Tufts Technology Services
169 Holland Street, Suite 211
Somerville, MA 02144

Information Classification and Handling Policy

Purpose

This policy establishes a framework for classifying the confidentiality level of *institutional data*. It also establishes the requirements for maintaining the integrity and availability of *institutional data*.

This policy is part of a suite of information policies that includes:

- The Information Stewardship Policy, which presents the core principles for the stewardship of *institutional data* and *institutional systems*;
- The Information Roles and Responsibilities Policy, which defines the roles and responsibilities for individuals with respect to *institutional data* and *institutional systems*;
- The Use of Information Systems Policy, which sets forth the manner in which Tufts' *institutional systems* are to be used; and
- Additional University policies, standards, guidelines, procedures, and student, faculty, and employee handbooks, including those that address specific technologies and compliance requirements.

Scope

This policy applies to all faculty, students, staff, guests, and other persons associated with the Tufts community, regardless of affiliation. This policy applies to all *institutional data*.

Definitions

Institutional Data. All information that is created, discovered, collected, licensed, maintained, recorded, used, or managed by the University, its employees, and agents working on its behalf, regardless of ownership or origin. Such information is *institutional data* regardless of the ownership of any device, machine or equipment used to create, discover, collect, store, access, display, or transmit the information.

Institutional Systems. The electronic and physical systems owned, leased, licensed, managed, or otherwise provided by Tufts University used to create, discover, collect, store, access, display, or transmit *institutional data. Institutional systems* include, without limitation, desktop computers; laptops, telephones and other mobile devices; servers, printers, scanners, and copiers; research equipment; telephone systems, email systems, networks, databases, and cloud storage services; other software applications and services; and other devices, machines, equipment, and hardware. *Institutional systems*, such as software applications, that have been loaded onto a device, machine or other equipment that is not owned, leased, licensed or otherwise provided by Tufts, continue to be subject to the provisions of this policy.

Policy Statement

This policy provides a three-level classification scheme for the confidentiality of *institutional data* and establishes the requirements to maintain the integrity and availability of *institutional data* regardless of its ownership or origin. This policy, together with University guidelines on the handling of *institutional data* and use of *institutional systems*, supports the establishment of an appropriate level of security for *institutional data* and advances the goal of promoting and enabling the use of data in support of the University's mission.

Confidentiality

This policy establishes three levels of confidentiality for *institutional data*. All members of the community must understand the level of confidentiality for *institutional data* under their care. All members of the community must manage *institutional data* under their care, whether collecting, discovering, creating, storing, using, sharing, archiving, destroying, or otherwise handling *institutional data*, with safeguards that are commensurate with the data's level of confidentiality and the harm that would result from improper handling. This includes implementing and operating *institutional systems* that support the confidentiality of the *institutional data* under their care. Members of the University community should consult University guidelines, which provide information about the proper handling of institutional data and use of institutional systems.

Notwithstanding the definitions and examples provided below, a Data Authority may from time to time assign a different classification level for a particular data type assigned to that Data Authority, following a determination such classification will provide an appropriate level of confidentiality for the information.

Restricted Institutional Data (Highest - Level 3) 🔒🔒🔒

Data for which the unauthorized disclosure or unauthorized use may have a severe adverse effect on the university's reputation, finances, or operations, or on individuals. This classification includes data governed by privacy or information protection requirements articulated by law, regulation, contract, binding agreement, or industry groups.

Examples of data included at this level:

- Sensitive Personal Information (SPI) including:
  - Social Security numbers
  - Any other government issued numbers used for identification,
  - Individuals' financial account numbers, including bank account numbers and JumboCash account numbers
  - Biometric indicators for identity
- Protected Health Information (as defined in the Health Insurance Portability and Accountability Act (HIPAA))
- Identifiable Human Subject research data, including research data involving human subjects that are subject to the Common Rule (Federal Policy for the Protection of Human Subjects, 45 CFR 46.101 et seq)
- Cardholder data subject to the Credit Card or Payment Card Industry Data Security Standards (PCI DSS)
- Export controlled research (International Traffic in Arms Regulation (ITAR) and Export Administration Regulations (EAR))
- Attorney Client Privileged information
- Federal Information Security Management Act (FISMA) data
- Personally Identifiable Information in Student Education Records (Federal Education Rights and Privacy Act (FERPA)) unless the information is Directory Information (as defined in the applicable University FERPA policy) for a student that has not requested a Privacy Block
- Financial Customer Nonpublic Personal Information as defined in and subject to the Gramm – Leach – Bliley Act (GLBA)

- Personal Data collected or otherwise processed in such situations that cause such Personal Data to be subject to the General Data Protection Regulation (GDPR) as adopted by the European Union Parliament or similar regulations adopted in other countries
- Authentication data: passwords, keys, other electronic tokens

Confidential Institutional Data (Middle Level – Level 2) 🔒🔒

All institutional data is Confidential Institutional Data unless the data has been designated as or otherwise qualifies as either Restricted Institutional Data or Public Institutional Data. Confidential Institutional Data includes data for which unauthorized disclosure or use may have a significant adverse effect on the university's reputation, finances, or operations, or on individuals.

Examples of data included at this level:

- University ID numbers
- Some personally identifiable information not included in Restricted Institutional Data
- Faculty and staff personnel files, including compensation information, emergency contact information and personnel actions (other than SPI, which is Restricted Institutional Data)
- Admissions applications (other than SPI, which is Restricted Institutional Data)
- Alumni and donor personal data (other than SPI, which is Restricted Institutional Data)
- Individually identifiable health and medical information (if not PHI under HIPAA, which is Restricted Institutional Data)
- Financial data
- Proprietary information for university-owned inventions, for which the Office of Tufts Tech Transfer should be consulted
- University photos requiring a release
- Information related to university investments and investment planning
- Committee agenda and minutes
- Building plans and blueprints
- Aggregated public information for a significantly large number of persons, offices or departments, where the grouping of the information is of significant value in addition to the value of the individual data. For example, a list of all staff or student email addresses.

Public Institutional Data (Lowest Level – Level 1) 🔒

Data appropriately made available to all members of the University community or to the general public. This data includes data for which unauthorized disclosure or use would not have an adverse effect on the university's reputation, finances, or operations, or on individuals.

The University reserves the right to control the content, scope, volume, and format of data provided as Public information, as well as its method of disclosure and the intended audience.

Examples of data included at this level:

- Directory information (as defined in the applicable University FERPA policy), except for students that have requested a Privacy Block and except for aggregated information for a significantly large group of individuals as described above
- Fact Book data

- Information displayed on public facing web sites of the University or in University publications
- Research published with appropriate authorization
- University policies published with appropriate authorization
- Employee benefit plan coverage terms published with appropriate authorization

Integrity

All persons are responsible for maintaining the integrity of the *institutional data* that they access or use or is otherwise under their care ensuring that the *data* is complete and unaltered in all essential respects. The *Information Technology Administrators* who are responsible for implementing and operating *institutional system*s are required to do so in a manner that supports the integrity of the *institutional data* under their care.

Availability

All persons are responsible for maintaining the availability of the *institutional data* that they access or use or is otherwise under their care to persons who are permitted to use such data, ensuring the *data* is retrievable, deliverable, and understandable. The *Information Technology Administrators* who are responsible for implementing and operating *institutional systems* are required to do so in a manner that supports the availability of the *institutional data* under their care.

Policy Violation

Depending on the circumstances, and in management's sole discretion, persons who violate University policies may be denied access to *institutional data* and *systems*, and may be subject to other penalties and disciplinary action, both within and outside of the University. The University may refer suspected violations of applicable law to appropriate law enforcement agencies.

Review Entities

IT Steering Committee
Information Stewardship Subcommittee

Approval Date

September 15, 2011, revision November 6, 2012; revision June 6, 2018

Effective Dates

September 20, 2011; revision November 6, 2012; revision June 6, 2018

Executive Sponsor

Tufts Technology Services, Office of the Chief Information Officer

Policy Managers

Tufts Technology Services
Digital Collections and Archives
University Counsel

Responsible Offices

Tufts Technology Services

Digital Collections and Archives
University Counsel

Revision

The University reserves the right to change this policy from time to time. Proposed changes will normally be developed by the policy managers with appropriate stakeholders. The review entities have sole authority to approve changes to this policy.

Distribution

Related Policies

Information Stewardship Policy
Use of Information Systems Policy
Information Roles and Responsibilities Policy
Business Conduct Policy
University Records Policy