Media Disposal Procedure

1 Purpose

Workday needs to ensure that the data contained on media such as hard drives is not exposed to an actual or potential security breach. This means that all media must be either sanitized or destroyed, depending on the type of device, the device's ultimate destination, and who will be performing the required procedure. The following sections describe the procedures that should be followed to properly sanitize or destroy media. The answers to the following three questions will help you determine which procedure to perform.

- Will the media remain within Workday or not?
- For what type of device is the media being disposed of?
- Who will perform the disposal?

2 Scope

The Media Disposal Procedure describes all possible media disposal scenarios, when each scenario applies, what happens, and who performs the required tasks.

3 Media Destruction Procedures

The following sections describe the procedures that should be followed to properly dispose of all electronic media.

3.1 If the Media Will be Reused Within Workday…

If the media will be reused elsewhere within Workday, depending on the type of media, perform the steps in one of the following sections.

3.1.1 Storage Device

If the media is a storage device such as a hard drive, then, depending on who is doing the sanitization, that person should follow the procedure described in one of the following bullets:

- **Workday Cloud Operations**: If a member of Workday Cloud Operations staff will be performing the procedure, then that person must sanitize the hard drives using a Workday-approved disk utility or appliance that uses a low-level format and performs the sanitization three times to ensure that the drive is sufficiently clean.
- **Outside vendor**: If a Workday-approved vendor will be performing the disk sanitization, then the procedure must be supervised by a Workday Cloud Operations staff member, and the vendor must create a certificate of sanitization and provide it to Workday.

3.1.2 Systems and Network Appliances

If the media is a systems or network appliance, then, depending on the appliance, the procedure described in one of the following bullets applies.

- **NAME OF APPLIANCE REDACTED**: If the systems infrastructure team will be sanitizing a NAME OF APPLIANCE REDACTED, perform the following steps:
  1. Perform the commands provided by NAME OF COMPANY REDACTED to clean the selected drives. Note the following considerations:
     - This process should take place on Workday property or within the data center (DC).
     - The drives should not be removed from Workday property until they are wiped.
  2. Verify that the relevant logs record that the drives have been wiped clean.
  3. Capture a screenshot of the results showing the drives are clean and attach it to the destruction JIRA issue for auditing purposes.
- NAME OF APPLIANCE REDACTED: If the media to be repurposed is NAME OF APPLIANCE REDACTED, then its internal hard drive must be removed and destroyed. For more information, see Section 3.2.1 Storage Device.

Note: If the media to be repurposed is a networking device—including but not limited to switches, routers, firewalls, load balancers, and security appliances that do not have physically installed local media such as a hard drive—then there are no installed parts that need to be removed or destroyed. If the media to be repurposed is to be removed from an existing data center cage, then a factory reset of the device should be performed. This reset can be performed locally or remotely by anyone with sufficient credentials.

3.2 If the Media Will not be Reused by Workday…

If the media will not be reused by Workday, then, depending on the type of media, perform the steps in one of the following sections.

3.2.1 Storage Device

If the media is a storage device such as a hard drive that is not to be reused elsewhere within Workday, then it must be physically destroyed. To do this, perform the following steps.

1. Write the server's serial number and JIRA issue number (where the drive came from) on a sticker and place it on the hard drive. LINK REDACTED
2. Record the hard drive serial number on the corresponding On-Site Drive Shred spreadsheet (under current quarter): LINK REDACTED
3. Put the hard drive in a locked hard drive container to wait for the next on-site shredding event. Note the following:

   - Each quarter, Cloud Operations MUST review the quantity of hard drives waiting to be shredded.
   - Cloud Operations should schedule shredding of hard drives at least twice a year.
   - Additional shredding events should be scheduled as needed.

4. Before scheduling the shred service, you must match the hard drives to the On-Site Drive Shred spreadsheet to ensure accuracy and that the counts match.
5. Capture the hard disk serial numbers in the corresponding DC OPS Quarterly Hard Disk Shred JIRA issue with the JIRA issue number also referenced on the corresponding On-Site Drive Shred spreadsheet.
6. Assign the DC OPS Quarterly Hard Drive Shred JIRA issue to the DC Asset Manager for approval and service processing. The Asset Manager will complete a recycle pickup request through the vendor online portal.
7. When the vendor arrives on-site with the shredder truck, per official policy, you must perform the following steps:

    a) Walk the container to the vendor truck.
    b) Unlock the container.
    c) Witness the shredding of hard drives.

    When the shred process has finished, the vendor will provide an audit of all hard drives shredded along with a certificate of destruction.

8. Once the hard drive destruction has been completed and a certificate of destruction has been issued, notify the Asset Manager. He or she will update the DC OPS JIRA issue with the destruction date and all reference information.

3.2.2 Systems and Network Appliances

If the media is a systems or network appliance, then, depending on the appliance, the procedure described in one of the following bullets applies:

- **NAME OF APPLIANCE REDACTED**: If the systems infrastructure team will be sanitizing a NAME OF APPLIANCE REDACTED, perform the following steps:

    1. Perform the commands provided by NAME OF COMPANY REDACTED to clean the selected drives. Note the following considerations:

        - This process should take place on Workday property or within the data center (DC).
        - The drives should not be removed from Workday property until they are wiped.

    2. Verify that the relevant logs record that the drives have been wiped clean.
    3. Capture a screenshot of the results showing the drives are clean and attach it to the destruction JIRA issue for auditing purposes.
- **NAME OF APPLIANCE REDACTED**: If the media to be repurposed is a NAME OF APPLIANCE REDACTED, then its internal hard drive must be removed and destroyed. For more information, see Section 3.2.1 Storage Device.

Note: If the media to be repurposed is a networking device—including but not limited to switches, routers, firewalls, load balancers, and security appliances that do not have physically installed local

media such as a hard drive—then there are no installed parts that need to be removed or destroyed. If the media to be repurposed is to be removed from an existing data center cage, then a factory reset of the device should be performed. This reset can be performed locally or remotely by anyone with sufficient credentials.

3.3 If the Media Will be Sent to an Outside Third Party…

If the media to be disposed of will be sent to an outside third party, depending on the type of media, perform the steps in one of the following sections.

3.3.1 Storage Device

Some storage devices (such as hard drives) must be sanitized by an outside vendor. To have a vendor sanitize a hard drive, Workday Cloud Operations must perform the following steps:

1. Open a DC OPS JIRA issue and populate it with the server/device serial number (where the drive came from) and indicate who the drive will be sent to. Note the following:

    - Hard drive sanitization MUST be performed by a Workday-approved vendor and *MUST be conducted on Workday facilities*.
    - When the hard drives are sanitized, the vendor MUST create a certificate of sanitization and provide it to Workday.
    - All work MUST be supervised by a Workday Cloud Operations staff member.

2. When the procedure has finished, attach proof to the DC OPS JIRA issue.
3. Update the JIRA issue with the ship date once the hard drive has been shipped.

3.3.2 Systems and Network Appliances

If the media is a systems or network appliance, then, depending on the appliance, the procedure described in one of the following bullets applies.

- **NAME OF APPLIANCE REDACTED**: If the systems infrastructure team will be sanitizing a NAME OF APPLICANCE REDACTED, perform the following steps:

    1. Perform the commands provided by NAME OF COMPANY REDACTED to clean the selected drives. Note the following considerations:

        - This process should take place on Workday property or within the data center (DC).
        - The drives should not be removed from Workday property until they are wiped.

    2. Verify that the relevant logs record that the drives have been wiped clean.
    3. Capture a screenshot of the results showing the drives are clean and attach it to the destruction JIRA issue for auditing purposes.

- NAME OF APPLIANCE REDACTED: If the media to be repurposed is an NAME OF APPLIANCE REDACTED appliance, then its internal hard drive must be removed and destroyed. For more information, see Section 3.2.1 Storage Device.

Note: If the media to be repurposed is a networking device—including but not limited to switches, routers, firewalls, load balancers, and security appliances that do not have physically installed local media such as a hard drive—then there are no installed parts that need to be removed or destroyed. If the media to be repurposed is to be removed from an existing data center cage, then a factory reset of the device should be performed. This reset can be performed locally or remotely by anyone with sufficient credentials.

4 Roles and Responsibilities

Organization	Responsibility
Cloud Operations	DC Asset Manager
Cloud Operations	DC Engineer
Systems	Systems Engineer
Network	Networking Engineer

5 Definitions

Term	Definition

6 References

The following documents are referenced in the Media Disposal Procedure.

- Media Disposal and Reuse Policy: LINK REDACTED
- On-Site Drive Shred Spreadsheet: LINK REDACTED

7 Revision History

Action	Action Taken By	Version	Date
Standard Created			
Standard Reviewed			
Standard Approved (Last Effective Date)			