Data Security and Confidentiality Policy

Contents of Policy

- Policy Overview
  What is Considered Confidential Information?
  Confidential Personally Identifiable Info
  Confidential Non-Personally Identifiable Info

- Guidelines
  Accountability and Security
  Controlling Access
  Information Handling
  Electronic Information
  Physical Documents
  Verbal Information

- Remote Access
  Obtaining Access
  Working from Home
  Mobile Employee

- Working with Vendors
  Protecting Confidential Information

- Exiting Employees

Policy Overview
Harvard University is committed to protecting information resources that are critical to its academic and research mission. Protection may be governed by legal, contractual, financial or University considerations.

Some of the data that Harvard departments deal with is confidential and may contain information about individuals or University operations and plans that must be protected against general disclosure. The following provides guidelines on HUIT employee responsibilities in the collection, handling and use of information considered confidential and sensitive.

What is Considered Confidential Information?
Confidential information is information about a person or an entity that, if disclosed, could reasonably be expected to place either the person or the entity at risk of criminal or civil liability, or be damaging to financial standing, employability, or reputation. Harvard is bound by law or by contract to protect some types of confidential information. Additionally, Harvard requires protection of some other kinds of information beyond legal or contractual requirements as an additional safeguard.

Confidential Personally Identifiable Information
Confidential personally identifiable Information includes information that can be linked directly or indirectly to individual people. Harvard's requirement to protect confidential personally identifiable information is largely governed by law or contract (e.g., HIPAA, FERPA, GLB, PCI, and human subject data). Examples include Social Security number, Harvard University ID, credit card, health and employment records, human subject data, and all FERPA non-directory information about students and former students.
Confidential Non-Personally Identifiable Information
Confidential non-personally identifiable information includes summary information about people where the identities of individual people cannot be determined and information about university-related activities. Harvard's requirement to protect confidential non-personally identifiable information is governed by Harvard's own policies. Examples include detailed information about some University buildings, activities or events, information about future University development plans, and grant information.

Guidelines
Accountability and Security
All information gathered and maintained by the staff for the purpose of conducting University business is considered institutional information, and as such, each staff person who uses, stores, processes, transfers, administers and/or maintains this information is responsible, and should be held accountable for its appropriate use. Responsible parties and proper security measures should be established to protect user files and system resources from loss, damage, inappropriate access and unauthorized disclosure.

Controlling Access
Before individuals are given access to sensitive information, they should be trained in the importance of protecting that information from being disclosed. While gathering information as required by job responsibilities, staff should make reasonable attempts to prevent disclosure. Access to confidential information and to systems containing confidential information should be confined to staff that need to know, and must be controlled by a process that meets the following criteria and characteristics:

- Access to University administered systems (Oracle, PeopleSoft, Harvard Data Warehouse, etc.) should be restricted to those who require it as part of their job description.
- The Harvard PIN Server is to be used for all applications at Harvard that access confidential information.
- Confidential information, IDs and passwords transported over a network must always be encrypted.
- All access must be by individuals who identify themselves uniquely to the systems.
- A combination of a log-in name and a password known only by the user, or a combination of a log-in name, a password known only by the user, and a piece of data generated by an electronic device in the possession of the user (e.g., SecureID card).
- HUIT Security recommends the following guidelines for passwords that are used to access systems containing confidential information:
  o Never give your username, password or Harvard Key to anyone else.
  o Never use someone else’s user name, password or Harvard Key.
  o Do not use easy-to-guess passwords.
  o Be aware of those around you to ensure they can’t watch you typing your passwords or Harvard Key.
  o Do not write down passwords or Harvard Key.
  o Do not allow others to access programs or data from within your account.
  o Change your password often.
  o Log off your workstation when leaving for the day.
  o Lock your workstation when leaving the area.
  o Do not use your Harvard Key with external vendors.
For more information on controlling data access, please go Risk Management & Audit Services.

Information Handling
Staff must take special care when transporting, storing, displaying and disposing of confidential information regardless of the data form.

Electronic Information
Electronic information is at particularly high risk due to the ease of transport. Staff should take the following precautions when dealing with confidential information electronically:

- **Computer Systems.** Staff should ensure that the software on their computers is secure and the machines are operated in a way to minimize the chance of a security breach. All computers used to access Harvard confidential data must have installed an approved anti-virus, Internet security and firewall software applications.

- **Data transmission.** Staff should take the following precautions when transmitting information electronically:
  - Email may, in some situations, be considered an insecure mechanism for exchanging information. The confidentiality of information contained within email messages can be exposed, especially when either the sender or any of the recipients are off-campus or use a wireless network connection.
  - Special care should be taken when selecting addresses or distribution lists to avoid unintended recipients from receiving the information.
  - Salary information and ID information should not be transferred via email.
  - When sending a fax, be sure that the correct number is dialed and that a cover sheet is always used.

- **Data Storage.** No member of the Harvard community is permitted to store Social Security, credit card, or bank account numbers in any way relating to Harvard or Harvard sponsored activities on any user computer. This information must be stored on protected servers or secure shared file systems. This rule applies to all desktops and laptops, whether the computer is owned by Harvard or not, and whether the data is encrypted.

- **Data Disposal.** Destruction of information on computer disks and other magnetic formats should be done with an overwriting process that meets Federal Guidelines. Simply “erasing” the data is not sufficient to completely destroy the information, resulting in potential recovery and disclosure. Hard disk drives or other data storage systems may require physical destruction.

- **Display Screens.** The display screens for PC’s and workstations used to view or process sensitive information should be positioned such that those who do not have access cannot view them. A password-protected screensaver should be activated on your computer to ensure your system is secure when away from your work area.

- **Testing and Education.** The University maintains additional environments for development in which institutional data is retained. Precautions should be taken when testing or educating others to use systems that contain sensitive information. Application system developers and installers shall provide user education on security issues when new systems are installed. Copies of production data should not be used for purposes that may compromise the confidentiality of individuals or organizations.

Physical Documents
When handling physical documents containing sensitive information, steps should be taken to safeguard the information from disclosure. Below are some HUIT Security recommended guidelines for handling documents containing sensitive information:

- Documents should be clearly stamped “Confidential” and/or “Do not copy or distribute.”
Data Security and Confidentiality

- Documents should be stored in a secure location (a room, file cabinet, etc.) to which only specifically approved individuals have access through lock and key at all times.
- Never leave extra copies of handouts in conference rooms or other public areas.
- When printing to a public printer, be sure to retrieve documents immediately.
- Documents must be shredded using a University-approved device or shredding facility prior to being discarded.

Verbal Information
When discussing sensitive or confidential information with other individuals either within or outside of the University, HUIT Security recommends the following guidelines:

- Staff should not verbally disclose confidential information to individuals outside of the University (e.g., vendors or peer institutions) except as authorized when obtaining quotes, purchasing, benchmarking or doing research.
- When passing information to individuals outside of the University, staff should ensure that the recipient understands that they cannot disclose or use the information in a way that is inconsistent with the intended use.
- When communicating confidential information to others within the organization, staff should make sure that these conversations only take place in areas where unintended recipients cannot overhear information.
- When a telephone speakerphone is used during a phone conversation, staff should make sure that all participants in the conversation know that a speakerphone is being used and are informed of each participant in the room. Speakerphone meetings should only take place in an office or conference room with a closed door so that remote participants in the meeting can be ensured of the confidential nature of the conversation.

Remote Access
Individual employees and departments need to acknowledge ownership and responsibility for the Harvard information accessed remotely or stored on remote access devices.

Obtaining Access
Remote access to desktop or laptop computers at Harvard is prohibited unless specific permission has been granted by an employee's supervisor and IT support group, or if the access is performed by a help desk as part of the process of assisting an employee with a problem. Thus, applications such as "VPN RDP" are not to be installed on any Harvard computer without specific permission by an employee's supervisor.

All remote access to Harvard systems must be done using a Harvard-owned and managed computer. Such computers will be inventoried and configured by local technical support groups and will conform to normal Harvard Central Administration standards. The computer must have approved, standard licensed software installed, SMS or other standard remote management and support tools. Local technical support groups will decide if employees will have administrative rights on the Harvard-provided computer.

Working from Home
Staff should remember that even though the transmission of information outside of the Harvard network can be achieved through secure mechanisms (e.g. VPN), once this information is saved on a remote system (e.g., in your home), the security of these documents is no longer assured. Confidential information stored on remote systems should be encrypted. The Harvard owned computer is for the exclusive use of the employee and must not be used by others.
**Mobile Employee**
A growing number of staff continues to rely on mobile computing devices (MCDs) for work and personal uses. Laptop computers, personal digital assistants (PDAs), USB memory (aka thumb drives), smart phones, iPods, and a variety of wireless accessories have become pervasive on campus and in society. Although these devices provide conveniences, they also include unacknowledged risks.

Users should always be wary of what kind of data is stored on these devices including:

- Confidential financial information
- Account names and passwords
- Social Security and/or credit card numbers
- Personal contact names and phone numbers
- Decryption keys or pass-phrases

HUIT Security recommends that you leave data on the server as much as possible and do not copy sensitive information onto the mobile device. A password-protected mobile device will usually prevent a novice from gaining access to the internal information, but a skilled and motivated person generally has tools that allow him/her to crack the password or simply bypass it.

**Working with Vendors**

**Protecting Confidential Information**
When negotiating contracts with third-party vendors, staff should consider whether such vendors require access to University databases or to other filing systems containing confidential information. Vendors should be contractually obligated to implement data protection and security measures that match the University's practices. As with the outside vendor, the staff must be careful not to disclose confidential information contained within an agreement or contract.

If a vendor/consultant is to have access to information as determined by HUIT, the request for proposal (RFP) and resulting contract should have specific elements defined:

- Description of the purpose for access to information.
- Specific areas to which access is limited.
- Vendors/consultants should be held accountable for the security and protection of any information that is in their possession.
- Consultants must not disclose, allow access to, or permit other uses of information beyond what is outlined within the contract.
- Method of on campus authentication must be determined.
- No consultant or contractor is permitted to store Social Security, credit card, or bank account numbers in any way relating to Harvard or Harvard-sponsored activities on any user computer. This information must be stored on protected servers or secure shared file systems. This rule applies whether the computer is owned by Harvard or not, whether the data is encrypted or not, and whether the computer is portable or desktop.

**Exiting Employees**
Some of the University's most important assets may be intangible forms of intellectual property. Managers should be aware that employees who are exiting the University might be taking proprietary information. The following guidelines should be followed during the exiting process:

- Managers should make sure that proprietary information, such as vendor contracts or pricing information, including manuals, diagrams, and system flowcharts with internal financial information and technology applications are not removed from Harvard property.
Data Security and Confidentiality

- Staff should be instructed that they cannot disclose information outlined above to future employers or vendors or in any way use this information outside the University environment.
- Access to all systems and buildings must be terminated immediately.
- No software licensed by the University is copied or transferred to the employee.
- No unauthorized transfer of University institutional data is made from University servers or other computers to any personal computer, mobile computer, or storage device/portable media.

For further information regarding best practices around Data Security and Confidentiality, please contact Christian Hammer, Chief Information Security Officer (christian_hamer@harvard.edu) or visit the Harvard University Information Security and Privacy Web Site.