

# Tufts Checklist for Protecting Information

## Applicable to All Employees and Users with Access to University Data Resources

May 12, 2004

Tufts University is responsible for collecting, storing, and distributing voluminous amounts of information. Some of this information is federally legislated as private and must be protected in accordance with laws such as the Family Education Rights and Privacy Act of 1974 (for student records), the Gramm-Leach-Bliley Act of 1999 (for personal financial information), and the Health Insurance Portability and Accountability Act of 1996 (for protected health information). Other information should be protected because it is private by the commonly understood definition of the term. The terms "confidential," "sensitive," and "private" are used interchangeably in the following checklist. Although each term has a different technical meaning, the general principles for protection of information are applicable to each in the same way.

- Read this checklist for protecting information and adhere to its principles.
- Contact IT Security ([security\\_policy@tufts.edu](mailto:security_policy@tufts.edu)) with any questions you have about protecting information or contact the University IT Support Center ([UITSC@tufts.edu](mailto:UITSC@tufts.edu), 617-627-3376) for a referral to someone who can respond to your information security questions.
- If you are in doubt about whether or not certain information is considered private or may be shared with other people, contact the Office of University Counsel or the office responsible for that category of information for advice before disclosing or transmitting it.
- If you deal with vendors or other outside parties who handle Tufts information that must be protected, be sure that the necessary clauses pertinent to data protection responsibilities (available from the Office of University Counsel) are included in Tufts' contracts with them.

## Information Communicated Orally

- Make it a practice not to discuss confidential information outside of the workplace or with anyone who does not have a specific need to know it.
- Be aware of the potential for others to overhear communications about sensitive information in offices, on telephones, and in public places like elevators, restaurants, and sidewalks.

## Information Stored on Paper

Documents that include confidential information like social security numbers; student education records; an individual's medical, benefits, compensation, loan, or financial aid data; and faculty and staff evaluations need to be secured during printing, transmission (including by fax), storage, and disposal.

- Do not leave paper documents containing sensitive information unattended; protect them from the view of passers-by or office visitors.
- Store paper documents containing sensitive information in locked files.
- Do not leave the keys to file drawers containing confidential information in unlocked desk drawers or other areas accessible to unauthorized personnel.

- Store paper documents that contain information that is mission critical to the conduct of University business in fireproof file cabinets. Keep copies in an alternate location.
- Shred confidential paper documents that are no longer needed, and secure such documents until shredding occurs. If a shredding service is employed, ensure that the service provider has clearly defined procedures in the contractual agreement that protects discarded information, and that the provider is legally accountable for those procedures, with penalties in place for breach of contract.
- Make arrangements to immediately retrieve or secure sensitive documents that are printed on copy machines, fax machines, and printers.
- Double-check fax messages containing confidential information:
  - Recheck the recipient's number before you hit 'start.'
  - Verify the security arrangements for a fax's receipt prior to sending.
  - Verify that you are the intended recipient of faxes received on your machine.
  - Include a confidentiality statement on the fax cover sheet.

## Information Stored Electronically

All employees and users of networked computing devices on Tufts' network have a role in protecting the University's information assets because their machines provide potential gateways to private information stored elsewhere on the network. Therefore, whether or not you deal directly with sensitive or confidential University information, you should take the following steps to reduce risk to Tufts' information assets.

### First, Educate Yourself

- Read Tufts IT Resource Security Policy (<http://www.tufts.edu/tccs/p-resourcesec1.shtml>), and understand its implications for the information for which you are responsible.
- Know who your Front-Line Support Provider (FSP) is and what s/he can do for you.
- Immediately advise your FSP of any suspicious activity on your computer or a suspected information system security compromise. The FSP will report the event to Network Engineering and Security for follow-up action.
- Be mindful of how you are sharing or transmitting sensitive information across the network.

### Protecting E-Mail

- Understand that e-mail is not secure; it can be forged, and it does not afford privacy.
- Install anti-virus software on your computer and ensure that the software is set automatically to update its virus definitions, if technically possible. If you are in doubt about whether you have anti-virus software installed on your computer, contact your FSP.
- Do not open unexpected e-mail attachments, and do not download documents or software from unknown parties.
- Clear e-mail boxes of old messages on a regular basis.
- Take precautions not to send anything by e-mail that you wouldn't want disclosed to unknown parties. Recipients have been known to distribute information to unauthorized recipients or store it on unsecured machines, and viruses have been known to distribute archived e-mail messages to unintended recipients.

### Restrict Access to Information on Your Desktop

- Orient your computer screen away from the view of people passing by.
- Turn off your desktop computer at the end of the workday.
- Use password-protected screensavers on your desktop computer.
- Use security devices to lock down computers that are in public or otherwise unsecured spaces.

- Sanitize the hard drives of computers that you declare surplus and of those that are going out of service for other reasons to ensure that data is removed and not recoverable (consult your FSP for additional information). Deleting files, moving files to "trash," and emptying the "trash" file is insufficient because the files can still be recovered.
- Ensure that functions that enable data sharing on an individual workstation are either turned off or set to allow access only to authorized personnel.

## Secure Mobile & Cellular Devices

Information stored on laptop computers, personal organizers (e.g., Blackberry, Palms), cellular phones, and other similar mobile devices is susceptible to equipment failure, damage, or theft. Information transmitted via wireless connections is not always secure - even networks using encryption are vulnerable to intruders.

- Protect and secure mobile devices from theft at all times.
- Use internal firewalls and strong authentication when transmitting information via wireless technologies.
- Use personal firewalls on laptops that will access the Tufts Network from a remote location.
- Back up the data on your mobile devices on a regular basis.
- Change batteries on mobile devices as soon as the "low battery" prompt appears to avoid losing information, configurations, and settings.

## Protecting Passwords

- Employ passwords that are easy for you to remember but impossible for someone else to guess (see <http://www.tufts.edu/tccs/r-strongpass.html>):
  - Passwords should not consist of a word that can be found in a dictionary.
  - Passwords should be at least 8 characters in length and consist of a combination of numeric characters, mixed upper and lower case alpha characters, and at least one special character.
  - Consider combining parts of two different words that together do not form a word.
- Secure your passwords, and restrict access to them. Passwords written on a post-it in a work area, placed under a keyboard, or stored in an unlocked desk drawer are not safe from unauthorized access.
- Never share your passwords or accounts.
- Change your passwords regularly, every 3-6 months. The more sensitive the information being protected, the more frequently you should change your passwords.
- Understand how to properly restrict file sharing on your computer to mitigate the risk of unintentionally granting access to unknown parties.

## Protecting the Integrity of Information

- Apply system updates for your desktop systems and department servers' operating systems in a timely manner.
- Keep local applications updated and patched. (Contact your FSP for guidance.)
- Encrypt sensitive files.
- Secure local servers in a locked room and limit the access to the room to system administrators only.

## Back Up Information

- Know the back-up and recovery strategies for the information for which you are responsible.
- Know whether your data is backed up centrally and/or locally.
- Know the frequency with which the back-ups occur.
- Know who is responsible for backing up your information.
- Make sure that the recovery procedures for your information have been tested.
- Know where your back-ups are stored.
- Store back-ups of critical information in an alternate location, preferably in another building across campus or off-site.
- Make sure that private information stored on back-ups in alternate locations is protected from unauthorized access.
- Know how you will recover critical data and resume related business operations in the event of loss of power, disruption of network services, theft of your computing device, or inability to access your office or building.

## Assistance

- Contact your FSP first for assistance with any questions you might have. Your FSP knows how to obtain further assistance from IT Security.
- If you don't yet have an FSP, or if you need additional help with assessing your risk or protecting your electronic information, contact the University IT Support Center ([UITSC@tufts.edu](mailto:UITSC@tufts.edu), 617-627-3376) for a referral.
- Always feel free to contact Lesley Tolman, Director of IT Security directly if you have questions. Lesley can be reached at [lesley.tolman@tufts.edu](mailto:lesley.tolman@tufts.edu) or at 617-627-5073.

We wish to express our appreciation to Brown University Computing & Information Services for developing and providing much of this information.