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

Information Security Program

Information Security Program to support compliance with Massachusetts laws for safeguarding Personal Information

Objective

The objective of Tufts University, in developing and implementing this Information Security Program ("Program"), is to create effective administrative, technical and physical safeguards to protect personal information, and to comply with the University's obligations under M.G.L. 93 H, 93 I and 201 CMR 17.00 (the "Data Regulations"). This Plan explains the elements of the Program Tufts intends to establish, including the requirements for evaluating its electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting personal information. The Program covers all forms of personal information, whether it is maintained on paper, digital, or other media.

For purposes of this Program, "personal information" shall have the meaning set forth in the Data Regulations. In general, "personal information" includes an individual's first name and last name or first initial and last name, in combination with that person's: (a) Social Security number; (b) driver's license or other state-issued identification card number; or (c) 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. "Personal information" does not include publicly available information.

Purpose

The purpose of the Program is to affect compliance with applicable laws (including the Data Regulations) by:

1. identifying reasonably foreseeable internal and external risks to the confidentiality and/or integrity of any electronic, paper, or other records containing personal information;
2. assessing the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information;
3. evaluating the sufficiency of existing policies, procedures, information systems, internal controls and security practices, in addition to other safeguards in place to control risks;
4. designing and implementing a plan that puts safeguards in place to minimize those risks, consistent with the requirements of Massachusetts laws; and
5. periodically monitoring the effectiveness of those safeguards.

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

Approved
Patricia Campbell, Executive Vice President

Approval Date
February 26, 2010

Effective Date
March 1, 2010

Executive Sponsor
David Kahle, Vice President for Information Technology and 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 personal information, the unauthorized disclosure of which is most likely to cause substantial harm such as identity theft and major financial fraud. High-risk personal information combinations include the use of names in combination with financial account numbers, Social Security Numbers and/or state issued ID numbers.

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

Program Components

The Program will include the following components:

a. *Information Stewards*

Information Stewards are appointed within each division or school of the University. The Information Stewards will assist their managers in developing a framework to implement and maintain the Program, using resources provided by the Program as well as local resources.

b. *Information Stewardship Committee*

Members of the Committee will provide guidance on information security policy and on the development of resources for compliance with the Program and the law.

c. *The Office of University Counsel*

The Office of University Counsel coordinates the delivery of all legal services on behalf of Tufts University. This office provides advice and support to the University's administrative and academic departments on legal matters and the development of related policy and Program oversight.

d. *Tufts Technology Services / Information Security*

Technology Services delivers information technologies to the Tufts community in support of teaching, learning, research, administration, and outreach. Technology Services' Directorate of Information Security provides technical guidance and support to the University's administrative and academic departments.

e. *Training*

The University will provide personnel training on how to handle personal information appropriately as part of their job responsibilities.

f. *Communication*

Information - such as new tools, policies, or best practices - will be disseminated to organizational units in a timely manner.

g. *Policies and Procedures*

The University will create policies and procedures to protect the confidentiality of personal information and to comply with the requirements of the Data Regulations.

h. *Tools & Resources*

The University will make appropriate software, hardware, guidelines, and other resources available to business units to help ensure the confidentiality of personal information.

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

i. *Infrastructure*

The buildings, networks, and appliances that comprise the work environment of the business units at Tufts and help support secure management of personal information.

j. *Vendor Management*

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

k. *Monitor & Audit*

The process for checking compliance with the Program.

l. *Security Breach Response*

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

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

Roles and Responsibilities

1. Office of University Counsel & Tufts Technology Services

The Office of University Counsel (OUC) together with Technology Services shall be responsible for establishing, operating, and monitoring the Program.

OUC and Technology Services are responsible for managing and coordinating the following:

a. Developing and implementing a documented information security program.
b. Planning and facilitating a University-wide outreach and awareness program.
c. Advising business 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 personal information.
f. Monitoring changes to applicable laws, regulations, standards, and best practices.

2. Information Stewards

Each business unit shall appoint a representative as a designated Information Steward. An Information Steward is responsible for the distributed implementation and maintenance of the safeguards outlined in the Program within each specific area of operation. Security responsibilities and operational requirements of this individual may be delegated to appropriate managers.

Each designated Information Steward shall be responsible for:

a. Implementing the Program within his or her business unit.
b. Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks. Risk assessment shall occur at least annually or whenever material changes to the business occur.
c. Developing security policies and procedures for employees that take into account whether and how employees should be allowed to keep, access and transport records containing personal information outside of business premises.
d. Identifying paper, electronic and other records, computing systems, and storage media, including laptops and portable storage devices used to store personal information, to determine which records contain personal information.

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

e. Working with the head of the business unit to determine the appropriate retention period for all collected personal information.
f. Ensuring that employees and others with access to personal information have been trained on their responsibilities to protect personal information. Training shall consist of materials provided by Technology Services in addition to training addenda that may be specific to the business unit's operating environment and use of personal information.
g. Ensuring that third party vendors comply with applicable laws and regulations concerning the secure handling and destruction of personal information that the Information Steward's business unit handles or is otherwise responsible for.
h. Reviewing the business unit's implementation of security measures at least annually, or whenever there is a material change in business practices that may affect the security or integrity of records containing personal information.
i. Periodic testing and validation of the business unit's compliance with Program requirements.
j. In the event of a data breach, participating with University Counsel, appropriate business unit managers, and appropriate Tufts management and IT units in the post-incident review of the events and actions taken, to determine and implement improvements and/or corrective action.
k. Maintaining a list of authorized users of personal data, who require whole disk encryption licenses.
l. Documenting non-compliance exceptions and compensating controls.
m. Advising the Information Stewardship Committee of changes and developments to relevant laws, regulations, standards, and best practices specific to his or business unit of which the Information Steward becomes aware.

3. Information Stewardship Committee

The Information Stewardship Committee shall provide 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 law.

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

Response to Internal & External Risks

To address both internal and external risks to the confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving the effectiveness of the current safeguards for limiting such risks, Tufts shall implement the following measures:

1. Awareness

- The University shall distribute a description of the Program to persons with access to personal information within their business unit and such persons must comply with the processes and procedures of the Program that are generally applicable or specifically applicable to a business unit.
- The University shall provide ongoing training to all persons who access personal information as part of their job or contracted process.
- Existing new employee orientation programs shall be revised to include information on applicable laws, including the Data Regulations, and the employee's obligation to comply with them.

2. Compliance & Disciplinary Action

- Per Tufts' Business Conduct Policy, all employees must operate in compliance with applicable laws and regulations.
- Tufts shall take appropriate disciplinary action against employees and others for violating security provisions of the Program, in accordance with established Human Resources progressive disciplinary measures.

3. Limiting Collection of Personal Information

- The amount of personal information collected shall be limited to that amount reasonably necessary to accomplish Tufts' legitimate business purposes, or necessary for Tufts to comply with state or federal laws and regulations.
- Access to records containing personal information shall be limited to those persons who reasonably require such access such information in order to accomplish Tufts' legitimate business purposes, or as necessary for Tufts to comply with state or federal laws and regulations.
- The retention period for personal information shall be limited to the period that is reasonably necessary to accomplish Tufts' legitimate business purposes, or necessary for Tufts to comply with state or federal laws and regulations.
- The head of each business unit shall define retention periods for records and data with personal information.

4. Monitoring

- The University shall perform regular monitoring to ensure that the information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information.

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

- The University shall reasonably monitor computer systems that maintain or process personal information for excessive access to personal information or unauthorized use.

5. Security Scope Review

- The University shall review security measures at least annually, or whenever there is a material change in Tufts' business practices that may reasonably implicate the confidentiality or integrity of records containing personal information.

6. Separated Employees

- Any separated employee shall return all records containing personal information, in any form, that may be in his or her 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's physical and electronic access to personal information shall be blocked as soon as possible. The separated employees shall 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. A separated employee's remote electronic access to all forms of personal information shall be promptly disabled.

7. System and Application Passwords

- Passwords shall be robust and changed periodically in a manner consistent with password standards adopted by Tufts Technology Services.

8. Access Control

- Access to personal information shall be restricted to active users and active user accounts only.
- Access to electronically stored personal information shall be limited to those employees having a unique log-in ID; this means users shall not share a common login token or use a generic account.
- The secure access control measures in place shall include assigning unique identification tokens and passwords, which are not vendor-supplied default passwords, to each person with authorized access to personal information.

9. Secure Authentication

- There shall be secure user authentication protocols in place, including:
    1. Documented protocols for control of user IDs and other tokens or identifiers;
    2. A reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies;
    3. 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;
    4. Restriction of access to active users and active user accounts; and

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

5. Blocking of access to user identification after no more than five unsuccessful attempts to gain access where technically feasible. When not feasible, exceptions must be formally documented and require approval from the appropriate manager(s) and IT unit(s).

10. Physical Security

- Each business unit shall ensure that reasonable restrictions for physical access to records containing personal information are in place. This includes creating written procedures that set forth the manner in which physical access to such records will be restricted. Each business unit must store such records and data in locked facilities, secure storage areas, or locked containers.
- Employees shall be prohibited from leaving files containing personal information unattended in an unsecure area.
- At the end of the workday, all files and other records containing personal information shall be secured in a manner that is consistent with the Program's rules for protecting the security of personal information.

11. Secure Data Destruction (Physical & Electronic)

- All personal information stored electronically, on paper, or on other media that requires destruction at the end of its life cycle shall be destroyed in a manner such that the information cannot practically be read or reconstructed, as required by M.G.L. 93 I.

12. Firewall & Security Software

- The University shall maintain reasonably up-to-date firewall protection and operating system security patches, designed to reasonably maintain the integrity of the personal information, installed on all systems processing and containing personal information.
- he University shall make available reasonably up-to-date versions of system security agent software, which must include malware (e.g. virus) protection and reasonably up-to-date patches and virus definitions. Such software should be installed on all University-controlled systems processing personal information.

13. Laptop & Mobile Device Encryption

- All personal information stored on laptops or other portable devices, and all records and files transmitted across public networks or wirelessly, shall be encrypted to the extent technically feasible.*
- Portable devices include all media for backups of devices storing PI.

---

* *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 meaning cannot be assigned without the use of a confidential process or key, unless further defined by applicable laws or regulations.*

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

14. Suspicious Activities & Breach Reporting

- Employees and others (e.g. vendors) shall be required to report any suspicious or unauthorized use of personal information directly to the designated Information Steward within their business unit.
- Information Stewards shall be obligated to report suspicious activities directly to the Office of University Counsel within one business day, or sooner, depending upon suspected impact of the activity.
- Whenever there is an incident that requires notification under M.G.L. c. 93H, §3, per the decision of University Counsel, all responsive actions shall be documented. The affected Information Steward, Director of Information Security, and the Office of University Counsel shall perform a mandatory post-incident review of events and actions taken to determine whether any changes in Tufts security practices are required to improve the security of personal information.

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

Appendix A: References

Massachusetts General Law Chapter 93H: Security Breach
http://www.mass.gov/legis/laws/mgl/gl-93h-toc.htm

Massachusetts General Law Chapter 93I: Dispositions and Destruction of Records
http://www.mass.gov/legis/laws/mgl/gl-93i-toc.htm

Massachusetts 201 CMR 17: Standards for The Protection of Personal Information of Residents of the Commonwealth
http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf