THE OHIO STATE UNIVERSITY
UNIVERSITY LIBRARIES

Secure Destruction of S3 & S4 Data Requirements

According to OSU Information Security Control Requirements (ISCR), all OSU official records, copies and data classified as S3 and S4 security level must be securely destroyed.

When selecting a university-approved shredding service, Records Management strongly recommends choosing a NAID-certified vendor for secure destruction of physical records. NAID-certified destruction vendors have been certified to various privacy and security standards, have background checked employees, and are audited on their processes.

All electronic records and data must be destroyed by University Surplus.

Before secure destruction of official records or data, in any media format, may occur, an OSU Certificate of Destruction (CRD) must be submitted to OSU Records Management for approval, at least 1 week prior to the requested destruction date.

S3 & S4 Paper Records:

ISCR DAT3.2.1 requires secure destruction of paper records that contain S3 or S4 data:

Organizations must properly dispose of documents containing S3 (private) and S4 (restricted) institutional data. Documents must be disposed by physical destruction (e.g., shredding). Organizations must shred documents by using:

A. an organizationally-owned shredder which must be able to perform cross-cut shredding; or
B. a university-approved shredding service.

Note: Shredding services must provide documentation as evidence of document destruction for S4 (restricted) institutional data. [*Business units may submit the vendor's destruction documentation to OSU Records Management for long-term retention*.]

The size of the shredded material should be small enough to provide reasonable assurance that the data cannot be reconstructed.

S3 & S4 Electronic Media Records and Data:

ISCR IT15.2.1 requires the sanitation of storage media prior to disposal

Organizations must ensure all storage media is sanitized prior to disposal, repurposing, or release from university control. Sanitization methods depend upon the type of storage media:

A. magnetic media must be cleared (e.g., overwritten at least once) prior to disposal, repurposing, or release;
B. storage drives must be cleared (e.g., overwritten at least once) prior to disposal, repurposing, or release;

C. flash memory storage must be cleared (e.g., overwritten at least once) prior to disposal, repurposing, or release; and
D. optical media:
    1. read-only (e.g., CD-ROM, DVD-ROM) or write-once (e.g., CD-R, DVD-R) optical media cannot be reused and must be physically destroyed (e.g., shredded or incinerated); and
    2. rewritable (e.g., CD-RW, DVD-RW) optical media must be cleared (overwritten at least once) prior to repurposing or release.

For storage media that cannot be reliably used (e.g., media that is unreadable, unwritable, or otherwise unverifiable), the media must be physically destroyed (e.g., shredded or incinerated).

Storage media disposal must be performed and documented by a university-approved storage media destruction and disposal service.

ISCR IT15.2.2 requires secure destruction of electronic media that contains S3 or S4 data:

Organizations must ensure all storage media that has been used to store institutional data is securely sanitized prior to disposal, release from university control or repurposing. Secure sanitization methods depend upon the type of storage media:

A. magnetic media must be destroyed (e.g., degaussed or shredded) prior to disposal or release; magnetic media must be cleared (e.g., overwritten at least once) prior to repurposing;
B. storage drives must be destroyed (e.g., degaussed or shredded) prior to disposal or release; storage drives must be cleared (e.g., overwritten at least once) prior to repurposing;
C. flash memory storage devices must be physically destroyed (e.g., shredded or incinerated) prior to disposal or release; flash memory storage devices must be cleared (e.g., overwritten at least once) prior to repurposing; and
    a. Note: Flash memory that is integrated into an information system and cannot be removed for destruction may be cleared (e.g., overwritten at least once), if the organization can validate the flash memory was previously encrypted.
D. optical media (all types) and unencrypted solid state storage cannot be reused and must be physically destroyed (e.g., shredded or incinerated).

Organizations must review and approve storage media to be sanitized to ensure compliance with university records retention schedules.

Organizations must track and document actions associated with storage media disposal or release, if required by regulation.

For storage media that is integrated into an information system and cannot be reliably used (e.g., storage media that is unreadable, unwritable, or otherwise unverifiable), the information systems must be physically destroyed (e.g., shredded or incinerated).

Restricted storage media destruction and disposal must be performed and documented by a university-approved storage media destruction and disposal service:

- University Surplus