Decommissioning Checklist for Enterprises: PCs, Laptops & Other IT Assets

Secure, repeatable IT asset decommissioning processes are critical for regulation compliance, data protection, data retention and audit-ready record keeping. Use this 13-point checklist, along with your organization's internal data protection, retention and security policies, to guide you through the decommissioning process when you are:

- Preparing to return leased equipment to a technology vendor
- Moving technology assets from one department or employee to another for reuse
- Decommissioning devices for resale, recycling or physical destruction—either in-house or through an IT asset disposition (ITAD) vendor
- Otherwise retiring old data processing and storage technologies

This checklist accommodates network- and non-network-connected devices, whether one unit or a thousand. By including data erasure at key points in the process, you will ensure that sensitive data doesn't transfer with previously used hardware, including mobile devices, laptops and desktops, removable media, SSDs and HDDs—and provide record-keeping tips for compliance and auditing purposes.

Software-based data erasure ensures that data is completely unrecoverable on both magnetic and flash-based storage technologies.

Note: For server decommissioning, see our Decommissioning Checklist for Data Centers: Servers, available on our website.

Identify Devices and Schedule Decommissioning Processes

- ☐ **1. Identify and inventory:** Document all equipment to be decommissioned and software licenses associated with each device. You may need to record names of users and departments, as well as the types of information stored on the devices, to fully comply with mandated and internal data protection policies.
- ☐ **2. Determine destination:** Categorize devices by return to manufacturer/lessor, internal reuse, external reuse (e.g., donation or resale), physical destruction/recycling. Note any confidentiality protection requirements.
- ☐ **3. Schedule for decommissioning:** Confirm and communicate decommissioning and replacement dates and procedures. Note that end-of-lease planning, scheduling and communication processes may start several months in advance; confirm all processes with your leasing vendor.

Prepare Devices for Sanitization, Data Retention and Any Necessary Device Replacement

- ☐ **4. Prepare end users:** Prepare users for the scheduled transfer of all necessary files and applications. Set a disconnection date. Plan to fully erase decommissioned devices within one business week (two max) of being taken out of service.
- ☐ **5. Backup required files:** Identify and backup files needed for data retention requirements or subsequent operations.
- ☐ **6. Sanitize network-connected devices:** Take network-connected laptops, PCs, workstations and drives out of production, disable user access and sanitize using enterprise-grade data erasure software as a final step before taking the asset offline. Sanitizing with robust erasure software before removing devices from the network allows you to accelerate decommissioning through automated data erasure processes. Blancco data erasure solutions

allow you to define enterprise- or department-wide customizations—such as sanitizing according to specified erasure standards—and centralized erasure verification and report management.

- ☐ **7.** **Retrieve all non-network devices and disable user access, replacing the device as needed.** Independent devices should also be inventoried and prepped for erasure. Incidentally, non-network devices such as mobile phones and removable media (e.g., flash media such as SD cards, USB sticks and other flash memory storage devices) can also be erased at end-of-life using single data erasure processes or high-volume simultaneous erasure.
- ☐ **8.** **Schedule IT asset erasure within one work week, two at most, from pulling out of use.** This helps prevent inactive, but data-laden, devices from being compromised or forgotten about.
- ☐ **9.** **Provide secure storage:** Ensure security of inactive assets before data erasure has taken place. Work with your legal, IT and operations departments to document and execute security measures taken to ensure physical data protection during storage.

Execute Sanitization Processes by Device Destination

- ☐ **10.** **Sanitize drives according to device type, destination and confidentiality:** Whether sanitized in-house or through an external vendor, ensure that each device undergoes sanitization methods appropriate to that device (using incorrect destruction or erasure methods can leave data behind) and recognized best practice.

  Using enterprise-grade sanitization software, erase loose drives and removable media devices with the required data sanitization algorithm (DoD, NIST Clear or Purge, CESG CPA, HMG Infosec Standard 5, etc.).[1] The algorithm selected should be appropriate to the confidentiality level of the data, hardware requirements, compliance requirements and whether the device will be reused (internally or externally) or destroyed. Blancco-sanitized IT assets will come with digitally signed Certificates of Erasure that record what algorithm was used, any anomalies, the date of erasure and more. These can be centrally managed via the Blancco Management Console for auditing and compliance purposes.

  NOTE: For any assets leaving your facility for sanitization, ensure stringent chain of custody processes are in place from origination to final data destruction. Confirm that you will receive tamper-proof evidence that units have been completely erased.

Why are Blancco Certificates of Erasure So Important?

Blancco Certificates of Erasure:

- ☑ Show that the erasure was done and done properly
- ☑ Are digitally signed and tamper-proof for compliance purposes
- ☑ Are automatically sent to the Blancco Management Console for ease of record keeping and optional "view-only" access
- ☑ Can easily be exported to .XLS, .PDF or .XML formats to accommodate audit procedures

[1] The Department of Defense 5220.22-M data sanitization algorithm is not included in the current version of that document. Blancco supports both DoD 3-pass and 7-pass methods that are sometimes still required by internal policies, however. Even so, we highly recommend updating policies to specify following NIST SP 800-88 media sanitization guidelines. NIST SP 800-88 accommodates sanitization requirements of newer technologies, like SSDs and provides guidance on complete sanitization for a wide range of digital storage devices. See "Data Sanitization in the Modern Age: DoD or NIST?" available from the Blancco website, for more on this topic.

If returning to manufacturer/lessor:

- **If permitted in your lease agreement, consider removing hard drives before returning devices to the lessor, particularly for highly confidential data.** Note, however, that there may be fees incurred by the leasing vendor if the leased unit is not fully functional when you return it. Many ITAD vendors will provide turnkey services to remove and erase drives, replace or destroy drives, repair units under warranty and otherwise manage the leasing return process.
- **Sanitize loose drives or intact devices** with verified, certified data sanitization processes. If using an ITAD, disable any mobile device management (MDM) or Find My iPhone (FMiP) software.
- **Erase before destruction.** If leased units are destined for physical destruction rather than for return, erase data from assets beforehand to overcome the vulnerabilities that can arise with physical destruction (inadequate SSD shred sizes, for example).
- **If the lessor will be conducting data sanitization before refurbishing used devices,** work with the leasing vendor as well as legal and finance departments to ensure stringent data protection measures are agreed upon in writing for your most confidential data, as well as to ensure leasing payments cease appropriately.
- **Get sanitization verification:** Ask for certificates of erasure or other tamper-proof sanitization reports for all devices.

If reusing within the organization (internal reuse):

- **Sanitize all hard drives and devices using an approved data sanitization algorithm.** For drives being reused in-house, lower levels of sanitization may be appropriate. Retain all certificates of erasure or other tamper-proof sanitization reports for compliance and auditing purposes, preferably in a central management console that hosts erasure activity by device.

If donating or selling (external reuse):

- **Use the process for internal use (above), but sanitize to the most stringent method possible.** This may be done in-house with software-based data erasure or through an ITAD or other services provider that can sanitize and refurbish devices for donation or resale.
- **If working with an ITAD or other third-party processor,** make sure the vendor uses verified, certified data sanitization processes. If using an ITAD, disable any MDM or FMiP software.

If physically destroying or recycling:

- **Sanitize all devices using secure data erasure to add an extra layer of security during storage,** transport of devices or gaps in physical destruction approaches (small SSD chips making it through an HDD shredder's larger shred size, for instance). This is especially important for highly sensitive data.
- **Decide whether you are destroying the entire device or only the drives.**
- **Work with an ITAD or recycling company** for any physical destruction or use internal processes to dispose of any outdated IT assets, being sure to abide by e-waste disposal and recycling regulations.

Gartner provides the following user advice in the Hype Cycle for Data Security, 2019:

"Ensure your ITAD vendor provides a certificate of data destruction with a serialized inventory of the data-bearing assets they sanitized. Include a clause within your ITAD contract giving you the right to audit the ITAD vendor's data sanitization processes/standards to ensure their compliance with your security and industry standards (e.g., NIST 800-88). Regularly (e.g., annually) verify that your ITAD vendor consistently meets your data sanitization security specifications and standards."[2]

[2] Gartner "Hype Cycle for Data Security, 2019," Brian Lowans, 30 July 2019

- ○ **Destroy using methods appropriate to the drive type,** paying particular attention to shred size for solid-state drives (SSDs) and SSD-containing devices.
- ○ **Obtain certificates of destruction.**

Closeout Decommissioning Process

- ☐ **11. Record all drive sanitization results.** Log and verify any necessary information for auditing purposes, including a Certificate of Erasure if data erasure has been performed.
- ☐ **12. Distribute erased assets.** Distribute usable, sanitized devices accordingly, whether in-house or externally, documenting the transfer and itemizing each unit.
- ☐ **13. Facilitate accurate accounting.** Coordinate with your accounting department to confirm stop payments for leased assets, account for sold or donated devices and recover all software licenses.

Decommissioning assets with confidential data?
Read "Drive Destruction vs. Data Erasure: Which Data Disposal Method is Most Secure?" next.