Data Classification - Administrative Examples

See also: **Guides**

Classification Levels

L1 - Information intended and released for public use.

The University intentionally provides this information to the public.

L1 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.

L2 - Low Risk Confidential Information that may be shared only within the Harvard community.

The University chooses to keep this information private, but its disclosure would not cause material harm.

L2 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)
- Non-sensitive administrative survey data

L3 - Medium Risk Confidential

Information intended only for those with a “business need to know.”

Disclosure of this information beyond intended recipients might cause material harm to individuals or the University.

L3 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
- Security findings or reports (e.g. SSAE16, vulnerability assessment and penetration test results)
- Most Harvard source code
- Non-security technical specifications/architecture schema
- Library/museum object valuations
- IRB records
- Sensitive administrative survey data, such as performance reviews or course feedback, especially if free text response is permitted

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

L4 - High Risk Confidential Information that requires strict controls.

Disclosure of this information beyond specified recipients would likely cause serious harm to individuals or the University.

L4 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***
- Security system procedures and architectures
- Trade secrets
- Systems managing critical Operational Technology

*** *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.*

L5 - Reserved for **Research Data** only, as determined by IRB or Data Use Agreement.

Data that could place the subject at severe risk of harm or data with contractual requirements for exceptional security measures

L5 Examples

- Research data classified as Level 5 by the IRB
- Information or research under a contract stipulating specific security controls beyond L4

Using the Classification

Know the policy

The full policy and additional resources are at the **Security Policy website**.

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.

Print the current handout for reference

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

L2 - L4 Handling

Printing

- **L2**
  - Do not leave unattended on copiers/printers
- **L3**
  - Do not leave unattended on copiers/printers
- **L4**
  - Use badge retrieval for print jobs on an approved Level 4 printer.

Mailing paper-based info

- **L2**
  - Put in a closed mailing envelope/box and send via Interoffice or US mail.
- **L3**
  - Put in a sealed envelope/box and send via Interoffice or US mail.
- **L4**
  - 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

Storing files on external portable storage media

Sharing data/files with authorized individuals

Sending data/files to authorized individuals

Engaging vendors to store/process data

Secure disposal

How to delete electronic files

- L1-L3: Use standard Delete/“X” commands and empty trash bin
- L4: Use a secure overwrite or removal tool (e.g. Spirion/Identity Finder)

How to dispose/recycle paper

- L1 Only: Use single-stream/commingled recycling program
- L2-L4: Paper must be put through a cross-cut shredder prior to recycling

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

- Contact local IT Support for pick-up or drop-off: they will remove data and recycle

- Shred CD/DVD at provided shredders or contact local IT Support
- Enter incorrect passwords until device reformats itself or select Reset in Settings

---