Information Security Quick Reference Guide

HARVARD BUSINESS SCHOOL

CLASSIFICATION				
L1 Information intended and released for public use.	**L2** Information that may be shared only within the Harvard community.	**L3** Confidential and sensitive information, intended only for those with a "business need to know."	**L4** High-risk information that requires strict controls.	**L5** Extremely sensitive information requiring specific controls and isolation from the network.
The University intentionally provides this information to the public.	The University chooses to keep this information private, but its disclosure would not cause material harm.	Disclosure of this information beyond intended recipients might cause material harm to individuals or the University.	Disclosure of this information beyond specified recipients would likely cause serious harm to individuals or the University.	Disclosure of this information could cause criminal liability; loss of insurability or employability; or severe social, psychological, reputational, financial, or other harm to an individual or group.
Examples • Published research • Course catalogs • Published faculty and staff information • Student directory information* • Basic emergency response plans (life safety) • University-wide policies • Harvard publications • Press releases • Published marketing materials • Regulatory and legal filings • Published annual reports • Code contributed to Open Source • Released patents • Plans of public spaces *Directory information about students who have requested FERPA blocks must be classified and handled as L3, at minimum.	**Examples** • Department policies and procedures • Employee web/intranet portals • Harvard training materials • Pre-release articles • Drafts of research papers • Work papers • Patent applications • Grant applications • Non-public building plans or layouts (excluding L3 or L4 items) • Information about physical plant (excluding L3 or L4 items)	**Examples** • Non-directory student information • Non-published faculty and staff information • Information protected under FERPA, in general • HUID tied to an individual • Personnel records** • Donor information (excluding L4 data points or special handling) • Non-public legal work and litigation information • Budget /financial transactions information • Non-public financial statements • Information specified as confidential by vendor contracts and NDAs • Information specified as confidential by Data Use Agreements • General security findings or reports (e.g. SSAE16) • Most Harvard source code • Non-security technical specifications/architecture schema • Library/museum object valuations • IRB records	**Examples** • Passwords and PINs • System credentials • Private encryption keys • Government issued identifiers (e.g. Social Security Number, Passport number, driver's license) • Individually identifiable financial account information (e.g. bank account, credit or debit card numbers) • Individually identifiable health or medical information*** • Individually identifiable research data • Details of significant security exposures at Harvard (e.g. vulnerability assessment and penetration test results) • Security system procedures and architectures • Trade secrets • Systems managing critical Operational Technology	**Examples** • Research data classified as Level 5 by the IRB • Information or research under a contract stipulating specific security controls beyond L4

Know the policy: The full policy and additional resources are at http://policy.security.harvard.edu

Seek assistance: If you have questions or concerns about the policy, or if you know of items that are out of compliance, please contact your manager or your School Security Officer.

Use good judgment: The lists above are only examples, not definitive classifications.

**Employees have the right to discuss terms and conditions of their own employment, including salary and benefits, with each other or with third parties.

*** Harvard units or programs that qualify as "covered entities" under the Health Insurance Portability and Accountability Act (HIPAA) must comply with HIPAA's data security rules.

Revision Date: 09/20/2017

Information Security Quick Reference

HARVARD BUSINESS SCHOOL

General Safeguards for all non-public levels:

- Share only with those authorized to have access
- Use caution when discussing in public places
- Secure paper-based information in locked desk/office/cabinet when not in use
- Report possible or actual loss immediately to your supervisor or Security Officer

L5 handling and disposal requirements are specific to each project. Consult with HBS Information Security on all L5 implementations.

Never share passwords/PINS with anyone or carry them with the device they unlock!

HANDLING			
Activity by Data Level	**L2**	**L3**	**L4**
Printing	Do not leave unattended on copiers/printers	Do not leave unattended on copiers/printers	L4 data must be immediately retrieved, and secured in a locked cabinet or drawer when not in use.
Mailing paper-based info	Put in a closed mailing envelope/box and send via Interoffice or US mail.	Put in a sealed envelope/box and send via interoffice or US mail.	Put in a sealed envelope/box and send via FedEx/UPS/USPS mail with tracking/delivery confirmation where feasible.
Storing electronic files on work or personal computer (including portable devices)	Computer must meet Harvard security requirements, including device password, anti-virus, current patches, encryption, and remote wiping.	Computer must meet Harvard security requirements, including device password, anti-virus, current patches, encryption, and remote wiping.	Never copy/store L4 data onto your work or personal computer. Data should remain within the secure managed system or encrypted external storage media.
Storing files on external portable storage media	No specific requirements	USB stick, CD/DVD, back-up tape, etc. must be encrypted and password protected.	USB stick, CD/DVD, back-up tape, etc. must be encrypted and password protected.
Sharing files with authorized individuals	Use approved collaboration tools and share with specific individuals, not anonymous or guest links.	Use approved collaboration tools and share with specific individuals, not anonymous or guest links.	Use only security-cleared L4 SharePoint or network locations to share files with named individuals.
Sending data/files to authorized individuals	Use email and send only to those authorized to view it.	Encrypt when transmitting data both internally and externally: Use a School-supported Secure File Transfer method (e.g. OneDrive, Accellion). On website forms, use HTTPS.	Encrypt when transmitting data both internally and externally: Use a School-supported Secure File Transfer method (e.g. L4 SharePoint, Accellion). On website forms, use HTTPS.
Engaging vendors to store/process data	No specific requirements	Engage Information Security to determine if a security review should be completed and include Harvard's data security addendum in the vendor/hosting agreement.	Engage Information Security for a security review and include Harvard's data security addendum in the vendor/hosting agreement.
Deleting electronic files	Use standard Delete/"X" commands and empty trash bin	Use standard Delete/"X" commands and empty trash bin	Use a secure overwrite or removal tool (e.g. Spirion / Identity Finder)

How to dispose/recycle paper:

L1 Data only for single-stream recycling

L2-L4 Data to be shredded and recycled

How to dispose of devices and/or prepare them for recycling or upgrade:

Enter incorrect passwords until device reformats itself or select Reset in Settings

Shred CD/DVD at provided shredders or contact local IT Support

Remove all sensitive data, and wipe drive yourself. Contact TSS for suggestions on individual devices

Publication Date: 11/3/2017