TIPS AND GUIDELINES FOR SENSITIVE PERSONAL INFORMATION (SPI)

For questions about these Tips and Guidelines, please contact your Information Steward or the Information Security team

These Tips and Guidelines are a resource developed under the Tufts Information Security Program, which supports compliance with the Massachusetts laws for safeguarding personal information.

Report an Incident:
Information at Reporting an Information Security Incident

TTS Service Desk:
617 627-3376 (preferred) or it@tufts.edu

Table of Contents

WHAT IS SENSITIVE PERSONAL INFORMATION (SPI)?

GOVERNMENT–ISSUED IDENTIFYING NUMBERS	• Social Security numbers • Driver's License numbers • Other Massachusetts ID numbers • Passport and Visa numbers • All Government ID numbers
REGULATED FINANCIAL INFORMATION FOR INDIVIDUALS	• Credit or Debit card numbers • Financial Account numbers (e.g. Bank Accounts)
BIOMETRIC INDICATORS FOR IDENTITY	For example: • Fingerprints • Retina Patterns • Genetic Information

Financial accounts includes accounts for individuals, such as listed on a check, other bank accounts, and accounts at other financial institutions. Include Tufts accounts for individuals where Tufts provides a service or product similar to those provided by a financial institution. Include student loan accounts. Do not include Tufts Dept IDs.

Biometric Indicators for Identity includes any unique biological attribute or measurement that can be used to authenticate the identity of an individual, including, but not limited to, fingerprints, genetic information, iris or retina patterns, facial characteristics, and hand geometry.

GENERAL SAFEGUARDS FOR ALL SENSITIVE INFORMATION

PASSWORDS

USE A PASSWORD TOOL. There are many password tools available to help you securely store your passwords. Some are even free. Instead of leaving a written list of passwords on your desk, try one of these tools. Though it may seem insecure to keep all that information on a computer, these applications have been developed to protect your information. See Password Tools.

ALWAYS be careful with your passwords.

Remember, if you have access to SPI, if your password is disclosed, it could be used by an unauthorized person to access valuable identity information that can cause significant harm to you or others in our community. Stolen passwords have been used at universities to redirect paychecks and commandeer email accounts to send spam.

Do NOT share your passwords with anyone. Do NOT send your passwords in email.

Do NOT leave your passwords written on a piece of paper or a post-it in a place accessible or viewable by any other person. It is preferable to memorize your password.

NEVER save your passwords in any browser.

- Do not share a common login token or use a generic password.

- For any workstations shared within your office, always use your own individual account.
- Do not use vendor supplied default passwords.
- Do not use a Tufts Password for any account outside of Tufts.
- Change your password at least every 180 days.
- Follow the Tufts Password Policy.

ENROLL IN TUFTS TWO FACTOR AUTHENTICATION

For your protection, we recommend that you enroll to use Tufts Two Factor Authentication. It is based on a solution from Duo. When you enroll in this solution, many of Tufts' applications and the VPN can be locked down so that if your userID and password are stolen, you will be protected. Logging in to Tufts using Duo will require two steps: first entering your userID/password and then second, requesting verification through Duo. More information is available at https://it.tufts.edu/qs-twofactor.

CONVERSATIONS

- Make it a practice not to discuss confidential information, including SPI, 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 confidential information, including SPI, in offices, on telephones, and in public places. Make it a practice to not repeat confidential information, especially SPI, you receive on a phone to reduce the potential for unauthorized persons to overhear the information.

WORKING WITH DOCUMENTS

- Never leave documents containing confidential information, including SPI, unattended. If you must step away from your desk, lock them up.
- Protect documents from the view of passers-by or office visitors.
- Orient your computer screen away from the view of persons passing by.
- Log off of your computer or lock the screen whenever you are away from it, whether during the day or at the end of the day. For the simple steps to lock your computer's screen, see Manually Locking your Computer's Screen.

REMOVING, REDACTING AND DESTROYING SENSITIVE INFORMATION

- Paper Documents:
    - Destroying:
        - If shred, must be cross-cut or micro-cut (preferred) shredded into squares or rectangles.
        - May use a vendor-supplied bin for secure disposal if the vendor is Tufts approved for this purpose. Shred-it is approved.
        - Do not use paper-recycling bins UNLESS already cross-cut or micro-cut shredded in squares.
    - Removing or redacting:
        - Use opaque (100% impenetrable by light; neither transparent nor translucent) tape or paper to cover over the sections to be redacted. Do not use plain paper as the scanner may pick up images through the paper. Even some black paper may allow some light reflection - so be careful. Copy after redacted and shred or otherwise properly dispose of the original. Confirm that the redacted area of the copy is completely opaque.
        - Cut-out (literally) all the text to be redacted and properly dispose of (shred) the clippings. This method will always be 100% effective.

        - Do NOT black out information using ink. It can still be recovered using tools like Photo-Shop.
- *Electronic Documents and Emails:*
    - *Documents on a PC:*
        - Use Identity Finder File Shredder. This tool may be used for a document without conducting a full scan.
        - Or delete the document and empty the trash/recycle bin.
    - *Documents on a MAC:*
        - Use Secure Empty Trash. To use Secure Empty Trash, open Finder (upper left) and click on Secure Empty Trash.
        - Use Identity Finder File Shredder. The Identity Finder File Shredder tool may be used for a document without conducting a full scan.
    - *Emails:* To securely delete email messages and their attachments, see *Securely Deleting Email in Outlook*. After deleting the message and emptying the Trash, you also need to purge the email to fully delete it.

ONLY INSTALL TRUSTED APPLICATIONS

Only install trusted applications from reputable software providers, such as download.cnet.com. Do not download applications offered by email, text messages, or web links. Do not install applications offered on pop-ups from third-party websites.

USING COPIERS, PRINTERS AND SCANNERS

- Immediately pick up any documents sent to a printer.
- Do not leave any records unattended.
- Any copy machine or printer used for sensitive information should be in a secure area with access only to authorized persons.
- Limit the number of copies made to as few in number as possible.
- Only use copiers, printers and scanners purchased or leased by Tufts, so that hard drives are disposed of properly.
    - Copier Information from Purchasing
- See below for information about retiring copiers, printers and scanners.
- Most Tufts supplied printers may be enabled for password protected printing. Secure Print enables delaying printing until you enter a password at the printer. See Using Secure Printing on Konica Minolta BizHub Copiers.

TRAVELLING INTERNATIONALLY

If you are planning to travel outside the United States, it is generally advisable to use a loaner laptop rather than your current laptop. Using a loaner laptop enables you to select and isolate the information you travel with and will ensure that other data stored on your current laptop will not be at risk of loss or theft. If you plan to travel with any SPI on any of your devices, it is important that you consult with Information Security in advance of your travel.

To request a Travel Laptop Loaner, go to Loaner Laptop Request. A request should be made at least 5 business days in advance of travel. The loaner laptops can be loaded with any software you require. It is important to note that some countries do not permit you to use an encrypted laptop.

DO NOT ALLOW OTHER PERSONS YOU DO NOT KNOW AND TRUST TO CONNECT TO YOUR DEVICES

Seeking to connect to a device through deception is a common ploy used by hackers. Do not permit any such connection. The only permissible remote connection is by the TTS Service Desk, after you have contacted them.

TRANSFERRING AND RETIRING OLD COMPUTERS, DEVICES, COPIERS, PRINTERS, SCANNERS, FAX MACHINE AND OTHER MEDIA: INCLUDING HARD DRIVES, FLASH DRIVES, CDS, AND OTHER DISKS

- *Transfers to a new user:* Do NOT transfer a device to a new user without first having it securely wiped and then re-imaged. Computers and these other devices store data in a complex manner that is not readily apparent to end-users. It is much safer (and easier) to have your machine wiped than to assume that you can manually find and delete all the files on your computer with confidential or sensitive data. Contact the TTS Service Desk for support.
- *Found Device:* If you locate a computer or other device in your office that has not been used for some time and there is uncertainty about what is stored on it, it should not be turned on. Contact the TTS Service Desk to arrange for its delivery to TTS.
- *Disposal:* Before any computer, hard drive, flash drive, copier, printer, scanner, fax machine, CD, other disk or other storage media is disposed of or transferred outside Tufts, it should be securely wiped or destroyed. Computers and these other devices store data in a complex manner that is not readily apparent to end-users. It is much safer (and easier) to have your machine wiped than to assume that you can manually find and delete all the files on your computer with confidential or sensitive data. Contact the TTS Service Desk for support. In some cases Tufts contracts with the lessors for the wiping of hard drives of copiers, printers and scanners.

ARCHIVING DOCUMENTS

- Limit the length of time that you store records containing SPI to the time reasonably necessary to accomplish a legitimate business purpose or to comply with state or federal regulations. See the general Records Retention Schedule to learn how long offices and departments need to keep their records and what they should ultimately do with their records.
- Appropriately archive documents containing SPI that should be retained. See Guidelines for Managing University Records.
- Consult with Digital Collections and Archives (DCA). Liz (Elizabeth) Francis, the University Records Manager, consults with staff about record management.

GUIDELINES PREPARED SPECIFICALLY FOR SPI

GENERAL

- **You may only collect, use, handle or have access to stored SPI if necessary for your job responsibilities.**
- **You may only share SPI with persons who have a need to know for their job responsibilities.**
- Eliminate or reduce collecting, using, handling, and storing SPI as much as possible.
- Read a copy of the local SPI policy for your office, department, or unit. Follow the requirements in your local policy.
- Know who your Information Steward is. Your Steward is available to help you with questions about SPI.

- Pay special attention to the use of credit card data, health information and education records. There are additional regulations, rules and policies that apply.

SPECIAL RESTRICTIONS FOR CREDIT OR DEBIT CARD DATA

The acceptance of credit cards or debit cards for payment is restricted by the Tufts University Policy for Accepting Credit Card and eCommerce Payments, which includes a requirement to comply with the Payment Credit Industry Data Security Standard (PCI DSS). No school, department, organization, employee, contractor or agent is authorized to process Internet-based payment transactions, credit or debit card payments or electronic funds transfers without prior approval from Treasury Operations.

WHAT TO DO IF YOU RECEIVE SPI THAT YOU DID NOT REQUEST OR DO NOT NEED

- Contact the sender and determine why the information was sent to you. Request that the sender cease sending the information.
- Consider whether to securely store the information or securely dispose of the information. See the guidelines for securely storing and disposing of documents.
- Notify and consult with your Information Steward.

WORKING WITH FORMS YOU REQUEST OTHERS TO COMPLETE

- Very carefully consider if any item of SPI is needed, or whether the purpose for collecting it may be satisfied in another manner. Limit any item of SPI requested to the least needed.
- State on the form that the form should be returned by US mail or a similar service or delivered in person and that the form should not be returned by email. (In limited situations, email may be used to transmit SPI, but the use of email is strongly discouraged. See **Email Restrictions for Sensitive Personal Information**.)
- Handle and store any completed form that contains SPI in accordance with the guidelines provided below.

COMMUNICATION/SENDING SPI TO OTHERS

- *Always:* Verify the information is being provided to a permitted person and office with a need to know because of their job responsibilities.
- *Phones for Voice:*
    - Do NOT use voicemail to communicate SPI. Include a message advising callers to not leave SPI on voicemail.
    - If you would like to disconnect the voicemail/email translation function, then have the setting changed to “Privacy” voicemail. You’ll receive an email that you have a voicemail, but that email will not have the message left. To receive that message, you’ll have to dial in to listen to the messages via telephone. To have the setting changed, put in a ticket to the Service Desk at it@tufts.edu and request to have your voicemail changed to “Privacy voicemail,” and include the affected phone number.
    - See information below about using mobile phones for other than voice communications.
- *Email:* Permitted ONLY IF encrypted. This restriction is imposed by a Massachusetts regulation. See **Email Restrictions for Sensitive Personal Information**, which includes information on using email between tufts.edu addresses and also on using Tufts Secure Email, an encryption tool for email sent externally.
- *Alternatives to Email for sharing or sending SPI securely:*
  Some of the alternatives you can use are listed below. When using the Adobe or

Microsoft encryption solutions with email, you will still want to follow the email restrictions – see link above.

- *Use Box for regular collaboration and sharing significant amounts of information*. If you need to provide SPI on a regular basis to another Tufts staff member or if you need to provide a significant number of identification or financial account numbers, then it is strongly recommended that you establish a Box folder to share the information rather than using the Tufts email service. See the Tufts Box Use Guideline to learn what information may be stored in Tufts Box and see Box Collaboration/Sharing Tips for guidance on securely using Tufts Box.
- Adobe Pro Suite gives users the ability to protect and encrypt a pdf file, which then may be sent by email. See Adobe Encryption. NOTE: Do not send an email with the file and the password in the same email. Find some other way to communicate the password to users other than email.
- Microsoft Office Suite - Word, Excel, and PowerPoint have options to protect and encrypt Office files, which then may be sent by email. See Microsoft Encryption. NOTE: Do not send an email with the file and the password in the same email. Find some other way to communicate the password to users other than email.

- *Fax:*
    - Use a cover sheet that does not include any SPI and includes a confidentiality statement. For example: "This fax contains material that is confidential for the sole use of the intended recipient. Any review, reliance or distribution by others or forwarding without express permission is strictly prohibited. If you are not the intended recipient, please contact the sender and delete and destroy all copies."
    - Always confirm the recipient's number, the secure arrangements for the fax's receipt, and the receipt of the fax.
    - Any fax machine used for SPI records should be in a secure area with access only to authorized persons.
- *US Mail, Tufts mail, and Tufts approved couriers and delivery services*: Seal envelope and mark confidential and to be opened by addressee only. For packages with SPI relating to more than one person, it is advisable to use a courier or service that provides tracking of the package.

SHARING AND STORING DOCUMENTS WITH SPI

- *Paper Documents:* Keep paper documents in a locked file cabinet or drawer in a secure area. Do not leave the keys in an unlocked drawer. Access to the keys for the locked cabinet or drawer must be accessible only to authorized persons. Some offices use a lockbox that is accessible by a code. The code should be changed whenever a staff member leaves.
- *Electronic Documents:*
    - *Access*
        - Use access controls by limiting who may open a file.
        - Regularly review and update permissions for access.
        - If you cease to need access to the information, request that your access be removed.
    - *Drives:*
        - Using your P Drive is permitted.
        - Using designated departmental shares such as folders on the Q or R drives is permitted. The folder must have access controls. Consult with your Information Steward to learn which folders are permitted and who controls their access.
    - *Email:* NEVER use email to store SPI.
    - *Cloud Services:*
        - The only cloud service currently approved at Tufts for storing and sharing SPI is Tufts Box.

        - See the Tufts Box Use Guideline for what information may be stored in Tufts Box.
        - See Box Collaboration/Sharing Security Tips for information on using Box.
        - Be sure to control access to documents stored in Tufts Box.
        - Only use Box Sync with strong controls on the endpoint device, as described below. See Box Sync Security Tips.
        - Do NOT use any other cloud service, such as DropBox or One Drive, to share or store any document that includes SPI. These services have not been approved for this specific use by TTS Information Security or in a written Tufts university-wide policy.
    - *Local Servers:* If your office has a local server that stores SPI, contact your Information Steward. There are specific management requirements based on Massachusetts regulations.

USING A DESKTOP PC

- Never use a public computer for SPI.
- Tufts supplied and managed PCs may be used for SPI. Save SPI on the PC only as otherwise provided in these Guidelines.
- A PC that isn't managed by TTS may only be used for SPI if the PC is protected by the Required Strong Controls (below) and if the PC is used only to view SPI using a secure connection, such as the Tufts VPN or Tufts Secure. A PC that isn't managed by TTS may never be used to store SPI, whether in "Documents," the "Desktop," "Downloads" or other location. See the requirements listed below under Required Strong Controls.

USING A LAPTOP, A MOBILE PHONE, IPAD OR OTHER TABLET

- Required Encryption.
    - If SPI will be on a laptop, the laptop must use whole disk encryption. This is a Massachusetts regulatory requirement. Contact the TTS Service Desk for full-disk encryption services for Tufts-owned devices.
    - Do NOT use *any* portable device for SPI, unless the device is encrypted. This is a Massachusetts regulatory requirement. Not all mobile phones are encrypted.
- Voicemail. Do NOT use voicemail to communicate SPI. Include a message advising callers to not leave SPI on voicemail.
- Sharing. Tufts-owned devices should not be shared with other persons outside of Tufts, including family members.
- Personal Devices.
    - If a laptop or other portable device is being used for SPI and it is not TTS-managed, it may only be used for SPI if the device is protected by the Required Strong Controls (below) and if the device is used *only* to view SPI, and uses a secure connection, such as the Tufts VPN or Tufts Secure. A device that is not managed by TTS may never be used to store SPI, whether in "Documents," the "Desktop," "Downloads," "Notes" or other location. See the requirements listed below under Required Strong Controls.
    - The one permitted exception to storing information on a personal device is the syncing of your exchange email to your personal device using the native email client on the device or by downloading the Outlook Exchange App to the device. It is very important that you understand that you will then have a copy of emails on your device. The use of email for SPI is strongly discouraged. See **Email Restrictions for Sensitive Personal Information.** The TTS website includes information about setting up email on your mobile phone, including selecting using a secure connection.
    - Do not use Box Sync to sync Tufts information to a personally-owned device..

- Wireless. If using wireless on campus, ONLY use Tufts Secure, which is encrypted. Do NOT use Tufts Wireless or Tufts Guest, which are not encrypted.
- Network Connection for Working Off-Campus. If working away from Tufts, be sure to use the Tufts VPN.

REQUIRED STRONG CONTROLS FOR PERSONAL DESKTOPS, LAPTOPS AND OTHER DEVICES

When using a personal or other desktop, laptop or other portable device that is not managed by TTS, you are responsible for installing and maintaining the technologies to the standards set forth below.

❑ **Require a Password** for access to your device and **Use a Strong Password**	Use a strong, unique password to log into the device and protect your login/password by not sharing it with others (including family members). Follow the same requirements as for your Tufts Password.
❑ **Manually Lock your Screen or Power Off** when you leave your device	Every time you leave your device unattended, you should either turn it off or activate the screen lock that requires you to enter your password to resume working. See Screen Lock
❑ **Set your Screensaver to Automatically Activate**	You should configure an automatic screen lock on your devices that requires you to enter a password to resume using the device after 20 minutes or less.
❑ **Review Privacy Settings**	Review the privacy settings on your devices and limit sharing to the minimum necessary. These settings limit applications' access to your location, contacts, calendars and reminders.
❑ **Apply Updates/Patches**	You are responsible for having all critical Operating System (OS), application and browser security updates applied and kept up to date with all new security updates as they are released (for example, Microsoft, Adobe, Google, Firefox). Configure automatic updates wherever possible, and when patches are finished installing, follow any prompts to reboot the device to ensure proper functionality. • Windows updates and other protection tools and advice can be obtained at: http://www.microsoft.com/security/default.aspx • Apple updates are available at: http://support.apple.com/kb/HT1222 or via iTunes Be sure to also update your mobile devices, including your smart phones or tablets. Updates can generally be found on the company website by searching for "security updates."
❑ **Install and use Antivirus Software**	All devices connected to Tufts via remote site access technologies must use current and updated antivirus software to assist in protection from hackers and malware. There are a number of options both free and for purchase. Faculty, staff and students may purchase a

	version of Trend Micro through the university at a discount. Go to https://it.tufts.edu/sw-trendmicro. There are many other vendors with inexpensive options such as McAfee or Norton and free options such as AVG, Malwarebytes, Avast, Sophos and Bitdefender. See Antivirus Applications. When downloading free software, use a trusted website, such as download.cnet.com.
❑ **Install a Firewall**	All devices connected to Tufts remotely, including via wireless, should employ a software or hardware based firewall. Most operating systems have built-in firewalls and enhanced security settings that can be turned on and configured. As an alternative, a firewall can generally be purchased and/or installed where you purchased your device.
❑ **Use Secure WiFi and Bluetooth Settings**	It's recommended that you turn off optional network connections, such as for WiFi and Bluetooth, when you are not using them. Also, limit your WiFi sharing settings to the minimum needed. Be aware that Wi-Fi Sense, which is part of Windows 10, may share access to your networks with others and connect you to open networks automatically. **Do not use the Express settings.** Customize your settings and uncheck the options you don't want. See the Microsoft Wi‑Fi Sense FAQ.
❑ **Limit Sharing of Devices**	If you share a personally-owned device with family members, be sure to log out of all Tufts tools and information before permitting any one else to use the device. Consider carefully whether to share a device that you also use for your Tufts work. Often it is through family members that malicious software is inadvertently downloaded to a device.
❑ **Physically Protect all Portable Devices**	Portable devices, such as phones, laptops, and other mobile devices, are particularly vulnerable to theft. They are easily lost or misplaced. All portable devices must be kept secure, password protected and locked when unattended.

USING USBs, DISCS AND OTHER PORTABLE MEDIA

- Do NOT use for SPI.
- If have used for SPI, see provisions for retiring devices under General Safeguards for All Sensitive Information.

WEBEX

Think before you share. Be mindful that when you share your screen through WebEx, your entire screen will be visible. Be sure to close any document that contains SPI if it is not intended to be shared. Know who is receiving the information.

USING OTHER SERVICES AND APPLICATIONS; THIRD PARTY VENDORS AND OTHER SERVICE PROVIDERS

Before using a service or application that is not discussed in these Guidelines, it is important that you contact your Information Steward to learn whether it is a Tufts-approved service or application for SPI. Massachusetts regulations require using only those third-party vendors and other service providers that commit in writing to complying with particular requirements for protecting SPI. This prohibition applies to all third party applications and services, whether free or paid. If you are investigating working with a third party vendor or other service provider that is not approved for working with SPI, contact TTS Contract and Licensing Services.

WORKING OFF CAMPUS AND TELECOMMUTING

If you work remotely, you are responsible for protecting Tufts data and systems whether the data or systems are located remotely or are located at Tufts facilities but accessed remotely. You must follow the TTS Technology Guidelines and Services for Working Off Campus or Telecommuting whether you are telecommuting or occasionally working remotely.

See the requirements described above for using a personal PC or laptop for SPI.

The requirements provided in these Tips and Guidelines for protecting SPI at Tufts must be complied with when working remotely as well. These procedures include:

- Paper documents must be kept secure.
- Disposal of paper documents must follow the same secure procedures identified above.
- When working away from Tufts, always use the Tufts VPN.
- Do not use personal or other copiers, printers, fax machines or scanners that are not Tufts provided for SPI. The hard drives retain usable data.
- If using email to transmit or receive SPI, the SPI must be encrypted.

COMPLIANCE AND DISCIPLINARY ACTION

The University shall take appropriate disciplinary action against employees and others for violating security provisions of the University's policies and guidelines.

EMPLOYEES LEAVING YOUR OFFICE

Any separated employee must:

- Return all records containing SPI that may be in his or her possession (including all information stored on laptops or other portable devices or media, and in files, records, work papers, etc.).
- Surrender all keys, IDs or access codes or badges, business cards, and the like, that permit access to Tufts premises or information.
- Return any laptop, desktop or other device that was purchased by Tufts, unless otherwise agreed in writing with an authorized Tufts representative. When it is returned to Tufts, it should always be sent to TTS to have the hard drive securely wiped. If you have been granted permission to retain the device, the hard drive should first be securely wiped by TTS to remove Tufts institutional data.

When an employee leaves your office:

- Disable all physical and electronic access to SPI as soon as possible.
- Confirm that all remote electronic access to all forms of SPI has been promptly disabled.
- Before the employee's PC, laptop or other device is transferred to any other employee, be sure that it is securely wiped as provided above.