|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CLASSIFICATION | | | | |
| **L1** Information intended and  released for public use. | **L2** Information that may be  shared only within the project  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 company intentionally provides this information to the public. | The company 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 company. | Disclosure of this information beyond specified recipients would likely cause serious harm to individuals or the copmany. | 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. |
| * Published articles in Live Magazine/Press releases * Currently offered treatments/products * Division information, organizational structure * List of collaborators * Published annual reports * Currently recruiting clinical trials * Commercial model, values * Statistics of employees and collaborators | * Department policies and procedures * Drafts of research papers * Work papers * Non-public building plans or layouts (excluding L3 or L4 items) | * Intranet website portal * Guidelines * Emails | * Research data * Personal data * Surveys * Locked mail | Outside of network, not accessible from Internet, stored in a safe physical isolation with restricted access |

**General Safeguards for all non-public levels:**

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

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

* 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

|  |  |  |  |
| --- | --- | --- | --- |
| HANDLING | | | |
| **Activity by Data Level** | **L2** | **L3** | **L4** |
| **Printing** | Do not leave unattended on copiers/printers | Do not leave unattended on copiers/printers | Send to printer using stored/locked job. Enter passcode at machine to print (see security.harvard.edu for instructions). |
| **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, antivirus, 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 | Ensure vendor/hosting agreement includes Harvard’s data security addendum. | 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. Identity Finder) |



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

L2-L4 Data to be shredded and recycled

L1 Data only for single-stream recycling

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

**How to dispose/recycle paper:**