Information Security and Privacy Program for Restricted Institutional Data

TABLE OF CONTENTS

OBJECTIVE

The objective of Tufts University, in developing and implementing this Information Security and Privacy Program for Restricted Institutional Data (the "Program"), is to create effective administrative, technical and physical safeguards to protect Restricted Institutional Data and to comply with the University's privacy and security obligations under applicable laws, regulations, standards, policies, contracts and agreements.

Restricted Institutional Data is defined in the University's Information Classification and Handling Policy, and provided below under Definitions. Generally, Restricted Institutional Data includes:

1) Data subject to protection requirements imposed by law or regulation
2) Data subject to protection requirements binding on the University as provided in a contract or agreement, or as imposed by industry standards
3) Data designated to be treated as Restricted Institutional Data by the Data Authority for the data type or otherwise
4) Other institutional 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

Among the applicable laws and regulations included within this Program are:

- The Massachusetts Data Privacy Laws and Regulations at M.G.L. c. 93H, c. 93I and 201 CMR 17.00
- The Safeguards Rule issued under the Financial Modernization Act of 1999 (also known as the Gramm-Leach-Bliley Act (the GLBA)) and associated regulations
- The Payment Card Industry Data Security Standards (PCI DSS)
- The Family Education Rights and Privacy Act (FERPA) and associated regulations
- The Health Insurance Portability and Accountability Act (HIPAA) and associated regulations
- The European Union (EU) General Data Protection Regulation (GDPR) and the United Kingdom (UK) GDPR (UK GDPR), tailored by the Data Protection Act 2018 (UK DPA)

This Program is intended to support employees and all other persons associated with the Tufts community (associated persons) in meeting their stewardship obligations for Restricted Institutional Data under the Information Classification and Handling Policy, by applying safeguards that are commensurate with the data's level of confidentiality and the harm that would result from improper handling, disclosure or use.

This Program is composed of several elements, including the requirements for evaluating electronic and physical methods of accessing, collecting, storing, using, transmitting, sharing, protecting, and disposing of Restricted Institutional Data. The Program covers all forms of Restricted Institutional Data, whether it is maintained on paper, digital, or other media.

In addition to the requirements of this Program, Tufts units and departments are subject to other Tufts programs, policies, procedures, guidelines, and standards, including those established to comply with the laws and regulations referenced in this Program, and to other laws and regulations with respect to the Restricted Institutional Data specifically referenced in this Program.

In support of this Program, the University may also establish and document security plans that are developed to comply with the specific requirements of a law, regulation or industry standard applicable to Restricted Institutional Data.

DEFINITIONS OF INSTITUTIONAL DATA, INSTITUTIONAL SYSTEMS, AND RESTRICTED INSTITUTIONAL DATA

Institutional Data

As defined in the Information Stewardship Policy, institutional data is 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

As defined in the Information Stewardship Policy, institutional systems are 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 the University's policies.

Restricted Institutional Data

As defined in the University's Information and Classification Policy, Restricted Institutional Data is:

> 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 include:

- Massachusetts Personal Information (as defined in and referenced by c.93H of the Massachusetts Data Privacy Laws and Regulations),
- Sensitive Personal Information (SPI), as defined below
- Financial Customer Nonpublic Personal Information as defined in and subject to the Gramm Leach Bliley Act (GLBA)
- Cardholder data subject to the Credit Card or Payment Card Industry Data Security Standards (PCI DSS)
- 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
- Protected Health Information (as defined in the Health Insurance Portability and Accountability Act (HIPAA))
- 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 subject to the UK GDPR, tailored by the UK Data Protection Act 2018 (UK DPA)
- 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)
- Other research data subject to confidentiality, security, use and other restrictions imposed by contractual arrangements or other regulations
- Export controlled research data subject to the Department of State International Traffic in Arms Regulation (ITAR) (22 CFR §§120-130) and the Department of Commerce Export Administration Regulations (EAR) (15 CFR §§730-774)
- Attorney Client Privileged information
- Federal Information Security Management Act (FISMA) data
- Authentication data, including passwords, keys, other electronic tokens

DEFINITIONS OF SELECTED TYPES OF RESTRICTED INSTITUTIONAL DATA

Definitions of terms used in the above definition of Restricted Institutional Data are provided here to facilitate an understanding of selected types of institutional data that are classified as Restricted Institutional Data.

Massachusetts Personal Information

As defined in and referenced by c. 93H of the Massachusetts Data Privacy Laws and Regulations.

An individual's first name and last name or first initial and last name, in combination with that person's:

1. Social Security number;
2. Driver's license or other state-issued identification card number; or
3. Credit or debit card number or other financial account number, in each case with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account.

"Massachusetts Personal information" does not include publicly available information.

Sensitive Personal Information (SPI)

1. All Massachusetts Personal Information;
2. Biometric indicators (as included in the definition of personal information subject to c. 93I of the Massachusetts Data Privacy Laws and Regulations); and
3. Any government-issued identification card numbers whether issued by the United States government, a state government, or a foreign government, and includes, without limitation, passport numbers and visa numbers.

Financial Customer Nonpublic Personal Information under the GLBA (Financial Customer GLBA Data)

Any personally identifiable information:

1. A student, patient, customer or other person provides in order to obtain a financial service or product from Tufts,
2. About a student, patient, customer or other person resulting from any transaction with Tufts involving a financial service or product, or
3. Otherwise obtained about a student, patient, customer or other person in connection with providing a financial service or product to that person.

Financial Customer GLBA Data does not include publicly available information.

Examples of Financial Customer GLBA Data include addresses, phone numbers, bank and credit card account numbers, income and credit histories, account balances, tax return information, and Social Security numbers.

Cardholder Data under the PCI DSS

Payment card components that are required to be protected, including primary account number, cardholder name, expiration date, service code, card verification code, full magnetic strip data and PIN.

Personally Identifiable Information in Student Educational Records under FERPA

Personally Identifiable Information in Student Educational Records (each as defined in the statute and the associated regulations) is subject to protection under FERPA, and includes, but is not limited to:

a) The student’s name;
b) The name of the student’s parent or other family members;
c) The address of the student or student’s family;
d) A personal identifier, such as the student’s Social Security number, student number, or biometric record;
e) Other indirect identifiers, such as the student’s date of birth, place of birth, and mother’s maiden name;
f) Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or
g) Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

Protected Health Information (PHI) under HIPAA

Includes all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.” At Tufts, the School of Dental Medicine, the Human Resources Benefits Administration Office, Athletic Training, and the Health and Wellness Services on the Medford campus operate as covered entities.

“Individually identifiable health information” is information, including demographic data, that relates to:

a) the individual’s past, present or future physical or mental health or condition,
b) the provision of health care to the individual, or
c) the past, present, or future payment for the provision of health care to the individual,

and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. “Individually identifiable health information” includes many common identifiers (e.g., name, address, birth date, Social Security Number).

Personal Data under the GDPR and the UK GDPR

Any Personal Data, that is, any information relating to an identified or identifiable natural person (e.g., name, identification number, location data, online identifiers such as IP addresses, images), when any of the following circumstances apply:

a) For a Tufts program or activities established in the EEA or the UK, the Personal Data is collected or otherwise processed with respect to its activities that occur in the EEA or the UK, respectively, regardless if the processing takes place in the EEA or the UK; or
b) For Tufts programs not established in the EEA or UK, the Personal Data is of persons who are in the EEA or UK, respectively, when (i) they provide the Personal Data and (ii) they are either (A) offered goods or services by Tufts, or (B) having their behavior monitored by Tufts.

PURPOSE

The purpose of the Program includes to:

- identify reasonably foreseeable internal and external risks to the confidentiality, security, and/or integrity of any electronic, paper, or other records containing Restricted Institutional Data;
- assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Restricted Institutional Data;
- evaluate the sufficiency of existing policies, plans, procedures, protocols, information systems, internal controls and security practices, in addition to other safeguards in place to control risks;
- design and implement plans, policies, procedures, protocols, information systems, internal controls and security practices that put safeguards in place to minimize those risks, consistent with the requirements of applicable laws, regulations, and standards; and
- periodically monitor the effectiveness of those safeguards.

PROGRAM COMPONENTS

The Program includes the following components:

Information Stewards

Information Stewards are appointed within each division or school of the University. The Information Stewards shall assist their managers in implementing and maintaining the Program, using resources provided by the Program, as well as local resources.

Information Stewardship Subcommittee (ISS)

The *Information Stewardship Subcommittee (ISS)* is a subcommittee of the IT Steering Committee. The ISS's Charge includes to

- Contribute to developing university-wide policy and strategy for the stewardship of institutional data. Considerations will include information security, privacy, government and industry regulation, and information management principles.
- Consider and advise on programs and practices advancing information stewardship across Tufts.
- Promote Tufts community members' awareness of and engagement in the university's information policies and programs.

The Office of University Counsel (OUC)

The *Office of University Counsel (OUC)* handles a broad spectrum of legal issues involving the University, including operations, transactions, litigation, student issues, fundraising, government regulations, intellectual property, employment, tenure, finance, academic affiliation, and general legal policy. Its goals are to provide, manage, and coordinate quality legal services for the university; minimize legal risks and costs; reduce litigation; and promote legal compliance.

Tufts Technology Services (TTS) and TTS Office of Information Security

Viewing technology in the context of work, scholarship and campus life, *Tufts Technology Services (TTS)* is a university-wide service organization committed to delivering technology services that support Tufts' mission of teaching, learning, research, and service. TTS' staff includes Technology Information Administrators.

TTS' Office of Information Security provides University-wide information security services to support the University's academic, research, and scholarship mission. The Information Security team offers consulting services to support good Information Stewardship at Tufts, working with partners in all departments and schools to cost-effectively understand and manage risk to their sensitive information and the personal privacy of members of our community.

Data Authorities and Data Authority Delegates

Data Authorities. Each Data Authority is assigned to and has primary responsibility for a particular data type or domain, and each data type or domain generally has one Data Authority.

Data Authority Delegates. Each Data Authority may designate one or more Data Authority Delegates to whom they may delegate authority to make determinations about the data type or domain. Each Data Authority Delegate is assigned to and has primary responsibility for a particular data type or domain. Each data type or domain may have more than one Data Authority Delegate, who coordinate their work for a particular data type or domain.

Additional University Offices and Departments

Additional University offices and departments, including:

- Finance Division (Finance)
- Audit and Management Advisory Services (AMAS)
- Digital Collections and Archives (DCA)
- Office of the Vice Provost for Research (OVPR)
- Data Management staff at school libraries
- HIPAA covered entities

Training and Awareness

University provided training and awareness programs for staff on how to work with Restricted Institutional Data appropriately as part of their job responsibilities, and training and awareness programs for other members of the Tufts community.

Communication

Information, such as in policies, guidelines, standards, procedures or best practices for Restricted Institutional Data, that is disseminated to organizational units, staff, faculty, students and others with respect to Restricted Institutional Data.

Policies, Standards, Guidelines, Protocols, Procedures, and Programs

University, school and departmental policies, standards, guidelines, protocols, procedures and programs that establish required and recommended practices to protect the confidentiality, integrity and availability of Restricted Institutional Data and to comply with the requirements of applicable laws and regulations, industry standards and other university obligations.

Tools & Resources

The software, hardware, and other resources available to departments and units to help protect the confidentiality, integrity and availability of Restricted Institutional Data.

Vendor Management

The process for ensuring that vendors contractually comply with applicable law concerning the secure handling and disposition of Restricted Institutional Data and meet Tufts' legal requirements.

Monitor

The process for examining and evaluating compliance with the Program, including appropriate risk assessments and audits, when required.

Security Incident Response

The controlled process for investigating a potential information security incident, mitigating the impact of an incident, and taking appropriate notification and corrective action as necessary.

ROLES AND RESPONSIBILITIES

Tufts Technology Services

TTS, in consultation and collaboration with the Office of University Counsel (OUC), the ISS, Finance, AMAS, DCA, the OVPR, and other University offices and departments, is responsible for establishing, operating, and monitoring the Program, including managing and coordinating the following with respect to Restricted Institutional Data:

a) Developing and implementing a documented data privacy and confidentiality program
b) Planning and facilitating a University-wide outreach and awareness program
c) Advising departments and units on security measures, acceptable practices, breach notification, and data destruction procedures

d) Planning and facilitating the development and implementation of information policies and procedures
e) Developing best practices for ensuring that third party vendors comply with applicable laws and regulations concerning the secure handling and destruction of Restricted Institutional Data
f) Monitoring changes to applicable laws, regulations, standards, and best practices
g) Assessing the program for effectiveness of controls and processes

The Director, Information Security, TTS, and the Director's designees are responsible for maintaining this Program, in coordination with other employees of TTS, the ISS, the IT Steering Committee, the OUC, Finance, AMAS, DCA, OVPR, other Tufts offices and departments, and within the University's departments and units, managers, Information Stewards and other staff designated to oversee privacy or information protection requirements articulated by law, regulation, contract, binding agreement, or an industry group.

Office of University Counsel (OUC)

The OUC advises on contractual, policy, regulatory and other legal matters pertaining to the collection, use, storage, sharing and handling of Restricted Institutional Data by faculty, staff and other persons associated with the University. In addition, the OUC provides support to TTS and other University offices and departments for the oversight of the Program. The OUC is responsible for overseeing any investigation and associated actions necessitated by a possible breach of Restricted Institutional Data.

Information Stewards

Each unit or department must appoint one or more representatives as designated Information Stewards. Information Stewards are responsible for organizing and supporting the proper handling of Restricted Institutional Data in their unit or department. Information Stewards carry out their responsibilities by coordinating and collaborating with their unit or department's manager, who shares with the Information Steward responsibility for the proper management and protection of Restricted Institutional Data.

An Information Steward:

a) Knows about protecting Restricted Institutional Data in their group:
    - Regularly attends training and reviews information provided by Information Security
    - Is familiar with the laws and regulations and the University policies that apply to the Restricted Institutional Data in their group and knows whom to contact to advise on and address compliance matters
    - Is familiar with best practices for protecting Restricted Institutional Data
b) Knows and learns about their group:
    - Knows and learns about what type of Restricted Institutional Data their group uses or stores
    - Is able to describe the activities that use or store Restricted Institutional Data in their group

- Using supporting tools, documents what Restricted Institutional Data is used and how it is used

c) Consults with Information Security to evaluate and develop their group's practices to protect Restricted Institutional Data:
- Develops local policies and procedures for their group for collecting, accessing, transporting, storing, and disposing of records containing Restricted Institutional Data
- Coordinates and supports implementing University and local policies and procedures to safeguard handling Restricted Institutional Data by their group

d) For the staff, faculty, students and others that are part of their group, raises their awareness of the importance of protecting Restricted Institutional Data:
- Educates and provides training, using supplied materials
- Acts as a resource as staff and others implement practices to protect Restricted Institutional Data

e) Understands what initial steps to take if there is a possible breach of Restricted Institutional Data, including prompt reporting

Information Stewardship Subcommittee (ISS)

The Information Stewardship Subcommittee provides advice and guidance on matters concerning the proper stewardship and protection of information, information policy, and resource development for compliance with the Program and the applicable laws and regulations, policies and contractual arrangements.

Data Authorities and Data Authority Delegates

A Data Authority is designated for a grouping of a type of data. The Data Authority has the responsibility to determine what specific data within that grouping, if any, is classified as Restricted Institutional Data.

The Data Authority also:

- Identifies the federal, state, and other applicable laws and regulations; University policies, procedures, guidelines, and standards; and applicable licenses and other contracts that affect the data under their care
- Identifies authorized users of the data, whether by individual identification or by job title or role
- Develops and approves policies, guidelines, standards, and procedures specific to the particular data type or domain, defining specific access, handling, use, and management requirements
- Provides communications and education to information users on the appropriate use and care of the data
- Interprets and applies policies, guidelines, standards, and procedures for the particular data type or domain
- Coordinates with, advises, and oversees their Data Authority Delegate(s)
- Works with Information Technology Administrators to establish and maintain trustworthy information systems for the particular data type or domain
- Coordinates their work with the ISS

- Participates in meetings and deliberations of the Data Authorities

Data Authority Delegates. Data Authority Delegates process data access and use requests and apply policies, guidelines, standards, and procedures for the assigned data type or domain. They provide communications and education to information users on the appropriate use and care of the data. Data Authority Delegates may exercise some discretion in their application of policies, standards, and procedures to particular requests, based on guidance from the Data Authority. Data Authority Delegates are responsible to and report to the applicable Data Authority for their work as a Data Authority Delegate. Data Authority Delegates are required to document their determinations for all data requests. The Delegates will also work with Information Technology Administrators to establish and maintain trustworthy information systems for the particular data type or domain. Data Authority Delegates coordinate their work with the ISS and participate in meetings and deliberations of the Data Authority Delegates.

Information Technology Administrators

The Information Technology Administrators work with faculty and staff to establish and maintain trustworthy information systems for Restricted Institutional Data, including by maintaining and operating institutional systems in a manner commensurate with the confidentiality level of Restricted Institutional Data, as held or accessed by the institutional systems. Information Technology Administrators follow and implement applicable policies, guidelines, standards, and procedures with respect to managing Restricted Institutional Data. Information Technology Administrators follow and implement the decisions granting or disabling access to institutional data as made by the Data Authorities and the Data Authority Delegates. The Information Technology Administrators generally are Tufts Technology Services staff.

Digital Collections and Archives (DCA)

Digital Collections and Archives provides guidance and direction for University offices and departments, staff, faculty, and affiliates on the management of records. As part of the DCA staff, the University Record Manager's role includes providing advice on storage, retention practices and terms, and proper disposition of records containing institutional data, including Restricted Institutional Data, and developing and maintaining records retention schedules and related policies for institutional data, including Restricted Institutional Data.

Office of Vice Provost for Research (OVPR)

The OVPR works with members of the faculty and other administrative offices to support research while protecting the University's interests and assuring that Tufts is in compliance with all relevant laws and regulations, including those applicable to Restricted Institutional Data. The OVPR coordinates with other offices and departments to support the collection, use, storage, handling, sharing, and other management of research data that qualifies as Restricted Institutional Data in accordance with the University's privacy and security obligations under applicable laws, regulations, standards, policies, contracts and agreements.

Library Data Management Services Teams

Tisch Library, Ginn Library and Hirsh Health Sciences Library employ staff whose responsibilities include advising faculty, students and staff in the creation of Data Management and Data Sharing Plans and providing advice on navigating requirements for the storage, organization, sharing and use of electronic tools and resources for managing research data that qualifies as Restricted Institutional Data. These staff members collaborate with the TTS Office of Information Security, the TTS Office of Research Technology, and other TTS offices.

Audit and Management Advisory Services (AMAS)

AMAS, in coordination with TTS and other University offices, shall provide periodic assessments concerning the achievement of Program objectives and compliance with its requirements.

RESPONSE TO INTERNAL AND EXTERNAL RISKS: SAFEGUARDS AND REQUIREMENTS

To address both internal and external risks to the security, confidentiality, availability, and/or integrity of any electronic, paper or other records containing Restricted Institutional Data, Tufts shall implement the following safeguards and all persons with access to Restricted Institutional Data shall be obligated to comply with the following requirements.

Education, Training and Awareness

- The University shall make available a description or copy of the Program and any associated plans to all persons with access to Restricted Institutional Data.
- The University shall provide ongoing training to all persons with access to Restricted Institutional Data, including all persons who administer the University’s computer security systems.
- Training shall include information on the importance of Restricted Institutional Data security, the requirements set forth in this Program and in associated plans, and the obligations under applicable laws and regulations.

Access to and Collection of Restricted Institutional Data

- Access to records containing Restricted Institutional Data must be limited to those persons who reasonably require such access in order to accomplish Tufts’ legitimate business purposes, or as necessary for Tufts to comply with applicable laws and regulations.
- Employees and other associated persons may only collect, use, store, handle, or have access to Restricted Institutional Data if such information is necessary for accomplishing their job or other contractual responsibilities.
- Reading Restricted Institutional Data not directly required for job or other contractual performance, such as an employee, student, or patient record, even if

with good intentions, and even if that information is not further disclosed, is strictly prohibited.

- The amount of Restricted Institutional Data collected must be limited to that amount reasonably necessary to accomplish Tufts' legitimate business purposes, or necessary for Tufts to comply with applicable laws and regulations.
- Employees and other associated persons may only share Restricted Institutional Data with other employees and other associated persons if such information is necessary for accomplishing those persons' job or other contractual responsibilities.
- Calls or other requests for Restricted Institutional Data are to be referred to responsible individuals who are knowledgeable in the regulatory requirements applicable to the requested information.

Applications, Tools and Services

- The collection, use, storage, handling, and processing of, and the access to, Restricted Institutional Data shall be limited to methods, applications, tools and services that comply with applicable regulatory and contractual requirements for such information.
- The self-provisioning of cloud services to collect, use, store, process, or manage Restricted Institutional Data is prohibited. Tufts offices, departments, employees and others shall work with TTS in order to properly evaluate and manage the risks that come with using the service for Restricted Institutional Data.

Physical Security

- Each business unit and department must ensure that reasonable restrictions for physical access to and secure storage of records containing Restricted Institutional Data are in place.
- Access to offices must be secured by giving access only to authorized persons.
- Lost or stolen keys or identification cards that enable access are to be reported to Tufts Public and Environmental Safety promptly.
- Users must position their desktop and laptop screens so as the screens are not readily viewable by unauthorized persons. Users are required to lock their desktop or laptop screens or to log off of their device whenever they leave their device unattended.
- Access to keys and alarm, lockbox and other codes must be limited to those requiring such access. When a person who had such access is no longer employed or otherwise providing services at a site, it is strongly recommended that the code or other security method be changed immediately.
- All persons are prohibited from leaving files containing Restricted Institutional Data unattended in an unsecure area. Whenever reasonably possible, files containing Restricted Institutional Data must be shielded from view by unauthorized persons.
- At the end of the workday, all files and other records containing Restricted Institutional Data must be secured in a manner that is consistent with the Program's rules for protecting the security of Restricted Institutional Data. Paper

records must be secured by being stored in a locked file cabinet, drawer or other container, that is located in a locked space (the two-lock standard).

- Copiers, scanners, printers, and fax machines used for Restricted Institutional Data must be located in a work area during the workday and in a locked space after the workday ends.

Data Encryption

- *Encryption at Rest.* All Restricted Institutional Data when stored on a portable device, including, without limitation, laptops, tablets, mobile phones, external hard drives, usb sticks and other media to store data, must be encrypted.
- *Encryption in Transit.* All records and files containing Restricted Institutional Data transmitted across public networks or wirelessly, must be encrypted.
- Encryption here means the transformation of data through the use of an algorithmic process, or an alternative method at least as secure, into a form in which there is a low probability of meaning being assigned without the use of a confidential process or key.

Personal Devices

- No Restricted Institutional Data may be stored on any desktop, laptop, smartphone or other device unless either (a) the device is managed by TTS, or (b) the device is managed in accordance with guidelines established by TTS.
- In any event, Tufts email that contains Restricted Institutional Data may be stored on a personal smartphone only if:
  - The storage is temporary, such that the information is transferred to approved storage promptly and the information is securely deleted from email,
  - The smartphone is well-managed, in accordance with guidelines established by TTS, and
  - The use of Tufts email for Restricted Institutional Data is in compliance with TTS guidelines for email use.
- Users are encouraged to use a Tufts provisioned Virtual Desktop Interface (VDI) via the Tufts VPN to access Restricted Institutional Data when using personal devices.

Tufts Wireless, Tufts VPN, and Virtual Desktops

- When on campus, employees and other persons with access to Restricted Institutional Data may only use either an Ethernet connection to the Tufts network or the Tufts_Secure encrypted wireless service. Persons with access to Restricted Institutional Data may not use either Tufts Guest wireless or Tufts Wireless, which are not encrypted.
- When off-campus, an employee or other associated person may only access Restricted Institutional Data that is stored or processed by a Tufts application or other service by using the Tufts VPN, unless expressly authorized by the Data

Authority to use an "https" secured site or similarly encrypted service. Ideally, the VPN should still be used when off campus for all access to Tufts data.

Use of Email

- The use by employees and other persons with access to Restricted Institutional Data of any email system other than Tufts email for Restricted Institutional Data is prohibited.
- "Tufts email" refers to the @tufts.edu system. It does not include other email systems that may be established that use @[abc].tufts.edu or similar addresses.
- It is also strongly recommended that employees and other persons with access to Restricted Institutional Data use communication tools *other than* email for Restricted Institutional Data. Errors in email addresses are common, which may result in unintended disclosure of Restricted Institutional Data to unauthorized persons. Email is also a frequent target of hackers seeking to fraudulently obtain person's credentials to access Restricted Institutional Data. Therefore, all persons are advised to avoid the use of Tufts email for Restricted Institutional Data whenever reasonably feasible.
- If use of Tufts email is necessary to send or receive Restricted Institutional Data, then one of the following methods must be used:
    1. the message is sent from a name@tufts.edu to a name@tufts.edu address,
    2. the Tufts Secure Email encrypted service is used, by sending a message from a name@tufts.edu address and placing the word "secure" in square brackets in the subject line, or
    3. the information is in an encrypted, password protected document and the password is securely communicated without using email.
- Employees and other associated persons with access to Restricted Institutional Data must not enable automatic forwarding of their Tufts email account to any other email account that is not in the Tufts email system.
- In any event, Tufts email should never be used to store Restricted Institutional Data, except temporarily. Any Restricted Institutional Data sent or received through the Tufts email system should be promptly moved to secure storage and the email message should then be securely deleted following the three-step instructions provided by TTS on its website (delete, empty trash, purge).

Data Preservation and Retention

- Employees and other associated persons must store and otherwise manage Restricted Institutional Data in a manner that protects the access to the data by use of storage applications approved by TTS. Restricted Institutional Data must never be stored solely on a desktop or any portable devices, including a laptop or tablet.
    - Employees and other associated persons may not use the Box sync or other Box functions to store Restricted Institutional Data on any personal device.
    - Employees and other associated persons may not grant access to Tufts Box folders that contain Restricted Institutional Data to non-Tufts persons, unless proper authorizations have been signed and recorded.

- The retention period for Restricted Institutional Data must be limited to the period that is reasonably necessary to accomplish Tufts' legitimate business purposes, or necessary for Tufts to comply with applicable laws and regulations.
- DCA is responsible for determining retention periods for university records (including university records containing Restricted Institutional Data) in consultation with the necessary administrators and staff. DCA articulates these decisions in records retention schedules and related policies.
- The head of each business unit or department, working with Digital Collections and Archives, is required to define retention periods for records with Restricted Institutional Data in accordance with University policies and procedures.

Secure Data Destruction (Physical & Electronic)

- All Restricted Institutional Data stored electronically, on paper, or on other media that requires destruction at the end of its life cycle must be destroyed in a manner such that the information cannot practicably be retrievable, recognizable, read or reconstructed. Destruction in these circumstances will be in accordance with rules as put forth by relevant governing authorities.
- Paper documents with Restricted Institutional Data must be disposed of by either placement in a Shred-it supplied locked bin, the only authorized Tufts vendor for secure off-site shredding, or in an electronic shredder that shreds by cross-cutting (preferably by a micro-cut). Shredders that shred into strips only are not approved for destruction of documents with Restricted Institutional Data.
- Before disposal, all copiers, scanners, printers, and fax machines with a hard drive must have the hard drive securely wiped. The University has contracted with Konica to securely wipe all hard drives for copiers, scanners, printers and fax machines provided by Konica.
- All laptops, computers and other devices with a hard drive must be securely wiped prior to being re-provisioned, retired, donated, disposed of or recycled. Users may contact the TTS Service Desk to arrange for secure wiping of Tufts devices.

Working Remotely

Employees are required to comply with special restrictions that apply when working off-campus, including while travelling, to protect Restricted Institutional Data from unauthorized use and disclosure. See Technology Guidelines and Services for Working Off-Campus, Telecommuting and Personal Devices. These restrictions include:

- The use of Tufts VPN to access Tufts services
- When available, the use of the Tufts provisioned virtual desktop infrastructure
- The segregation of Restricted Institutional Data from personal information
- Restricting the access to devices used for the collection or storage of Restricted Institutional Data to Tufts authorized persons.

System and Application Passwords

- Electronic access to Restricted Institutional Data must be protected by usernames and passwords.

- All system and application passwords must be robust and changed and otherwise managed in a manner consistent with password standards adopted by TTS.
- Passwords are not to be shared by other users.

System and Application Access Control

- Access to Restricted Institutional Data must be restricted to active users and active user accounts only with a need to access the data as part of their current job responsibilities.
- As a user's role changes, prior and current management and Data Authorities (or their delegates) should review access provided to the user to ensure any access previously provided, but no longer required for the user's responsibilities, is terminated.
- Access to electronically stored Restricted Institutional Data must be limited to authorized persons having a unique log-in ID; this means users must not share a common login token or use a generic account.
- The secure access control measures in place must include assigning unique identification tokens and passwords, which are not vendor-supplied default passwords, to each person with authorized access to Restricted Institutional Data.
- Security screening of prospective and current employees and other associated persons shall be conducted in accordance with the University's departmental and Human Resources policies and procedures, including background check procedures. Some positions may require additional certifications for specific work environments or incompliance with licensure, law or regulations.
- Data Authorities, or their delegates, shall work with Information Technology Administrators to routinely review access to Restricted Institutional Data and to remove any person's access who does not require such access to fulfill their responsibilities.

Secure Authentication

There must be secure user authentication protocols in place, including:

- Documented protocols for control of user IDs and other tokens or identifiers;
- A reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies;
- 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;
- Blocking of access to user identification after multiple unsuccessful attempts to gain access where technically feasible and in accordance with TTS policies on authentication. When not feasible, exceptions must be formally documented and require approval from the appropriate manager(s) and IT unit(s); and
- Mandatory use of two-factor authentication (2FA) for applications designated by Data Authorities, university leadership and/or TTS.

Firewall, Security and System Software, and Configurations

- The University shall maintain reasonably up-to-date firewall protection and operating system security patches, designed to reasonably maintain the security and integrity of the Restricted Institutional Data, installed on all systems processing and containing Restricted Institutional Data connected to the internet.
- The University shall make available reasonably up-to-date versions of system security agent software, which shall include malware protection and reasonably up-to-date patches and virus definitions. The most current security updates shall be applied on a regular basis.
- Systems with Restricted Institutional Data shall be configured to established baseline configurations for Restricted Institutional Data and all systems shall be tracked in an inventory designating that they are systems with Restricted Institutional Data.

Suspicious Activities & Breach Reporting

- Employees shall be instructed to report any lost or stolen device on which Restricted Institutional Data was stored or any suspicious or unauthorized disclosure or use of Restricted Institutional Data in accordance with the University's policies and procedures. See Reporting Information Security Incidents.
- Employees shall be provided an opportunity to report suspected unauthorized disclosure or use of Restricted Institutional Data anonymously, such as through EthicsPoint.
- Suspected fraudulent attempts to obtain Restricted Institutional Data and other possible security incidents are to be reported promptly to the TTS Service Desk at 617 627-3376.

Third-Party Service Providers

- For services that will include Restricted Institutional Data, the University shall take reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect Restricted Institutional Data consistent with the applicable data laws and regulations.
- The University shall require such third-party service providers by contract to implement and maintain such appropriate security measures.
- Upon the termination of any arrangement with a third-party service provider of a system or application that includes storage or other processing of Restricted Institutional Data, the primary contact at the University for such third-party shall be required, with assistance from the Information Technology Administrators, to ensure that all Restricted Institutional Data stored on such system or application is either securely transferred to Tufts or securely destroyed.

Compliance with Laws and Regulations

- All employees and associated persons are required to comply with the processes and procedures of this Program and the associated plans.

- In accordance with the Information Stewardship Policy, the Information Roles and Responsibilities Policy, the Use of University Systems Policy, the Tufts' Business Conduct Policy, and the Standards of Professional Conduct and Integrity, all persons with access to Restricted Institutional Data are required to operate in compliance with applicable laws and regulations.

Employee Disciplinary Action

Tufts may take appropriate disciplinary action against employees and others for violating the provisions of this Program.

Separated Employees and other Persons

- Any employee whose employment by Tufts will have ended for any reason (a separated employee), and any person whose association with Tufts will have ended for any reason (a separated associated person) must return any and all records containing Restricted Institutional Data, in any form and on any device, that may be in the employee's or other person's possession at the time of such separation (including all such information stored on laptops or other portable devices or media, and in files, records, work papers, etc.).
- A separated employee or person's physical and electronic access to Restricted Institutional Data must be blocked as soon as reasonably possible, and the separated employee or person must be required to surrender all keys, IDs or access codes or badges, business cards, and the like, that permit access to the University's premises or information, except to the extent expressly approved in extraordinary circumstances for a particular individual by a senior administrator.

A separated employee or person must return any laptop, desktop or other device purchased or otherwise owned by Tufts immediately upon separation, except to the extent expressly approved in extraordinary circumstances for a particular individual by a senior administrator, provided, further, the device is securely wiped. In any event, any device with a hard drive must be securely wiped prior to being re-provisioned, retired, donated, disposed of or recycled.

Monitoring and Upgrades

- The University shall perform reasonable regular monitoring of its computer and information systems to ensure that this Program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of Restricted Institutional Data. The University shall upgrade its information safeguards based upon its assessment of risk.
- The University shall reasonably monitor computer and information systems that maintain or process Restricted Institutional Data for excessive access to Restricted Institutional Data or unauthorized use.
- Effective monitoring includes enabling and routinely reviewing and monitoring information system logs or audit records.

Security Scope Review and Risk Assessments

- The University shall regularly review security measures for Restricted Institutional Data, or whenever there is a material change in Tufts' business practices that may reasonably implicate the confidentiality or integrity of records containing Restricted Institutional Data.
- The University shall require routine or annual assessments of this Program.
- This Program shall identify reasonably foreseeable external and internal risks to the security, confidentiality, and integrity of Restricted Institutional Data that could result in the unauthorized disclosure, misuse, alteration, destruction, or otherwise compromise such information, and assess the sufficiency of any safeguards in place to control these risks. Risk assessments shall include consideration of risks in each area that has access to information covered by the applicable law or regulation. Risk assessments shall include, but not be limited to, consideration of employee training and management; information systems, including network and software design, as well as information processing, storage, transmission and disposal; audits, scans, penetration tests, and other methods necessary to identify vulnerabilities and measure the effectiveness of mitigating controls and response processes; and systems for detecting, preventing, and responding to attacks, intrusions, or other system failures. Risk assessments shall include system-wide risks, as well as risks unique to each area with Restricted Institutional Data.
- The Program shall verify that information safeguards are designed and implemented to control the risks identified in the risk assessments. The Program shall ensure that reasonable safeguards and monitoring are implemented and cover each office or department that has access to the in-scope Restricted Institutional Data.
- The following is a partial list of threats to Restricted Institutional Data that will be mitigated through the implementation of this Program:

    1. Unauthorized access to data through software applications
    2. Unauthorized use of another user's account and password
    3. Unauthorized viewing of printed or computer displayed data
    4. Improper storage of printed data
    5. Unprotected documentation usable by intruders to access data
    6. Improper destruction of printed material

ADDITIONAL REQUIREMENTS FOR THE GRAMM-LEACH-BLILEY-ACT (GLBA) AND THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

The GLBA mandates that the University appoint an Information Security Program Coordinator, conduct a risk assessment of likely security and privacy risks, institute a training program for all employees who have access to covered data and information, oversee service providers and contracts, and evaluate and adjust the Information Security Program periodically.

HIPAA mandates that Security and Privacy Officers must be appointed to oversee a covered entity to ensure the program meets the required safeguards for in-scope Restricted Institutional Data.

GLBA Coordinator

The GLBA Coordinator for this information security program for the GLBA is the Director of the TTS Office of Information Security. The GLBA Coordinator consults and coordinates with TTS, the OUC, Finance and the several Tufts offices that are subject to the GLBA, together with other Tufts departments, as described above in Roles and Responsibilities.

Risk Assessments

The GLBA Coordinator and HIPAA Security and Privacy Officers, as applicable, will work with all relevant offices to carry out risk assessments to identify potential and actual risks to security and privacy of the in-scope Restricted Institutional Data.

Safeguards and Service Providers

With respect to GLBA and HIPAA, the Program will include the safeguards listed above under Response to Internal and External Risks: Safeguards and Requirements. The Program shall regularly test or otherwise monitor the effectiveness of the safeguards.

With respect to GLBA and HIPAA, the Program will include the safeguards for service providers described above at Response to Internal and External Risks: Safeguards and Requirements: Third-Party Service Providers.

Adjustments to the Program

The GLBA Coordinator and the HIPAA Security and Privacy Officers are responsible for evaluating and adjusting the Program based on the risk identification and assessment activities undertaken pursuant to the Program, as well as any material changes to the University's operations or other circumstances that may have a material impact on the Program.

PROGRAM AMENDMENT

This Program may be revised or amended from time to time to update the Program's provisions to meet its objectives, upon approval by the University's Executive Vice President.

PROGRAM APPROVAL

Approved

Executive Vice President

IT Steering Committee

Information Stewardship Subcommittee

January 1, 2021: Director, Information Security, Tufts Technology Services

Approval Dates

September 6, 2016, February 26, 2010, May 14, 2019, January 1, 2021

Amended

September 6, 2016, May 14, 2019, January 1, 2021

Effective Date

March 1, 2010, September 6, 2016, May 14, 2019, January 1, 2021

Executive Sponsor

Office of the Chief Information Officer

Policy Managers

Tufts Technology Services
Office of University Counsel
Digital Collections and Archives

Implementation Priority

Tufts University places a priority on protecting combinations of Restricted Institutional Data, the unauthorized disclosure or use of which is most likely to cause substantial harm such as identity theft and major financial fraud.

Related Policies and Standards

Information Stewardship Policies:

- Information Stewardship Policy
- Use of Information Systems Policy
- Information Roles and Responsibilities Policy
- Information Classification and Handling Policy

Business Conduct Policy
Standards of Professional Conduct and Integrity