disposal of Information Technology
5. UMass Amherst IT Security Center
   http://www.umass.edu/it/security [14]

Source URL: http://www.umass.edu/it/policies/drafts

Links:
[1] http://www.umass.edu/it/policies/drafts
[2] http://www.umass.edu/it/security/incident-reporting
[3] http://www.umass.edu/it/security/data-categorization
[4] http://www.umass.edu/it/security/controls
[5] http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
[6] http://www.umass.edu/it/security/roles
[7] http://www.umass.edu/it/security/information-management
[8] http://www.umass.edu/it/security/informationsecurityliaisons
[9] http://www.umass.edu/it/support/security/informationtechnologyarchitecture
[10] http://www.umass.edu/it/security/access
[11] http://www.umass.edu/it/security/conf-policy
[12] http://www.umass.edu/it/security/acceptable-use-policy
[13] http://www.umass.edu/records/record-retention-and-disposition-schedules
[14] http://www.umass.edu/it/security

UNIVERSITY OF MINNESOTA
Driven to Discover℠

University of Minnesota
https://twin-cities.umn.edu/
612-625-5000

UNIVERSITY OF MINNESOTA

ADMINISTRATIVE PROCEDURE

Sharing Data with University Educational and Administrative Audiences

Related Policy: Internal Access to and Sharing University Information

This procedure provides guidance on how and when members of the University community can share public or private unit record data and or aggregate-level data with audiences internal to the University. This procedure applies to all University providers of data, including individuals and units, including central units (e.g., Office of Institutional Research, central-work streams such as Human Resources, etc.), as well as colleges, departments and other units.

Individuals or units providing data in any form, including the secondary release of data, are responsible for the application of this procedure and its related policy (see Administrative Policy: *Public Access to University Information*).

The standard for sharing personally identifiable private student data is defined in the Regents Policy on Student Education Records. The policy defines "legitimate educational interest" as "an interest in reviewing student education records for the purpose of performing an appropriate University research, educational, or administrative function. The University uses the same definition of "legitimate educational interest" for sharing other private data on individuals within the University.

Definitions

Unit Record Data is considered non-aggregated data at the lowest level of detail (e.g., individual student or employee level data).

Public Data is defined by Minnesota Statutes as "data collected, created, received, maintained or disseminated by a government entity" unless classified as private by statute or federal law. For purposes of this procedure, public data are those data elements that are non-FERPA suppressed. All other data are considered private. For a list of public and private data elements see the *list of examples* provided through Administrative Policy: *Public Access to University Information*.

Providers refer to individuals responsible for providing data in any form to those audiences requesting either aggregated data or detail unit record data.

Internal audiences are defined as current University employees (non-student) who have a need to know for the purpose of performing appropriate University research, educational, or administrative function and whose work assignment reasonably requires access (see the below standard).

Out of Scope

Private data (e.g., *HIPAA*, social security numbers, *PCI DSS*) that is classified as Private-Highly Restricted as defined in Administrative Policy: *Data Security Classification* will not be shared in this manner and are out of scope for this procedure.

Those receiving requests (providers) from University of Minnesota faculty and researchers should be directed to the procedure for "Sharing Data with University Faculty and Researchers".

Those receiving requests (providers) for data from external University audiences should be directed to the procedure for "Sharing Data with Audiences External to the University".

Procedural Guidelines for Sharing Data with Internal Audiences

1. Those requesting private data need to demonstrate a "legitimate educational interest". At the discretion of the data owner or data provider and on a case by case basis; requests may require review and approval by the owner of the requested content.
2. At the discretion of the data owner or provider, requests may require follow up with the respective department head, dean's office or administrative office of those requesting data to determine appropriate use and to determine if requester's work assignment reasonably requires access.
3. Providers determine if the request is for public, private, or a combination of public and private data. For a list of public and private data elements see the appendix: *Examples of Public, Private and Confidential Information* in Administrative Policy: *Public Access to University Information*.
4. If all data being requested are classified as public, providers may share the data with internal audiences in unit record form or in aggregate form no matter the cell size (see Table 1.0 below).
5. Aggregate data that is classified as private may be shared with internal audiences assuming the requester has a business need to know to perform their job duties. (see Table 1.0 below).
6. Those who do not meet the need to know requirement should be directed to the public reports available (see Administrative Procedure: *Sharing Data with Audiences External to the University*).
7. The completion of an *Access Request Form* (ARF) will be required for those requesting access to private unit record data used for query/direct access to the Data Warehouse and other PeopleSoft sources and approved by the respective data owner.
8. When sharing the data, providers should limit the data and reporting to the scope, depth and breadth that is consistent with the requester's needs.
9. Data suppression or masking is not needed for reporting containing only public data
10. Data will be shared in a number of ways including following methods:
    a. Through the web (e.g., *www.oir.umn.edu*)
    b. Through ad hoc reporting requests
    c. Through secondary release via subsidiary reporting systems

Table 1.0 – Summarizing requirements for sharing data with audiences internal and external to the University including University faculty and researchers

		A	B	C	D
		Public Data		**Private Data**	
Audiences to Share Data with	**Item**	**Aggregate**	**Unit Record**	**Aggregate**	**Unit Record**
Internal Audiences (with need to know)	**1**	Yes	Yes	Yes	ARF
Audiences External to the University	**2**	Yes	Yes	Suppression	No
University of MN Faculty and Researchers	**3**	Yes	Yes	Case-by-case	Case-by-case

Table Descriptions:

1. 1D = Access Request Form (ARF) used by those requesting query access to data
2. 2C = Suppression should be applied with no more than one private data element per aggregate
3. 2D = Private unit record data will not be shared; however appeals can be sent to the OGC
4. 3C = Requests will be reviewed on a case-by-case basis and may require a non-disclosure agreement
5. 3D = Requests will be reviewed on a case-by-case basis and may require a non-disclosure agreement

General Notes:

1. Suppression involves applying the rule of five to summarized data through the use of percentages, ranges or masking
2. Unit Record Data refers to individual student and employee level data
3. Aggregate refers to the summarization of unit record (detail) data
4. OGC refers to the Office of the General Counsel

All questions about this procedure or how to apply it should be routed to Data Governance by sending an email to *edmr@umn.edu*.

UNIVERSITY of VIRGINIA

INFORMATION SECURITY AT UVA

INFORMATION POLICY LIBRARY

HOME / INFORMATION POLICY LIBRARY / DATA PROTECTION

Data Protection

ABOUT

Users must comply with all University policies and standards for the data to which they have been granted the ability to view, copy, generate, transmit, store, download, or otherwise acquire, access, remove, or destroy. Users must also meet any additional compliance requirements for data protection stipulated by various governmental, legal, or contractual entities.

POLICY

Data Protection of University Information (IRM-003)

STANDARDS

Electronic Data Removal

Electronically Stored Information Release

Highly Sensitive Data Protection Standard for Individual-Use Electronic Devices or Media

University Data Protection Standards (UDPS 3.0)

University Use of Highly Sensitive Data

PROCEDURES

Electronic Data Removal Procedures

Electronically Stored Information Release Procedures

Highly Sensitive Data Protection Procedures for Individual-Use Electronic Devices or Media

Procedures on the Use of Data Loss Prevent (DLP) Tools

GUIDANCE

Electronically Stored Information Release - Guidance for Authorizing Officials

Security Tools

Printer-friendly version

REPORT AN INFORMATION SECURITY INCIDENT

Please report any level of incident, no matter how small. The Information Security Office will evaluate the report and provide a full investigation.

COMPLETE REPORT FORM

UNIVERSITY of VIRGINIA

2400 Old Ivy Road
P.O. Box 400898
Charlottesville, VA 22904

EMAIL: Information Security

UVA POLICE

UVA EMERGENCY

UNIVERSITY OF VIRGINIA
Information Security at UVA | Information Security
http://security.virginia.edu/information-security

UNIVERSITY of VIRGINIA

INFORMATION SECURITY AT UVA

INFORMATION POLICY LIBRARY

HOME / INFORMATION POLICY LIBRARY / INFORMATION SECURITY

Information Security

ABOUT

Owners and overseers of the University's information technology (IT) resources must take reasonable care to eliminate security vulnerabilities from those resources.

POLICY

Information Security of University Technology Resources (IRM-004)

STANDARDS

Elevated Workstation Privileges

Information Security Risk Management

Reporting an Information Security Incident

Revoking Information Technology Resource Privileges

Security of Network-Connected Devices Standard

PROCEDURES

Information Security Risk Management Procedures

Reporting an Information Security Incident Procedures

Revoking Information Technology Resource Privileges Procedures

GUIDANCE

Information Security Incident Response Guidelines for IT Professionals

Printer-friendly version

REPORT AN INFORMATION SECURITY INCIDENT

Please report any level of incident, no matter how small. The Information Security Office will evaluate the report and provide a full investigation.

COMPLETE REPORT FORM

2400 Old Ivy Road
P.O. Box 400898
Charlottesville, VA 22904

EMAIL: Information Security

UVA POLICE

UVA EMERGENCY

SECRETARIAT

Guidelines for Managing Student Information for Faculties, Academic Departments and Schools

February 1, 2012

Endorsed by Graduate Operations Committee, Undergraduate Operations Committee and Deans' Council

Scope and Purpose

Student information maintained in faculties, academic departments, and schools may include information on which the admission decision was based; information regarding performance in classes and the completion of program milestones; information related to academic advising and information related to accommodation for special circumstances, petitions, discipline, grievances, and appeals. The information which the university collects, creates, and maintains about students is personal information under Ontario's Freedom of Information and Protection of Privacy Act (FIPPA).

These guidelines are a resource for faculty and staff members who manage student information. They are intended to promote awareness of the university's obligations under FIPPA, to highlight university policies and procedures relevant to student information, and to provide recommendations and best practices for managing student information.

Statutory and Policy Requirements

Faculty and staff who create or maintain student information should be familiar with the following legislation, university policies, and breach response procedure:

- *FIPPA*
- Policy 46: Information Management
- Information Security Breach Response Procedure

Responsibilities

The Registrar's Office and the Graduate Studies Office are responsible for managing the university's general, contractual relationship with undergraduate and graduate students respectively. These offices are responsible for the official student academic record maintained in the student information system (Quest).

Faculties, academic departments and schools, and associated academic support units such as Cooperative Education and the Centre for Extended Learning are responsible for managing the university's relationship with the student as a learner. They create the supporting information that documents the student's academic career including achievement in individual courses, fulfilment of program milestones and other requirements, and program completion. This information is often forwarded to the Registrar's Office or the Graduate Studies Office to authorise updates to the core student record in Quest.

Faculty associate deans, directors of schools, and chairs of academic departments are responsible for ensuring that student information created and/or maintained in their departments is kept securely and retained and disposed of according to the university's approved policies and procedures. This responsibility extends to information such as class grades, assignments, and examination papers that are often managed on a day to day basis by individual faculty members and other course instructors.

All faculty and staff are responsible for ensuring that they are managing student personal information in accordance with FIPPA and the university policies listed above. New faculty and staff members, including part-time instructors and teaching assistants, should be made aware of their responsibilities regarding privacy and retention of student information.

Privacy

The only information about a student that is considered publicly available by the university (see Policy 46) is name, degrees received and date of graduation, faculty or college of enrolment, programs of study, merit-based awards and scholarships, and directory information used to facilitate communication among students. Individual students may

request that this information not be released. See below for information about access to and disclosure of student information.

All other personally identifiable information about a student must be kept confidential according to the requirements of university policies, FIPPA, and any other legislation relevant to particular types of records. Confidential information includes:

- student ID and other identification numbers
- biographical information, such as home address and telephone number, personal e-mail address
- educational history including classes taken or enrolled in
- assessments or opinions about the student including marks and grades, comments on student work, and reference letters
- needs-based scholarships, bursaries, or awards
- photographs
- health information

Security

Student information must be kept in secure facilities and equipment (e.g., locked rooms and filing cabinets, password protected computer systems) accessible only to staff and faculty whose work requires them to have access. The university's policy with regard to information security is Policy 46: Information Management.

Extra care must be exercised if student information is taken off-campus. The use of encryption is strongly recommended to prevent or minimize the potential for a breach. See: IST's Security Standards for Desktops and Laptops, and Data Encryption pages for more information.

Keeping student information on personal equipment is discouraged. Any student information maintained on personal equipment is subject to the same security, breach response, retention, and destruction requirements as that maintained on university equipment.

Student information stored offsite or in other parts of the university must not have personal information such as names or ID numbers on the outside of the storage containers.

Security Breaches

Most student information is subject to a security classification of "restricted." Some information might be "highly restricted" (see Policy 46). Any security breach of student information (unauthorized access or disclosure, such as the loss or theft of files, laptops, or flash drives containing student information, or misdirected e-mail, etc.) must be reported immediately to the appropriate university officer (see Information Security Breach Procedure). The Information Custodian will work with the Privacy Officer who will advise whether notice to affected individuals and the Office of the Information and Privacy Commissioner of Ontario (IPC) is required. If notice is required, the Privacy Officer will provide guidance to the Information Custodian about the contents of the notice to the individuals and will laise with the IPC.

Access to Student Information

Faculty and Staff: Access to student information should be limited to faculty and staff who need the information to do their job. Information regarding accommodation for medical reasons, information related to disciplinary procedures, and needs-based financial information is considered particularly sensitive and should be accessible strictly on a need to know basis.

Students: Under FIPPA students have the right to access most personal information pertaining to them. This right extends not only to formal student files but to personal information wherever it is maintained, including in e-mail messages. The university may refuse a student access to certain types of information, for example, evaluative material received in confidence to determine suitability, eligibility, or qualifications for admission to an academic program or suitability for an honour or award.

Students do not have the right to access the personal information of individuals other than themselves. Returning assignments or exams to students or posting grades must be done in a way which does not reveal personal information to other students in the class. For more information, see Guidelines on Returning Assignments and Posting Grades.

It is also recommended that information which pertains to multiple students, such as grade revision forms, be filed separately rather than in the files of individual students.

Disclosure of Student Information

Disclosure refers to releasing student information to any party or agency (including parents, spouses, employers, and landlords) other than the student and university faculty and staff with a legitimate need to know.

Electronic posting of student personal information (including photographs) on publicly available websites (including social media sites such as Facebook) or websites available to faculty, staff, and students requires prior notice to the students who must consent to the use of their personal information in this way.

References: Be aware that information contained in references or recommendations for students is considered the personal information of the student and therefore faculty and staff members should not provide references without the consent of the student. An email from the student asking for a reference or the student naming the referee in an application can be considered consent. Students are advised to seek the agreement of potential referees before naming them in an application.

Responding to information requests

Requests from students for letters confirming their status or other academic information must be directed to the Registrar's Office or the Graduate Studies Office. Employees should be cautious about responding to requests for student information even on an informal basis. Employees may seek advice from the Registrar's Office, the Graduate Studies Office, or the university's Privacy Officer.

Retention and Disposal of Student Information

Retention: Under FIPPA the university is required to keep personal information about students for a minimum of one year.

Beyond the one year minimum, student information must be kept only as long as necessary to complete the contractual obligations between the university and the student, to provide information on the academic achievements (such as transcripts) of the student to employers, educational institutions, licensing/regulatory bodies, and to the student him/herself, and to provide the student with appropriate support and other services.

In practice, this means that different types of student information are subject to different retention periods.

The **core academic record in Quest**, which includes data on a student's identity, years of study, grades and academic milestones, and degrees and certificates earned, is the only record that the university retains indefinitely in relation to individual students.

The university's approved retention schedules for student information can be found in the **Student Management** and **Teaching & Learning** sections of WatCLASS.

Disposal: Under FIPPA, the university is also required to dispose of personal information securely and to keep a record of the disposal. Disposal must be authorized by the unit head or his/her delegate. For more information see Records Disposal Procedures.

Copies and Non-Official Information: Faculty and staff managing student information should make a clear distinction between official records and copies and other non-official information (for more information, see Managing Transitory Records).

The following are common types of non-official student information:

- Copies of forms and other documents sent to the Registrar's Office or the Graduate Studies Office
- Copies provided to members of committees
- Database extracts

- Locally maintained databases, SharePoint sites, and other electronic collections of student information

Copies and other types of non-official student information are subject to the same security and destruction requirements as official records. Non-official information should be retained only as long as necessary for current work.

Anonymous data may be preserved. If a unit wishes to keep a database (for analysis or trend purposes, for example) which is otherwise scheduled for destruction, it may do so if all identifying information of individuals is removed from it. Assistance may be sought from the university's Privacy Officer.

Electronic versus paper documents: A common misperception is that retention and disposal rules apply only to paper documents. In fact, the same rules apply regardless of the format in which the information is maintained. Therefore, when it is time to dispose of the paper copy of a document, it also time to dispose of the electronic version and vice versa.

Legal action: Student information that is related to actual or pending litigation or a government investigation must not be destroyed even if the retention period has expired. This restriction begins from the moment when a legal action or a government investigation is reasonably foreseeable, and remains in effect until removed by the Secretary of the University. Any member of faculty or staff who suspects a legal action or investigation may be pending should ensure their department head is aware of the matter. The department head should inform the Secretary of the University. The Secretary will notify you when records should be retained.

For questions or concerns regarding retention and disposal of student information, contact the University Records Manager.

E-mail

Be aware that under FIPPA a student may request to see any e-mail about him/her sent by a faculty or staff member.

Most e-mails, such as correspondence between an instructor and a student relating to a course or relating to routine inquiries, should be retained for one year and then deleted. E-mails documenting a significant decision about a student's academic career should be retained as part of the student file.

E-mail is not secure unless encrypted. Avoid use of e-mail to transmit sensitive personal or confidential information. If you must use e-mail to communicate, consider how to minimize the consequences of unintended disclosure (e.g., by disclosing only some information or by deleting personal identifiers). If you frequently use email to send sensitive information, consider whether there are other ways to deliver the information, such as use of a SharePoint site, or a secured, shared network drive. It may be better to communicate some types of information by telephone or in person.

To minimize the potential for a breach, instructors are encouraged to correspond with students only through the students' Waterloo email addresses. It is suggested that instructors indicate on course outlines that they will only respond to emails sent from students' Waterloo email addresses. See the university's Guidelines on Use of E-mail for more information.

Best Practices for Managing Student Information

- Centralize student files where possible; this ensures that all substantive records relating to a student's academic history are located in one easily accessible location, and will mean that personal information about a student can more easily be protected as well as retrieved in the case of an information access request, dispute, or some other emergency.
- When working away from campus, access student information through central systems such as Quest or OnBase or using remote desktop, rather than by removing files.
- Include information on privacy, security, retention, and disposal of student information as part of the orientation for new faculty and other course instructors, teaching assistants, and staff members.
- Make arrangements for departing course instructors such as sessional lecturers who are leaving the university and faculty members who are retiring to leave their course records (class grades, examinations and assignments, etc.) with the academic department or school.
- File students' academic information separately from employment information (e.g., records of teaching or research assistantships, co-op or work study positions). Employment information has different retention requirements than student academic information.

- File information about multiple students separately rather than in individual student files (e.g., grade revision forms, ELPE result lists). Students may access much of their own information, but must not have access to information relating to other students.
- Keep particularly sensitive information such as discipline cases or medical information separately or in the file in a sealed envelope with access restricted only to those with a legitimate need to know.
- Make copies of student information only when absolutely necessary. Copies create extra work and extra responsibility since they are subject to the same security and destruction requirements as the official record.

Securely destroy expired student information on a regular basis – once a year or once a term is usually best – following the university's records disposal procedures