FAS

Information Security 201

Desktop Reference Guide

Introduction

Harvard University is committed to protecting information resources that are critical to its academic and research mission. Harvard is equally committed to preserving an environment that encourages academic and research collaboration through the responsible use of information technology resources.

The protection of confidential information is governed by legal, financial, and contractual obligations, in addition to University policy:

Federal Law

- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)

State Law

- 201 CMR 17.00: Standards for The Protection of Personal Information of Residents of the Commonwealth

Harvard Policy

- Harvard Enterprise Information Security Policy (HEISP)

University Contracts

- Non-disclosure agreements, sponsored research agreements, etc.

Harvard has developed an Enterprise Information Security Policy to ensure that its technical resources are properly protected, that the integrity and privacy of confidential information is maintained, that information resources are available when needed, and that those who use these resources understand their responsibilities. For the complete text of this policy, see *www.security.harvard.edu*.

Table of

Policy

- ☐ Confidential Information.....6
- ☐ Student Information.....8
- ☐ Annual Compliance Requirements.....9
- ☐ Encryption Policy for Laptops.....9
- ☐ Web Privacy Statements.....9
- ☐ Music and File Sharing Software.....10
- ☐ Working with Vendors.....10

Basic Best Practices

- ☐ Choose a Secure Password.....11
- ☐ Protect your Password.....12
- ☐ Password Protect your Computer and Mobile Device.....12
- ☐ Install the Latest System Updates on your Computer.....13
- ☐ Install Anti-Virus Software on your PC.....13
- ☐ Securely Dispose of Equipment and Data.....14

Contents

Daily Best Practices

- ☐ Lock your Computer when Away from your Desk.....15
- ☐ Save your Confidential Information on a Secure Server.....15
- ☐ Exchange Confidential Information Securely.....16
- ☐ Navigate the Web Cautiously.....16
- ☐ Do Not Reply to Suspicious Email.....17
- ☐ Use a Secure Connection when Working off Campus.....18
- ☐ Protect Confidential Papers and Physical Records.....18

Report Security Incidents (inside back cover)

Additional Help & Resources (back cover)

POLICY

☑ Confidential Information

Information about a person or an entity that, if disclosed, could reasonably be expected to place the person or the entity at risk of criminal or civil liability, or to be damaging to financial standing, employability, reputation, or other interests.

Harvard is bound by laws, such as FERPA and HIPAA, and by contracts, such as some grants and vendor contracts, to protect some types of confidential information. Additionally, Harvard, under University, School or unit policies, requires protection of other kinds of information about the University or Schools, faculties, departments and other units, and about Harvard property (tangible or intangible). Confidential Information also includes High-Risk Confidential Information, as defined below, as well as other non-public personally identifiable information about individuals.

High-Risk Confidential Information

High-Risk Confidential Information (HRCI) is personally identifiable information whose confidentiality is governed by law. HRCI includes a person's name in conjunction with the person's Social Security, credit or debit card, individual financial account, driver's license, state ID, or passport number, or a name in conjunction with biometric information about the named individual. HRCI also includes personally identifiable human subject information and medical information. Improper access to, use of, or release of High-Risk Confidential Information may trigger legal reporting requirements. Such information is subject to legal requirements upon disposal.

Examples

Examples of Confidential Information (in addition to HRCI) include the following:

- Unpublished University financial information and development plans
- Salary information
- Employee benefits and other HR information
- Grades and other non-directory education records
- Financial information about applicants
- Non-public personal and financial data about donors
- Harvard identification numbers
- Information received under grants and contracts subject to confidentiality requirements
- Information on facilities security systems
- Unpublished research data
- Invention disclosures and patent applications
- Information specifically designated as private or confidential

☑ Student Information

Harvard maintains extensive information about students and former students. The Family Educational Rights and Privacy Act (FERPA) is a federal law that controls access to these records.

Student Information falls into two categories: directory information, which can generally be included in published or electronic directories, and all other information, which is confidential.

Harvard's Registrars have agreed on a common set of public directory information for students. Examples include name, address, telephone listing, email address, photograph, date of birth, and field of study. A complete list can be found in the *Harvard College Handbook for Students* and the *GSAS Handbook* under "Academic Information" (see *www.registrar.fas.harvard.edu*).

All other information that Harvard collects about a student is considered confidential. This information may be disclosed to University officials with a legitimate educational interest, that is, to officials who require the information in order to execute their professional responsibilities in relationship to their roles within the FAS.

The Harvard University ID is not directory information, and must be protected. Posting lists of Harvard IDs and grades, for example, is not permissible. It is also a violation of FERPA to leave essays or other student material containing names or Harvard IDs and grades in a pile to be picked up by students.

FERPA Block

By application to the Registrar's Office, students can exercise their right to restrict the display or public disclosure of their directory information. Known as a "FERPA Block," this designation prohibits the disclosure of *any* information about these students.

☑ Annual Compliance Requirements

On an annual basis, all FAS staff are required to complete education about Information Security and to certify their awareness of Harvard's policies. FAS Human Resources will provide additional information about this requirement. In addition, all University employees must annually consent to a confidentiality agreement. This can be found under the "Self Service" menu in PeopleSoft.

☑ Encryption Policy for Laptops

The theft of a Harvard computer or portable storage device (e.g., CD, USB flash drive, external hard drive) must not put confidential information at risk of disclosure. Because University-owned laptops are particularly vulnerable to loss or theft, they must be encrypted.

Encryption software encodes and password-protects the contents of your hard drive when your computer is powered off. If you use a Harvard-owned laptop, make sure that it is encrypted using PGP Whole Disk Encryption. For assistance with this process, contact *help@fas.harvard*.edu. You can also find software and instructions at *http://pgp.fas.harvard.edu*.

University policy prohibits storing HRCI on laptops or other portable devices, even if they are encrypted, or transmitting HRCI by other than encrypted means. Other confidential information must be encrypted if it is stored on a portable device. For more information see "Daily Best Practices" below.

☑ Web Privacy Statements

All Harvard web sites must have a link to a privacy statement on the first page of the site. The privacy statement must also appear on the entry page of any group of pages under different management. The link must be in a visible location (often on the bottom line), in a font not smaller than that used elsewhere on the web page. The site must adhere to the privacy policy that is posted.

Examples of privacy statements can be found at *www.security.harvard.edu* under the heading "Resources" and subtopic "Sample Statements."

☑ Music and File Sharing Software

Do not install peer-to-peer filesharing software (e.g., BitTorrent, eDonkey, Gnutella, and LimeWire) on your Harvard computer without specific authorization. Doing so may subject you to University disciplinary action, as well as to civil or criminal penalties. File sharing software can pose a security threat to your computer and to the Harvard network.

If peer-to-peer file sharing software is required for your job, FAS Information Security must first review it to ensure that its use will not pose a security risk.

Legal use of copyrighted material with the permission of the copyright owner or under the fair use or another exemption under copyright law is permitted for legitimate purposes, such as research or teaching, as required by an individual's position at Harvard.

For more information on Harvard's policy with respect to digital copyright law, see *www.dmca.harvard.edu*.

☑ Working with Vendors

Vendors dealing with Harvard confidential information, whether or not they obtain the data directly from the University, must have a written contract covering their services, including a requirement to protect confidential information. If the services involve HRCI or regular work with any confidential information, then the contract should include or attach a contract rider governing the protection of that information. Contract riders can be found at *www.security.harvard.edu* under the heading "Enterprise Security Policy" and subtopic "Working with Vendors."

Those who wish to contract with a vendor to collect or work with High-Risk Confidential Information must obtain prior approval from the University CIO. The security policies and procedures of vendors who will receive, collect, store, or process this data must be reviewed by the Harvard Information Security Officer and/or Harvard Risk Management and Audit Services.

For more information, contact *security@fas.harvard.edu*.

Basic Best Practices

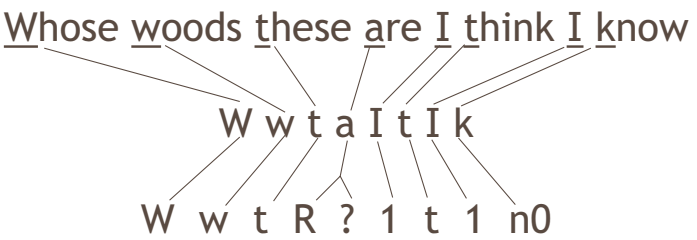
☑ Choose a Secure Password

- Choose a password that you can remember without having to write it down.
- Use at least 8 characters.
- Mix upper and lower case letters, and include combinations of numbers and symbols.
- Do not use real words, names, dates, phone numbers, addresses, or personally identifiable information as part of your password.

Tips for Choosing a Secure Password:

- Take the first letter of each word in a phrase you know.
- Substitute or add other letters, numbers, symbols, and capitalization.
- Do not use the example here or one that appears in any other document as your password.

EXAMPLE:



☑ Protect your Password

- Never share your password with anyone.
- Never write down your password (e.g., on a sticky note), especially next to your computer.
- FAS IT will never ask you for your password. Moreover, no one affiliated with Harvard can legitimately ask you for your password until you leave the University.

☑ Password Protect Your Computer and Mobile Device

Instructions for Windows XP:

- Press Ctrl-Alt-Delete
- Select “Change Password...”
- Under “User name” enter “Administrator”
- Under “Log on to...” select “this computer” from the pull-down menu

Instructions for Mac OSX:

- Go to the “General Tab” under “System Preferences”
- Select “Require password to wake this computer from sleep or screen saver”

Instructions for BlackBerry:

- Go to “Options”
- Select “Security Options” from the scroll-down menu
- Choose “General Settings”
- Next to “Password,” choose “Enabled” from the pull-down menu

Instructions for iPhone:

- Go to “Settings”
- Select “General”
- Select “Passcode Lock”

☑ Install the Latest System Updates on Your Computer

Ensure that you are running the latest version of the operating system that was installed on your computer when you obtained it.

For PCs:

- Launch Internet Explorer, and go to www.windowsupdate.com
- Choose the "Express" option to obtain high-priority updates
- Go to the "Start Menu," right-click on "My Computer," and select "Properties"
- Open the "Automatic Updates" tab and select a time each day that updates can be automatically downloaded and installed. Choose a time that you know your computer will be turned on and connected to the network.

For Macs:

- Go to www.apple.com/downloads/macosx

☑ Install Anti-Virus Software on Your PC

PC owners should download and install approved anti-virus software on their systems:

- Go to www.fas-it.fas.harvard.edu
- Select "Software Downloads" from the main menu

☑ Securely Dispose of Equipment and Data

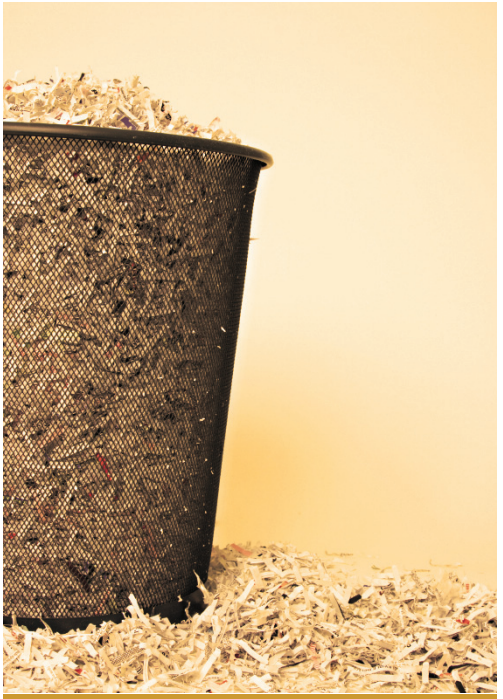
Before disposing of your computer:

- Securely erase the entire hard drive, including all data, software, and operating system components. Deleting your files or reformatting the hard drive is not sufficient. Contact FAS Information Security at *security@fas.harvard.edu* for more information.
- Contact DataShredder, a Harvard preferred vendor, to dispose of erased hard drives:

  Data Shredder
  800-622-1808
  www.datashredder.net

Before disposing of physical (non-electronic) media:

- Use a cross-cut shredder to ensure that confidential documents cannot be reconstructed.
- Dispose of hard-copy High-Risk Confidential Information, or CDs containing HRCI, in an approved, locked shred bin.



Daily Best Practices

☑ Lock your Computer when Away from your Desk

- Set your screen saver to lock automatically after no more than fifteen (15) minutes of inactivity.
- Before leaving your office for an extended period, either shut down your computer or put it into sleep mode:

  For PCs, press CTRL-ALT-DEL and select "Lock Computer"

  For Macs, go to the "General Tab" under "System Preferences," and then select "Require password to wake this computer from sleep or screen saver"
- Use a cable lock to secure your laptop.

☑ Save your confidential Information on a Secure Server

- The best location for confidential information is a secure server, such as the FAS shared file server.
- Never store High-Risk Confidential Information (HRCI) on your desktop or laptop, USB flash drive, CD, or external hard drive, even if the computer disk or device is encrypted.
- Confidential information that is not High-Risk can only be stored on a USB flash drive, CD, or external hard drive if it is encrypted. If you need to copy confidential information onto one of these devices, contact *security@fas.harvard.edu*.

☑ Exchange Confidential Information Securely

Use the Accellion Secure File Transfer Server to send files containing confidential information to others. Do not use regular email for this purpose.

- Login to Accellion at *https://fta.fas.harvard.edu* using your FAS or Life Sciences email address and password
- When you see a message regarding a digital signature or Java security prompt, click "OK" and then "Run" to continue
- In the "Send File" window, enter the address of the intended recipient, as well as a subject line and message
- Choose "Browse" to attach the confidential file to your message
- Choose "Send"
- The recipient will receive email with a link to the secure Accellion server where the file will be available for 15 days

Complete instructions on using Accellion can be found on the FAS IT website:

- Go to *www.fas-it.fas.harvard.edu*
- In the search field at the top of the page, enter "Accellion"

☑ Navigate the Web Cautiously

- Never provide personally identifiable information on a website that you did not intend to visit.
- Before submitting any confidential information, check for "https" in the URL and look for the lock symbol in your browser.
- Beware of non-Harvard URLs that claim to be official University websites.
- Do not use your FAS password for non-Harvard websites.
- Web sites that support gambling, pornography, or illicit behaviors may contain harmful code that can compromise your computer as well as your data.

☑ Do Not Reply to Suspicious Email

- "Phishing Schemes" are fraudulent email messages claiming to be from a legitimate source that ask you to submit confidential information such as your username, password, or date of birth.
- Never provide personally identifiable information in response to unsolicited email.
- Do not open email attachments that you were not expecting to receive.
- Beware of unsolicited email with links to the "Harvard" PIN site.
- Always copy and paste a link that you receive in email; don't just click on it.
- Never share your password with anyone.
- FAS IT will never ask you for your password. In fact, no one affiliated with Harvard can legitimately ask you for your password until you leave the University.

☑ Use a Secure Connection when Working off Campus

Install Virtual Private Network (VPN) software, known as AnyConnect, to use when connecting to Harvard's network from off campus:

- Go to *https://vpn.fas.harvard.edu*
- At the username prompt, enter your complete FAS email address

☑ Protect Confidential Papers and Physical Records

- Keep confidential paper records in locked filing cabinets when not in use.
- Keep fax and copying machines that are used with confidential information in locked, protected areas.
- Restrict physical access to any facility that contains confidential information. Access control measures include smart card swipes, PIN keypads, locked doors, and guards who can check photo IDs.
- Do not leave confidential information on copiers, fax machines, or other shared devices.

Report Security Incidents

Immediately report any loss or breach of High-Risk Confidential Information to FAS Information Security, who in turn will apprise the University CIO and Office of the General Counsel:

FAS Director of Information Security:

(o) 617-496-5704 | (c) 617-999-3867

FAS Information Security Team:

888-858-5357

In the event that any Harvard data, computer, or mobile handheld device is lost or stolen, report this to FAS Information Security (*security@fas.harvard.edu*), your Department Administrator or Chair, and the Harvard Police (617-495-1215).

FAS Information Security has a Computer Incident Response Team that can scan your computer for vulnerabilities or assist with any computer security concern. Please contact *security@fas.harvard.edu* at the first sign of a security issue. Do not take action on your own, as this may damage or destroy evidence required for a digital forensic investigation.

You can also contact FAS Information Security in the event of the following:

- You suspect that there has been a data breach
- Your password has been compromised
- The performance of your computer suddenly decreases
- You see new software on your computer that you do not recognize
- You believe that you have a computer virus
- You encounter a phishing scheme

Additional Help & Resources:

Harvard's Information Security Website: *www.security.harvard.edu*

FAS Information Security: *security@fas.harvard.edu*

FAS IT Support: *help@fas.harvard.edu, 617-495-9000*

Information Security 201
Desktop Reference Guide
April 2010
FAS Information Technology
Harvard University