

Tufts University

Information Technology Resources Security Policy

Introduction

To safeguard the University's **information technology resources** and to protect the confidentiality of data, adequate security measures must be taken. This Information Technology Resources Security Policy (hereafter, "Security Policy") reflects the University's commitment to comply with federal and state statutes, regulations and University protocols governing the security of **sensitive and confidential information**. Wherever possible, this policy attempts to establish a balance between the risk of loss of information resources, including data misuse, and the effort and cost of the security measures. It includes provisions to reduce, as far as feasible, the risk of theft, fraud, destruction or other misuses of the University's information technology resources. These security provisions are endorsed by the Information Technology Council (ITC), the Tufts General Counsel, and by Audit and Management Advisory Services.

Academic and administrative information processing, digital telecommunications and related technology are critical academic and business operations of Tufts University. Inappropriate exposures of **confidential and/or sensitive information**, loss of data and inappropriate use of **computer networks and systems** can be minimized by complying with reasonable standards, attending to the proper design and control of information systems and applying sanctions when violations of this Security Policy occur.

Security is the responsibility of everyone who uses Tufts information technology resources. It is the responsibility of employees, contractors, students, friends, associates, alumni, business partners, emeriti and agents of Tufts University. *Each should become familiar with this Policy's provisions and the importance of adhering to it when using University computers, networks, data and other information resources. Each is responsible for reporting any suspected breaches of its terms.* University computers and computer workstations, non-University computers, terminals, telephones, facsimile machines and other devices either owned by the University or authorized by the University to connect to its networks are primarily for University business - to further the University's mission as it relates to teaching, administration, research and community service. As such, all information technology resource users within the University community are expected to:

- Respect the privacy of other users.
- Respect the rights of others users.
- Respect the intended use of resources and systems.
- Respect the integrity of the system or network.
- Adhere to all University policies and procedures mandated by the Information Technology Council.

Questions or comments about this policy should be directed to
Security_policy@tufts.edu.

Purpose and Scope

The primary purpose of this Security Policy is to establish rules to insure the protection of confidential and/or sensitive information stored or transmitted electronically and to ensure protection of the University's **information technology resources**. The policy assigns responsibility and provides guidelines to protect the University's systems and data against misuse and/or loss.

This Security Policy applies to all **users of computer systems, centrally managed computer systems**, or computers that are authorized to connect to the University's Data Network. The policy applies to **users** of information services operated or administered by the University. Individuals working for institutions affiliated with Tufts University are subject to these same definitions and rules when they are using Tufts University **information technology resources**.

This Security Policy applies to all aspects of **information technology resource** security including, but not limited to, accidental or unauthorized destruction, disclosure or modification of hardware, software, networks and/or data.

Finally, this Security Policy represents minimum **information technology resources** security requirements. Schools and departments may, at their discretion, and with the approval of the appropriate committees and University Counsel, establish additional policies and standards governing security. If the provisions of this Security Policy are in conflict with school or departmental security policies and standards, the provisions of this Security Policy shall prevail.

Definitions

Access is the ability of a User or Computer Application to read, write, modify, delete or communicate information or otherwise make use of Confidential or Sensitive Information.

An **Access Coordinator** is an individual within a department who is responsible for defining departmental access profiles and notifying the Data Manager who takes care of access and authentication data bases and files when personnel changes necessitate access changes.

An **Affiliate** is anyone who has been extended privileges and rights at Tufts.

An **Application** is an automated system used by offices or departments for processing confidential and/or sensitive information for University business.

A **Centrally Managed Computer System** is a Computer System which is operated and managed centrally by Tufts Computer and Communications Services (TCCS) division.

A **Computer Application** is an automated system or process that performs a definable function.

A **Computer System** is one or more computers, associated peripherals and software which operate together to perform a definable University function.

Confidential Information shall include health, financial, personnel and student information that is exempt from disclosure under provisions of any state or federal law. Confidential Information shall also include health, financial, student and any other proprietary information that is exempt from disclosure as a consequence of published University policy.

A **Data Manager** is a manager and any members of his/her staff who have been given operational level responsibility for the capture, maintenance and dissemination of specific data by the appropriate Data Steward. Moreover, if any Tufts University employee chooses to maintain a data base containing individually identifiable Confidential or Sensitive information in the course of performing professional responsibilities, (s)he will be the Data Manager for that data base and must comply with all applicable policies and rules.

The **Data Network** is Tufts' portion of the Internet which includes network equipment such as routers, switches, hubs, wireless access points, network services including but not limited to DNS, DHCP and NTP servers and all copper and fiber optic wiring.

A **Data Steward** an executive officer of Tufts University having policy-level responsibility for managing a segment of the University's information resources.

A **Departmental Computer System** is any Computer System which operates independently of TCCS and which processes or contains confidential and/or sensitive information.

An **Electronic Identifier (ID)** is a unique identification assigned to each user of a Computer System. The Electronic Identifier is used to gain access to the Computer System and provide accountability for all actions taken by the user.

An **Individual** is a person to whom is attributable individually identifiable personal information.

The **Information Security Officer** is the person who has overall operational institutional responsibility for computer information and resource security.

An **Information Technology Resource** is any information, including but not limited to information stored in electronic format, and/or the tools used to access and make use of that information (including but not limited to computer programs and applications, databases, computer systems and networks).

A **Network** is a series of points, including computers and other devices, interconnected by communication paths. Networks include interconnections with other networks and sub-networks and may carry voice, data or other types of signals.

A **Network Manager** is a manager and any members of his/her staff who have been given responsibility for the operation and maintenance of a Network that is required for the performance of some identifiable business function or that supports the transmission of Confidential or Sensitive data.

A **Non-University Computer** is a computer which is not managed or owned by Tufts but which operates within the university network. Examples include student computers and computers which are owned and operated by business partners.

Removable Media are data storage media including but not limited to magnetic tape, floppy disks, zip disks, removable disk storage and CD-ROMs that can be removed from a Computer System and easily carried from place to place.

A **Security Breach** is a type of activity which includes, but is not limited to, an unwanted disruption or denial of service, the unauthorized use of a system for the processing or storage of data, and changes to hardware, firmware or software which are made without appropriate approvals.

Sensitive Information is information maintained by the university which requires special precautions to ensure its accuracy and integrity. It is information that requires a high level of assurance of accuracy and completeness (e.g., a GPA).

A **System Manager** is a manager and any members of his/her staff who have been given responsibility for the operation and maintenance of a Computer System.

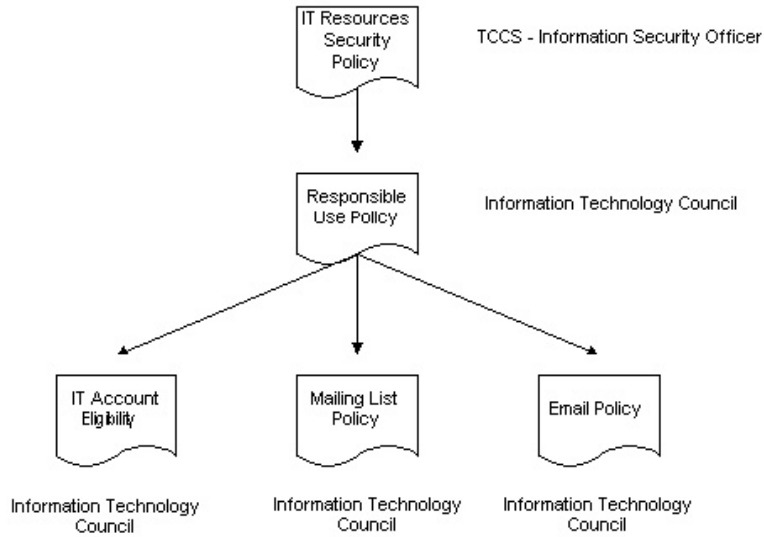
Tufts University, as an organization, is a guardian of data rights, a caretaker of individually identifiable information and owner of the medium of storage.

A **User** or **Authorized User** is a person who has been authorized to gain access to the Tufts network, computer systems and computer information.

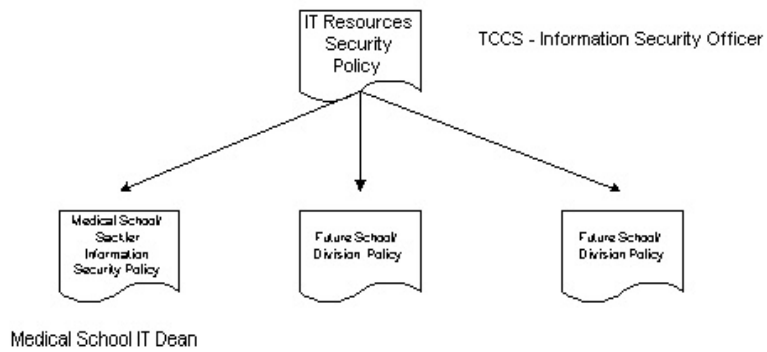
The **Voice Network** consists of those network components such as T1 cards and fiber optic interfaces located within each campus' PBX (including but not limited to terminal devices such as phones, facsimile machines and alarm systems) and vendor-supplied components such as T1 lines and copper trunks. These components permit the delivery of voice network services in the form of telephony between Tufts locations and the outside world. Additionally, the voice network consists of measured business service, ISDN services and other private lines which bypass the PBX to provide connectivity to locations with special applications that cannot be serviced from the PBX.

Tufts IT Policies - Derivative Relationships

Enterprise-Wide Policies



School, Division and Departmental Policies



DLN/TCCS
10/05/01

Security of Computers, Computer Systems and Servers

- a) Each data steward will ensure that a business resumption plan is in place.
- b) Each **system manager** will take reasonable action to provide necessary protection against natural disasters and will prepare adequate system disaster recovery plans and procedures.
- c) Each **system manager** will establish an environment which provides appropriate physical access for **authorized users** of the **computer systems**. Appropriate access may range from open access by students on networked computers in departmental workstation laboratories to severely restricted access in offices responsible for creating, modifying or deleting **confidential and/or sensitive information**.
- d) Each **system manager** will identify and analyze the risks of anticipated threats to physical security, identify responses and implement appropriate controls. This analysis and preparatory work will be recorded, maintained and updated as conditions change.
- e) Each **system manager** is responsible for the installation and use of virus detection software, where appropriate, for the protection of **information technology resources**.
- f) Each **data or system manager**, as appropriate, will provide and implement appropriate and adequate security measures to ensure recoverability of the information stored in **computer systems**.
- g) Each **system or data manager**, as appropriate, is responsible for keeping **computer systems** secure by ensuring that maintenance is performed in a timely manner. Maintenance may include but is not limited to application of software patches, preventative maintenance, software, firmware or hardware upgrades, or if necessary, by the exclusion or removal of outdated, non-conforming **computer systems**.
- h) Each **system or data manager**, as appropriate, is responsible for conducting periodic reviews of implemented security plans, measures, procedures and controls.
- i) Each **system manager** must provide the means to permit authorized personnel to audit and establish individual identification for any action which may provide access to, modify or release **confidential or sensitive information**.

- j) *Each **system manager** must initiate an investigation of any suspected **security breach** involving a computer, **computer system** or server and is responsible for documenting the suspected breach and actions taken.*

Security of the Network

At Tufts University, TCCS (Tufts Computers and Communication Services) manages the data and voice networks. In that capacity, TCCS management must assume the largest share of responsibility for identifying and analyzing potential threats to the networks as well as for network security planning, implementation, maintenance and monitoring.

- a) *TCCS **network managers** will identify and analyze potential threats to uninterrupted **voice and data network** availability and identify appropriate responses. The analysis and preparatory work will be recorded, maintained and updated as conditions change.*
- b) ***Network managers** will implement appropriate controls to ensure that connected users or computer services do not compromise the security of any other networked service.*
- c) *TCCS **network managers** are responsible for the implementation of any controls necessary to ensure that access is limited to **authorized users** of the Network.*
- d) *TCCS **network or system managers**, as appropriate, will establish procedures to identify and remove network services, protocols and network devices that expose the **network** to unauthorized access or attacks.*
- e) *Each **network manager** will take reasonable action to provide necessary protection against natural disasters and will prepare adequate disaster recovery plans and procedures for that part of the **network** for which he/she is responsible.*
- f) *TCCS **network managers** are responsible for establishing and maintaining standards for network naming and numbering. The head of each school/division's IT support organization is responsible for managing the local implementation of TCCS' network numbering and naming standards in concert with several TCCS departments: Network Engineering, WebCentral and the NT-LAN group.*
- g) *TCCS **network managers** are responsible for the maintenance and publication of network services responsible use guidelines to maximize network integrity and performance.*
- h) *Each **network manager** is responsible for conducting periodic reviews of implemented security plans, measures, procedures and controls.*

- i) *Each **network manager** must provide the means to permit authorized personnel to audit and establish individual accountability for any activity involving the **network** and which may or does result in a **security breach**.*
- j) *Each **system or network manager** must initiate an investigation of any suspected **security breach** involving his/her network(s) and is responsible for documenting the suspected breach and actions taken.*

Security of Desktops, Terminals, Client Devices, Voice Devices, Modems and Facsimile Machines

- a) *Each **data or system manager**, as appropriate, who is responsible for the maintenance of desktops, terminals, client devices, voice devices, modems and facsimile machines will institute appropriate safeguards to ensure that these devices are not misused, abused, or compromised.*
- b) *Each **data or system manager**, as appropriate, who is responsible for the maintenance of desktops, terminals, client devices, voice devices, modems and facsimile machines will institute appropriate safeguards to ensure that access to the devices is limited to authorized users.*
- c) *Each **data or system manager**, as appropriate, who is responsible for the maintenance of desktops, terminals, client devices, voice devices, modems and facsimile machines, will conduct periodic reviews of implemented security plans, measures, procedures and controls.*
- d) *Each **data or system manager**, as appropriate, who is responsible for the maintenance of desktops, terminals, client devices, voice devices, modems and facsimile machines, must initiate an investigation of any suspected **security breach** involving those desktops, terminals, client devices, voice devices, modems and facsimile machines and is responsible for documenting the suspected breach and actions taken. Under these circumstances, the data or system manager shall notify his/her dean or supervisor as well as the Information Security Officer regarding the suspected breach.*
- e) *As desktops, terminals, client devices, voice devices, modems and facsimile machines are removed from service or redeployed, each **data or system manager**, as applicable, is responsible for ensuring that **confidential or sensitive information** has been removed from the equipment.*

Security of Data and Data Bases

- a) *Each **data manager** will maintain records of the owner(s) of all **confidential and/or sensitive information** stored on his/her **computer systems**.*
- b) ***Data stewards** are responsible for conducting and documenting a risk analysis of anticipated threats to the **sensitive or confidential information** for which they are responsible. This analysis will be maintained and updated as conditions change.*
- c) ***Data managers** are responsible for the *classification of information as **confidential and/or sensitive***. Classifications must adhere to federal and state laws and regulations, and Tufts University policies. *Audit and Management Advisory Services reserves the right to review such classifications and, based on that review, make specific recommendations.* Using risk analysis, **data managers** will map data classifications into security levels. *These levels will be communicated to **access coordinators** and **system managers** along with specific recommendations regarding access to data.**
- d) *Owners of, or those who are the subject of, as applicable, **confidential and/or sensitive Information** will identify those to whom **confidential or sensitive information** may be released, unless such release is otherwise addressed by applicable law. It is the **data steward's** responsibility to ensure that this released information is obtained and recorded.*
- e) ***Data and system managers** will be granted access to **confidential or sensitive information** as required to satisfy operational needs.*
- f) ***Data stewards** are responsible for the periodic review and updating of their data risk analysis and data security classification levels.*
- g) *Users of **confidential and/or sensitive information** are responsible for proper security of that information when it's transferred from a computer system to hard-copy documents or removable media or when it's downloaded to computers on a **network**. **Data stewards and data managers** may require that **users** execute a separate confidentiality agreement before being given access to **confidential and/or sensitive information**.*
- h) ***Data stewards and data managers** will make their best effort to insure that hard-copy documents and removable media containing **confidential and/or sensitive information** are*
 - Made accessible only to authorized personnel

- Accounted for
 - Properly stored in appropriate facilities
 - Properly disposed of
- i) *Once it is no longer required, **data stewards** and **data managers** are responsible for ensuring that appropriate disposal or scouring procedures are used for all hard-copy documents and removable media containing confidential and/or sensitive information and for all downloaded **confidential and/or sensitive information**. (See also Tufts' General Policy on Access to University Records in the Archives for additional information on the disposition of **confidential and/or sensitive information**.)*
- j) **Data stewards** are responsible for ensuring that all data stored in databases are recoverable.
- k) ***Data stewards** are responsible for ensuring that authorized personnel are able to audit and establish individual accountability for any action which may provide or change access to, modify or release **confidential or sensitive information**.*
- l) *Each **data or system manager**, as applicable, must initiate an investigation of any suspected **security breach** involving data or a database for which (s)he is responsible and must document the suspected breach and actions taken. It is the responsibility of the data or system manager to notify his/her supervisor or dean as well as the Information Security Officer of any suspected security breach.*

Security of Programs and Applications

- a) *Each **access coordinator** will maintain a mechanism to restrict access to programs and applications which process **confidential and/or sensitive information**. This mechanism will be based on user **electronic identifiers (IDs)**.*
- b) *Each **access coordinator** will maintain a mechanism that allows the owner of a program or application which processes **confidential and/or sensitive information** to designate the set of users who can modify the program or application.*
- c) ***Data and system managers** having responsibility for **confidential and/or sensitive information** will participate in the development of application test data for all such information.*
- d) *Employees developing, modifying or testing programs or applications which are used to generate, modify or delete **confidential and/or sensitive information** will test programs and applications against appropriately masked test data.*
- e) ***Data and system managers**, as applicable, are responsible for ensuring that new and changed programs that process **confidential and/or sensitive information** move from test/development to production via an auditable change control process.*
- f) ***Data and system managers**, as applicable, are responsible for ensuring that employees who develop, modify or test programs of applications which are used to generate, modify or delete **confidential and/or sensitive information** dispose of test output appropriately.*
- g) ***Data managers** who establish data security levels are responsible for ensuring that access to applications is consistent with restrictions on data access.*
- h) ***Data or system managers**, as applicable, are responsible for ensuring that test functions are kept either physically or at a minimum logically separate from production functions.*
- i) ***Data or system managers**, as applicable, are responsible for ensuring that copies of production data are not used for testing unless the data have been classified as not **sensitive or confidential information**, or unless all staff and contractors with access to the test data are authorized to access it.*

- j) *Data or system managers, as applicable, are responsible for ensuring that appropriate information security and audit controls for **confidential and sensitive information** shall be incorporated into new systems.*

Access Control Security (Login/Logon-Logout/Logoff)

- a) *System managers are responsible for ensuring that each computer system for which they are responsible has at least one **access coordinator**.*
- b) *The **access coordinator** for each **computer system** will assign a unique **electronic identifier (ID)** to each user of the **computer system**.*
- c) *Under circumstances when a password is required, each **user** will establish a password, known only to him/her. The individual **user** will be responsible for the confidentiality of the password and for any breaches of security committed via access gained through his/her password or other electronic identifier.*
- d) *Each **system manager** is responsible for the development of mechanisms that require a user to change his/her password at regular intervals if the user's **ID** and password provide access to **information technology resources** or **confidential and/or sensitive information**.*
- e) ***System managers** are responsible for publicizing the procedure for changing passwords.*
- f) *Each **access coordinator** is responsible for notifying the appropriate **system manager** and revoking the relevant **electronic identifier (ID)** when a **user** no longer requires access to the information resources managed by the **system manager**.*
- g) ***System and data managers**, as applicable, will conduct and document a risk analysis for each system for which he/she has responsibility and based on that risk analysis, implement any time-out mechanisms that are warranted.*

User Notification and Obligations

- a) *The University's **Information Security Officer** will ensure that all persons who use **computer systems** and/or the University **network** are informed about this Security Policy.*
- b) *All **users** with access to **confidential and/or sensitive information** may be required to sign an acknowledgment of understanding and acceptance of this and/or other policies, rules and regulations pertaining to the use of Tufts University **information technology resources**.*
- c) *TCCS Training and Development is responsible for establishing a Security Awareness Class designed to sensitize employees to security issues.*
- d) *It is the responsibility of Tufts University managers to ensure that each direct report with access to **confidential or sensitive information** participate in the Security Awareness Class. For new employees, the class must be taken within the first six (6) months of his/her employment.*
- e) *Each University employee with access to **secure or confidential information** must be familiar with and abide by the University's Responsible Use Policy.*
- f) *Any employee who suspects that a violation of this Security Policy has occurred is obligated to report it to his/her manager or dean, as applicable, or to report it to the University's Information Security Officer at security_officer@tufts.edu. Suspected violations of this Policy may be reported anonymously by sending mail to Security Officer, TCCS, TAB (University IT Security Officer/Tufts Computing and Communications Services/ Tufts University/ 169 Holland Street, Somerville, MA 02144 from off campus) or by calling x7-3435 (617.627.3435 from off campus).*

Sanctions

Non-Compliance

If an audit, security scan or a computer security incident indicates that the University or a department or office within the University is deficient with respect to the security measures established by this Policy, the University, department or office may be subject to any or all of the following:

- Removal of the Computer System, server or desktop from the data network until such time as the security problems have been fixed and the system/server/desktop is in compliance with the provisions of this Policy.
- Audit by Audit and Management Advisory Services.
- Investigation by Campus Police and state or federal agencies, depending on the nature of the computer security incident.

Violations

Individuals including faculty, staff, students and affiliates who violate the provisions of this policy are subject to discipline up to and including dismissal or separation from the University. Where applicable, a violation may subject the violator to civil and/or criminal liability. Additionally, the University at all times maintains the right to determine who will be authorized to have access to its information and/or resources.

Persons subject to this Policy may also be bound by copyrights and contractual obligations of the University with respect to use of software and other matters. Other Tufts University policies that relate to this Policy include, but are not limited to the Responsible Use Policy, the IT Account Eligibility Policy, the Mailing List Policy and the Email Policy. Each person who is subject to this Security Policy is expected to be familiar with the relevant foregoing policies.

Ongoing Policy Management

- a) Tufts University reserves the right to modify this Security Policy. Audit Management and Advisory Services, the Tufts General Counsel and the Information Technology Council are available to advise the Information Security Officer on any changes made to this policy.
- b) The **Information Security Officer**, under the authority of the Trustees of Tufts University, shall be responsible for the management and oversight of this Security Policy.
- c) The **Information Security Officer** is responsible for performing an annual review of this Policy and for making any updates which are warranted.
- d) The **Information Security Officer** is responsible for verifying that security standards, procedures and guidelines are established in support of this Security Policy.
- e) The **Information Security Officer** is responsible for posting this Security Policy and any derivative standards, procedures and guidelines on the Tufts University web site. This web content shall be made accessible and available to all University employees, contractors, students, friends, associates, emeriti and agents.
- f) The **Information Security Officer** will, if requested to do so, review school and department-specific security policy provisions being proposed in addition to the ones contained in this Security Policy.
- g) The **Information Security Officer** will maintain a repository of **data stewards, system, network and data managers and access coordinators**.
- h) The Information Security Officer will maintain a log of violations of this policy.