UNIVERSITY OF CALIFORNIA

UCOP
ITS
Systemwide IT Policy

UC Institutional Information Disposal Standard

Revision History

Date:	By:	Contact Information:	Description:
05/15/18	Robert Smith	robert.smith@ucop.edu	Initial issue of the Standard. Approved by the CISOs for consideration by ITLC and shared governance. Interim until approved by ITLC.
5/24/18	Robert Smith	robert.smith@ucop.edu	Minor administrative updates correcting page numbering, typos and the ordering of Table 1 – in order alphabetically.

Contents

1 Background and Purpose

The primary purpose of this Standard is to ensure that electronically stored Institutional Information is not unintentionally released or accessed by unauthorized parties.

This Standard outlines the actions required of Workforce Members and Proprietors who must meet legal, regulatory and other obligations when disposing of electronic Institutional Information, electronic media containing Institutional Information or IT Resources containing Institutional Information. Laws, regulations, contracts, research agreements, UC's Record Management Policies and UC's Record Retention Schedule all inform decisions made to ensure the safe disposal of Institutional Information. Institutional Information classified at Protection Level 3 or higher requires that Workforce Members use special care for Sanitization (see definitions below).

The disposal of Institutional Information can involve data stored in multiple ways and in various forms. This Standard sets requirements for Workforce Members disposing of data stored on both physical and logical media (see definitions below).

Workforce Members should also note that sometimes Institutional Information must be held longer than the time outlined by the UC retention schedule. Records holds and business needs can prevent or delay the Sanitizing of specific records because the records may be needed as evidence in an investigation, for foreseeable or ongoing litigation, in an ongoing audit or for other special circumstances, such as a Public Records Act Requests. Workforce Members must work with the Location Records Manager in these cases.

UC has implemented other policies and standards regarding privacy and information security. This Standard complements (and should be interpreted consistently with) all other relevant policies and standards.

2 Scope

This Standard applies to all Workforce Members who, during the course of their jobs at the University of California, dispose of IT Resources (e.g., computers or electronic media) that contain Institutional Information.

3 Definitions

Clear: A disposal process using software or hardware products to overwrite storage space on media. Clear may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table), but also all addressable locations. Clear also protects against keyboard based or simple non-invasive data recovery techniques.

Cryptographic Erase (CE): A disposal process that safely destroys all copies of the decryption key. If all data is adequately encrypted, then once the decryption key is removed, the Institutional Information is not recoverable.

Delete: A disposal process that removes the ability to access the respective file, record or data in the operating system or application.

Note: Deleted information is not Sanitized from the IT Resource (e.g., operating system, file storage, application). Deleting data does not necessarily eliminate the possibility of recovering all or part of the original data. For example, dragging files to the Recycle Bin or Trash and emptying it does not eliminate the possibility of recovery. Using the rm command in Linux performs a delete function similar to moving files to recycle/trash. The possibility of recovery therefore still exists.

Degauss: A disposal process that 1) erases data by using a formalized technique that alters the magnetic storage of information in such a way that it cannot be accessed or recovered or 2) reduces the magnetic flux to virtual zero by applying a reverse magnetizing field.

Note: Some hard drives and magnetic tape media manufactured since 2010 cannot be reliably Degaussed. Workforce Members must verify that equipment is capable of properly Degaussing the media.

Destroy: A disposal process that makes media not usable again and renders Institutional Information irretrievable even using specialized recovery techniques. It also results in the subsequent inability to use the media for storage of data (e.g., shred, disintegrate, pulverize or incinerate by burning the device in a licensed incinerator).

L**ogical Delete**: A disposal process of non-destructive deletions of data, records or information within applications. The information is marked as "deleted" and may not be exposed to users, but some data may still be recoverable.

Logical Media: A set of data independent of the physical media on which it is recorded.

Examples include: cloud storage (e.g., Box, Google Drive/Sync/Backup/FileSteam, Onedrive, Dropbox, Amazon S3, Amazon Drive, RackSpace); devices formatted for Windows lettered drives (NTFS or FAT file systems); Macintosh HFS+ or APFS; or Linux Ext2/3/4. Data may be stored in files or in applications such as databases, document management systems, human resource management systems and formatting of physical media, etc.

Physical Media: The tangible, physical materials or devices that are used to store or transmit Institutional Information. They can be touched and felt, having physical properties such as weight and color.

Examples of physical media include: hard drives, rewritable optical media (CDs and DVDs), USB drives, tapes and tape cartridges, solid state drives, magnetic tape and optical media (e.g., CDs, DVDs, optical disks).

Purge: A disposal process that makes the media reusable but makes accessing the Institutional Information infeasible. This applies to physical or logical techniques that render Institutional Information recovery unachievable. Purge protects against laboratory attacks. Executing the secure erase firmware command on a disk drive, Cryptographic Erase and Degaussing are acceptable methods of purging.

Sanitization: A disposal process that renders Institutional Information on physical or logical media inaccessible at a certain level of effort. Various Sanitizing actions require

increasing levels of effort to recover information, including Destroy, which makes retrieval fully impossible. Actions taken to Sanitize media include: Clear, Purge, Cryptographic Erase and Destroy. Note that Delete and Logical Delete are not Sanitization techniques.

4 Requirements

Some methods of data destruction are more complicated, time-consuming or resource intensive than others. Workforce Members must select a method of data destruction based on the Protection Level classification of the Institutional Information to be destroyed and/or the potential harm that would result from data recovery and disclosure. For very low risk Institutional Information, Protection Level 1 (P1), this may mean simply Deleting electronic files. However, these types of destruction methods can be undone by a determined and motivated individual, which makes these methods inappropriate for more sensitive data. When handling Institutional Information classified at Protection Level 3 or higher, Workforce Members may need to employ stronger methods of disposal at a more granular level to ensure that data is truly irretrievable.

Sanitization is required to prevent unauthorized access to and properly dispose of Institutional Information.

Institutional Information may need to be Sanitized because:

- It is required by law/regulation or in other approved use cases.
- Institutional Information is at the end of its retention schedule.
- Electronic media is reused or retired.
- IT Resources are sent for repair or replacement.
- IT Resources are repurposed or are retired.

4.1 Appropriate Sanitization Methods

The table below summarizes appropriate Sanitization methods based on Protection Level. A more stringent sanitization method can be used.

Table 1

Institutional Information Disposal Overview

	Institutional Information Protection Level			
Device/Data Location	**P1**	**P2**	**P3**	**P4**

	Institutional Information Protection Level			
Device/Data Location	**P1**	**P2**	**P3**	**P4**
Hard disk drives (HDD) - portable or embedded/internal	Delete	Clear	Purge	Purge Destroy
Logical storage[1]	Logical Delete	Logical Delete	Cryptographic Erase[2]	Cryptographic Erase
Optical disk - read only (CD-ROM, DVR-ROM, etc.)	Destroy	Destroy	Destroy	Destroy
Optical disk - read/write (CD-R/W, DVD-R/W, etc.)	Delete	Clear	Destroy	Destroy
Other embedded storage devices[3]	Delete	Clear	Purge	Purge
Portable media - electronic (thumb drive, USB stick)	Delete	Clear	Purge	Destroy

[1] Logical storage is principally storage used within or by applications, such as databases, content management systems, cloud storage services, etc. An IT Workforce Member will be required to perform Institutional Information destruction on logical storage.

[2] Most databases have the ability to perform field (column) encryption or row-level encryption. Alternatively, entire tables can be encrypted. Once encrypted, destroying the key completes the Cryptographic Erasure.

[3] Consult the manufacturer and industry recommendations. Use a risk-based approach that considers the Institutional Information disclosure risks and device capabilities. Review with the Privacy Officer and CISO to make determinations that fall outside of this Standard or when the recommended technique cannot be confidently used.

	Institutional Information Protection Level			
Device/Data Location	**P1**	**P2**	**P3**	**P4**
Portable magnetic media – tape	Delete	Degauss	Destroy	Destroy
Solid state drives (SSD)[4]	Delete	Cryptographic Erase	Cryptographic Erase	Cryptographic Erase

4.2 Institutional Information Disposal Decisions

Workforce Members, before Sanitizing or Destroying media or IT Resources containing Institutional Information, must verify that:

- There are no record holds affecting the Institutional Information.
- The Sanitization process follows the UC retention schedule: https://recordsretention.ucop.edu/
- The Sanitization method is appropriate.

Workforce Members disposing of media or storage containing Institutional Information whose Protection Level classification cannot be determined must dispose of the media as if it contained information classified at Protection Level 4.

4.3 Cryptographic Erase

For a Cryptographic Erase[5] to be used, the following requirements must be met and documented:

- The IT Workforce Member must verify that all data is adequately encrypted.
- The location of all decryption keys must be known and documented.
- An action that safely destroys all copies of the key must be available.
- The cryptographic algorithm employed must meet minimum standards, as defined by NIST in Annex A: Approved Security Functions for FIPS 140-2, *Security Requirements for Cryptographic Modules* and NIST SP 800-131A Rev.

[4] Consult the manufacturer and industry recommendations. Consider secure erase functions when acquiring solid state drives. Some drives may not have a method to securely Purge Institutional Information.

[5] NIST Special Publication 800-88 Rev 1 - Guidelines for Media Sanitization, contains guidance on when to use Cryptographic Erase. See Section 2.6 - Use of Cryptography and Cryptographic Erase.

1 *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths.*

4.4 Logical Storage

IT Workforce Members administering Logical storage must:

- Use Logical Delete so the Institutional Information is no longer referenced and will not show in searches or transactions when the database is used.
- Use Cryptographic Erase so it is no longer feasible to access the Institutional Information when the database or other application is retired.
- Include removal of version histories as appropriate when executing Logical Delete and Cryptographic Erase processes.

4.5 Media Reuse

Workforce Members reusing media must ensure that required Sanitization was completed before the media is reused.

4.6 Degaussing

IT Workforce Members Degaussing magnetic tape media must use a CISO-approved method to Purge the Institutional Information.

Note: Some Degaussing equipment is not suitable for some media types. Consult the manufacturer's Degaussing recommendations. It may be necessary to have the media Destroyed or to have a Supplier with the proper equipment Degauss the media.

4.7 Physical Destruction

Workforce Members Destroying media must use a CISO-approved method to render the media unusable and the Institutional Information irretrievable.

4.8 Verification

Workforce Members performing disposal of Institutional Information classified at Protection Level 3 or higher must record the disposal, the Sanitization method and the verification process.

5 References

Department of Education - “Best Practices for Data Destruction”: https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Best%20Practices%20for%20Data%20Destruction%20%282014-05-06%29%20%5BFinal%5D_0.pdf

NIST FIPS PUB 140-2, Annex A - *Security Requirements for Cryptographic Modules:* https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402annexa.pdf

NIST SP 800-88 r1 - Guidelines for Media Sanitization: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

NIST SP 800-131A Rev. 1 Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths: https://csrc.nist.gov/publications/detail/sp/800-131a/rev-1/final

Records Retention Schedule: https://recordsretention.ucop.edu/

Records Management Committee, showing each campus records management coordinator: http://www.ucop.edu/information-technology-services/initiatives/records-management/records-management-committee.html

6 Standards

UC Health Insurance Portability and Accountability Act Procedures - http://www.ucop.edu/ethics-compliance-audit-services/compliance/hipaa/#2

7 UC Policy

UC Business and Finance Bulletin IS-3 - Electronic Information Security

UC Business and Finance Bulletin RMP-1 - University Records Management Program

UC Business and Finance Bulletin RMP-2 - Records Retention and Disposition: Principles, Processes and Guidelines

8 Appendix A – Other Supporting Roles

These roles can or do play an important part in the Institutional Information lifecycle.

Table 2

Responsibilities for Institutional Information Disposal by Role

IT Workforce Member	Verify the appropriate timing of Sanitization and then execute Sanitization.
Location Counsel	Issue guidance, answer questions and provide instructions related to legal issues and record holds impacting Institutional Information.
Public Records Act (PRA) Manager	Review Sanitization plans and requests that are outside the retention schedule or when public records requests are pending.
Proprietor	Set retention schedule requirements. Approve Sanitization plans.
Records Manager	Issue guidance, answer questions and provide instructions related to records management and the lifecycle of Institutional Information.
Unit Information Security Lead (UISL)	Support Workforce Members and Proprietors in planning and executing Sanitization. Liaison with Records Manager, CISO, Location Counsel and PRA Manager as needed.
Workforce Member	Consult with or utilize other roles as needed, particularly when disposing of Institutional Information classified at Protection Level 3 or higher. Verify the appropriate timing of Sanitization and then execute Sanitization.