
HARVARD UNIVERSITY
Information Technology

# IAM Security & Privacy Policies

## Scott Bradner

| | | | |
|---|---|---|---|
| November 24, 2015<br>December 2, 2015 | Tuesday<br>Wednesday | 9:30-10:30 a.m.<br>10:00-11:00 a.m. | 6 Story St. CR |

# Today's Agenda

- How IAM Security and Privacy Policies Complement University Policies:
  - University Information Security Policy
  - University Policy on Access to Electronic Information
- HUIT IAM Security and Privacy Policies

# **Harvard University**
# Information Security Policy

# University Information Security Policy

**The University has adopted an information security policy that:**

- Covers all University information in any form
- Applies to all the entire University community
- Includes a standard way to classify University information
- Includes high-level policy statements relating to protecting University information
- Includes requirements that must be met to ensure the proper protection of University information
- Includes specific “how-tos” that can be used to meet these requirements
- See: http://policy.security.harvard.edu/

# Harvard Confidential Information: Background

- Harvard maintains lots of information about individual people and about the university itself
- Some of this information is considered "confidential", either because non-Harvard laws and regulations say so or because Harvard has decided to keep it confidential.
- Three broad classes of information:
  - Information about individuals, whether as subjects in university research or as affiliates of the university (e.g. students, employees)
  - Non-individual research information with implications for national security
  - University operating data, such as financials or vendor contracts
- Under U.S. federal law, research on or about individuals must be reviewed by an Institutional Review Board (IRB)
  - IRBs review research plans to be sure the research complies with federal guidelines and determines the level of protection needed for any information generated by the research

# Harvard Confidential Information: Laws

- Harvard is subject to a number of U.S. federal laws as well as laws of the states in which Harvard operates or, in some cases, laws of states that Harvard students come from
- State laws require protection of certain financial information (e.g. SSNs)
- Federal laws require protection of most student information (FERPA), medical record information (HIPAA) and some financial information (GLB)
  - E.g., students, and prior students, have a right under FERPA to block public publication of information about themselves
- Harvard, as is the case with most private US employers, has decided to keep most employee-related information confidential
- The University Information Security Policy is designed to meet the requirements of the appropriate laws and decisions the university has made concerning its own information
- The policy covers both research and non-research information

# Data Classification

| | |
|---|---|
| LEVEL 1 | Public information |
| LEVEL 2 | Information the University has chosen to keep confidential, but the disclosure of which would not cause material harm |
| LEVEL 3 | Information that, if disclosed, could cause risk of material harm to individuals or the University |
| LEVEL 4 | Information that, if disclosed, would likely cause serious harm to individuals or the University |
| LEVEL 5 | Information that, if disclosed, would cause severe harm to individuals or the University |

# Level 1 Information: Examples

- Directory information (not including people with a FERPA block)
- De-identified research data
- Calendars for public events
- Press releases
- Campus maps
- Research data classified by an IRB as public

# Level 2 Information: Examples

- Drafts of research papers
- Patent applications
- Maps of campus utilities
- Building layouts
- Research data classified by an IRB as Level 2
- Information subject to a data use agreement that specifies a protection level best met by Level 2 classification

# Level 3 Information: Examples

- Information that includes HUIDs
- University financial information
- Employee records that do not include SSNs or bank account numbers
- Non-directory student information
- Directory information for students with a FERPA block
- Research data classified by an IRB as Level 3
- Information subject to a data use agreement that specifies a protection level best met by Level 3 classification

# Level 4 Information: Examples

- Credit card numbers
- Social security numbers
- Passwords
- Personally identifiable genetic information
- Personally identifiable healthcare information
- Student financial information
- Research data classified by an IRB as Level 4
- Information subject to a data use agreement that specifies a protection level best met by Level 4 classification

# Level 5 Information: Examples

- Research data classified by an IRB as Level 5
  - The only Level 5 information that I know of at Harvard is research related
- Information subject to a data use agreement that specifies a protection level best met by Level 5 classification

# More Details on Levels 1-4

- Information classified as Levels 1 through 4 can be stored on computers connected to networks if proper protections are in place and maintained
- Level1 information can be public
- Computers containing Level 2 information must be protected by common sense mechanisms such as virus checkers
- Level 3 information must be encrypted when stored if the computer on which it is stored is directly accessible (e.g. portable device or removable media)
- Level 4 information must remain on servers and cannot be directly accessible from the Internet or from most of the Harvard network (access through a VPN is OK)

# Level 5 is Special

- Level 5 information cannot be stored or processed on a computer connected to a **wireless** network
- Level 5 information cannot be stored or processed on a computer connected to a **wired** network — except for an isolated, limited-access, local wired network within a secure facility

# University Policy Statements: Introduction

- Harvard University's information security policy statements define the high-level goals involved in protecting University information
- Each policy is supported by one or more situation-specific requirements
  - e.g. different requirements based on data classification
- Policy statements are intended to be long-lived and technology-independent
  - e.g. "All users are responsible for protecting Harvard confidential information that they use in any form from unauthorized access and use."

# University Policy Statements (1 of 3)

1. All users are responsible for protecting Harvard confidential information that they use in any form from unauthorized access and use.
2. All users are responsible for protecting their Harvard passwords and other access credentials from unauthorized use.
3. All access to and use of Harvard confidential information must be for authorized Harvard purposes.
4. All access to systems handling Harvard confidential information must be for authorized Harvard purposes.
5. All persons accessing Harvard confidential information must be trained in protecting such information.
6. All users of Harvard confidential information resources must be accurately and individually identified.

# University Policy Statements (2 of 3)

7. Harvard confidential information must be protected on any user computer or portable device.
8. All servers storing Harvard confidential information must be protected against improper access.
9. All servers and locations where Level 4 or 5 information is stored must be accurately identified and physically secure.
10. Electronic and physical records containing Harvard confidential information must be appropriately protected when transported or transmitted.
11. Software must be kept up to date on all computers and devices that process or store Harvard confidential information.
12. There must be a mechanism to limit the number of unsuccessful attempts to log into an application or server that processes or stores Harvard confidential information.

# University Policy Statements (3 of 3)

13. Electronic and physical records containing Harvard confidential information must be properly disposed of so that the information cannot be retrieved or reassembled when no longer needed or required to be kept.

14. Harvard must conduct appropriate due diligence to ensure that third parties that store or have access to Harvard confidential information are capable of properly protecting the information and must require such third parties to protect the information.

15. Any actual or suspected loss, theft, or improper use of or access to, Harvard confidential information must be reported.

# University Policy Statements: What These Mean

- **You** must protect confidential information
- **You** must protect your passwords
- **You** must not access information for which you are not individually authorized
- **You** must not access systems for which you are not individually authorized
- **You** must be trained for the types of data you use
- **You** must protect any information you have on your devices
- **You** must protect your servers against improper access
- **You** must ensure locations with risky information you have are secure
- **You** must protect information being transported on physical media
- **You** must patch your computers
- **You** must limit password guesses if your system does its own authentication
- **You** must shred discarded information
- **You** must check the security of vendors before use
- **You** must report lost information or devices

# Requirements for Meeting Policies

- Situation-specific requirements for meeting policies
- Situations covered:
  - You and me (individual users)
  - Our devices (computers, including portable)
  - Physical records we may have
  - Server operators (including virtual servers)
  - People working with vendors
- Some requirements vary based on information classification
- Requirements apply to everyone in the University community working with, accessing, or possessing University confidential information
- Requirements apply to University- and personally-owned devices if they can access or store University confidential information
  - e.g. personally-owned smartphones used to access University email

# Requirements for Users

**These are requirements each of us must meet to ensure protection of University information.**

- Password-related requirements:
  - Protect passwords, and do not share them
  - Use different passwords for Harvard and non-Harvard systems
  - Use strong passwords and change passwords if compromised
  - Not in policy, but use of password manager is strongly recommended
- Other requirements:
  - Only access information for which you are authorized, and do not share
  - Protect the information and dispose of it properly
  - Report any loss or compromise
  - Do not store in unauthorized locations
  - Get training and acknowledge your responsibilities for protecting confidential information

# Requirements for User Devices

**These cover user desktop and portable computers (laptops, smartphones, tablets, etc.) used to access, store or process University confidential data.**

- Device must be configured for secure operation:
  - Use a password, encrypt device, auto-wipe on multiple bad guesses, enable remote wipe, use encryption for communication, etc.
- Patch software quickly
- Report any lost devices that could contain confidential information (including information in email)
- Wipe device before disposing of it

# Requirements for Physical Records

**These cover people who work with confidential University physical records (items on paper, etc.).**

- Protect records (e.g. lock your cabinets)
- Limit access to those with a valid business reason
- Transfer securely and verify receipt (including faxes)
- Properly dispose of unneeded physical records (e.g. compliant shredding)

# Requirements for Servers (1 of 4)

**These cover computers providing access to or processing of University confidential information.**

- Many requirements — with higher security required for higher-level information
- Applies to on-premise and cloud-based physical and virtual servers
- Special requirements for servers or other systems (e.g. HarvardKey) that manage passwords (their own or for others)
  - Must enforce complex passwords
  - Must inhibit password guessing
  - Must store passwords securely and not in a retrievable way
    - E.g. using bcrypt (iterated, seeded hash)
  - Must enforce secure password change mechanisms
  - And so on

# Requirements for Servers (2 of 4)

- Special requirements for all servers with confidential information
  - Know who owns and operates services on server
  - Configure for encrypted communications
  - Change all default passwords
  - Remove generic accounts (where possible)
  - Shared login accounts not permitted
  - Patch promptly
  - Run malware detection software
  - Scan for HRCI

# Requirements for Servers (3 of 4)

- Server operators must be properly trained
- Protect to the level of the highest-level classified information
- Control network-based access
  - Protect using firewalls
  - Filter inbound and outbound traffic
- Report theft or compromise
- Log administrative access and commands, as well as access to HRCI
  - Spool logs off local server
- Review logs, period depends on type of information
- Level 4 servers must not be directly accessible from the Internet or most parts of Harvard's network

# Requirements for Servers (4 of 4)

- Use private addresses (i.e RFC 1918) for Level 4 servers
- Keep servers in secure locations (AWS qualifies)
- Maintain an inventory of servers
- Scan for vulnerabilities
- Protect co-located servers from each other
  - E.g., use host-based firewalls or AWS security groups
- Remote access to Level 4 information must be limited to authorized employees
- Properly dispose of confidential information when it is no longer needed

# Requirements for Vendors

**These cover relationships with vendors who work with University confidential information.**

- Individual contracts are needed for vendors that deal with University confidential information
- Contracts must include OGC-approved language on protection requirements
- A University security officer must review security programs of vendors dealing with Level 4 information

# “How-To” Guidance

**Specific “how-to” guidance and instructions are provided for each of the policy requirements, such as:**

- Specific configuration and operations guides for Apple iOS and Android smartphones or tablets
- The reporting process for lost or compromised devices

# University Confidentiality Agreement

**Harvard employees must annually acknowledge the University Confidentiality Agreement.**

- Accessed through PeopleSoft under the Personal Information section
- Annual reminders are also emailed to all employees
- Acknowledges that you understand the security policy and good security practices
- Confirms that you will only access information that you need for your job, and that you will not otherwise use or disclose University confidential information

# **University Policy** on Access to Electronic Information

# University Policy on Access to Electronic Information

- University-wide mandatory policy on who can access electronic information relating to someone else *without their permission*
- Covers information created by an individual or information about the activities of an individual (e.g. email, files, and activity logs)
- Summary: Very few people at Harvard can authorize such access
- Applies to electronic information relating to faculty, students, and staff
- See:

http://provost.harvard.edu/files/provost/files/policy_on_access_to_electronic_information.pdf

# Policy on Access to Electronic Information: Principles

- Access should occur only for a legitimate and important University purpose
- Access should be authorized by an appropriate and accountable person
- In general, notice should be given when user electronic information will be or has been accessed
- Access should be limited to the user electronic information needed to accomplish the purpose
- Sufficient records should be kept to enable appropriate review of compliance with this policy
- Access should be subject to ongoing, independent oversight by a committee that includes faculty representation

# Authorization of Access

**Access to electronic information about faculty, students, or staff may only be authorized by the following parties.**

- **Faculty:** If the user is a faculty member or other holder of an academic appointment at Harvard, the dean of the relevant Faculty must authorize access.
- **Students:** If the user is a student, the School-level dean or the dean's designee must authorize access.
- **Staff:** If the user is an employee other than a faculty member:
  1. The human resources officer or his/her designee for the relevant School or administrative unit must authorize access in business continuity cases; and
  2. The dean of the relevant Faculty or the senior administrator of the relevant unit if not a Faculty, or their designees, must authorize access in investigative or other cases

# Exceptions to Authorization of Access

- Routine access by IT personnel
- Includes IT security investigations, if proper process followed
- The person in question consents to access
- Related to health and/or safety, if requested by OGC or reported to OGC
- Related to litigation, legal processes, or law enforcement investigations, if requested by OGC

# What Access Policies Mean for IAM

- No non-IAM disclosure of any logs that show user activities (e.g. authentication system actions) unless one of the following apply:
  - The person in question consents to access
  - Related to health and/or safety — but must be requested by OGC or reported to OGC afterward
  - Requested by an approved person
  - Requested by the IT Security Office following the process they have developed
- Report anyone else who asks for this information to Jane, Tim, or Jason

# **IAM Policy** on Security and Privacy

# IAM Policy: Overview

- General policies for HUIT IAM can be found at http://iam.harvard.edu/resources/iam-policies-standards
- Covers people (not processes or devices)
- Covers non-anonymous identifiers (not self-assigned XIDs)
- Does not include requirements for systems protected by HUIT IAM services (these are already covered by the University security policy)
- Assumes both the University information security policy and the University policy on access to electronic information

# IAM Policy: Key Sections

- **Identification**
  Identifying individuals
- **Information Access Control**
  Access to IAM-managed information
- **Authentication Services**
  The authentication services themselves
- **Privacy**
  Privacy-related policies
- **System Access Control**
  Administrative access to IAM systems
- **Operations Management**
  Managing IAM services
- **Policy Exceptions and Maintenance**
  Exceptions to and maintenance of the policies

# IAM Policy: Identification (1 of 2)

- **Password Strength**
  IAM systems that manage passwords must meet University requirements for password strength
- **HUID Eligibility and Assignment**
  A unique HUID is assigned to qualified individuals
- **UUID Eligibility and Assignment**
  A unique UUID is assigned to anyone who has been assigned another HUIT IAM identifier (e.g. HUID or XID)
- **HarvardKey Eligibility**
  Most HUID holders are eligible to claim a HarvardKey

# IAM Policy: Identification (2 of 2)

- **NetID Eligibility**
  University NetIDs (Active Directory IDs) shall be assigned to HarvardKey holders
- **Identity Proofing**
  Be able to understand how sure we are that a person is who we think they are
- **Identifier Management**
  Uniquely assign identifiers, first collecting at least a minimum set of information; maintain and update this information indefinitely
- **User Enrollment**
  Establish processes to ensure that an ID is assigned to the correct person

# IAM Policy: Information Access Control

- **Require Business Need**
  IAM-maintained information may only be supplied in cases of a business need
- **Review Access**
  Periodically review who has access to IAM-maintained information
- **No Other Use**
  Users must disclose what they are using protected information for, and not use it for anything else
- **No Unauthorized Forwarding**
  Users must agree to not forward protected information
- **OGC Vendor Contract Review**
  Approval from the University OCG of any contract must take place before IAM-maintained information is supplied to a vendor

# IAM Policy: Authentication Services

- **Multiple Services**
  IAM runs multiple authentication services: HarvardKey, PIN2, CAS, Shibboleth IdP, Duo, etc.
- **Authentication Security**
  Authentication services must be secure
- **Multifactor Authentication**
  IAM shall offer an option for multifactor authentication (“two-step verification”)
- **Authentication Logging**
  Authentication-related activities shall be logged

# IAM Policy: Privacy

- **Authentication Log Protection**
  Logs of authentication events shall be protected using multifactor authentication and protected as Level 4 information
- **Authentication Log Retention**
  Logs shall be only retained for a defined length of time
- **Log Access**
  Access to logs shall be restricted as per University Policy on Access to Electronic Information
- **Information Display Control Fields**
  IAM databases shall include fields used to control what information fields are included in directories

# IAM Policy: System Access Control

- **Administrative User Access Management**
  Only people with a current business need are allowed administrative access to IAM systems containing confidential information

# IAM Policy: Operations Management

- **Documented Operating Procedures**
  IAM shall develop operation procedures documents
- **Segregation of Duties**
  Duties of individuals shall be separated as necessary to prevent malevolent activity without collusion
- **Separation of (Operations, Test, and Development) Environments**
  Control access to different environments; keep enough state to support rollback; differently manage production and non-production environments

# IAM Policy Exceptions and Maintenance

**Policies and standards — exceptions**

- Requests for exceptions must be in writing and evaluated by Jane, who will maintain a list of such requests
- In case of a health and/or safety issue, it's OK to override without permission — but report to Jane ASAP

**Policies and standards — maintenance**

- Policies will be reviewed periodically and after incidents
- Jane is in charge of the review process
- Policies will be updated when required

# Summary

# Security & Privacy Policies: Summary

- Protect University confidential information and the computers on which it is accessed, processed, or stored
- Only access the information and systems you must use to do your job
  - Information only distributed when authorized
  - Careful process for ongoing feeds/access
  - Specific authorization required for non-ongoing cases
  - Heath and safety can be special exceptions

# Questions? Comments?

# Thank you!


HARVARD UNIVERSITY
Information Technology