Decommissioning Checklist for Data Centers: Servers

Most enterprise data centers, including heavily-regulated industries such as finance, healthcare and government, are required to keep very strict records of their servers. These records allow them to prove compliance when government agencies or industry auditors come calling. When a server is brought online or taken offline, the process must be documented with commissioning and decommissioning reports.

The following steps will take you through the server decommissioning process, including best practices for data erasure and reporting.

Server Decommissioning Process:

- ☐ **Step One:** Identify and record server to be decommissioned. Locate it in the data center. Schedule it for decommissioning,
- ☐ **Step Two:** Identify and retain all software licenses associated with the server.
- ☐ **Step Three:** Schedule the cancelation of any vendor maintenance contracts associated with the server or software.
- ☐ **Step Four:** Backup and save any necessary data.
- ☐ **Step Five:** Disconnect server from network. Remove from ACLs, subnets, and firewalls.
- ☐ **Step Six:** Turn the box of that's being decommissioned.
- ☐ **Step Seven:** Remove the server from the rack for physical destruction or data erasure sanitization with secure, certified, overwrite of all data. Or erase multiple servers in-rack using Blancco Management Console-based erasure.
- ☐ **Step Eight:** Erase the disks in the server using an approved data sanitization method (physical destruction or software-based data erasure). Data erasure ensures that the data is unrecoverable and is a more environmentally-friendly option.

Process with Physical Destruction & Free Data Wiping Tools:

- ○ Physically remove HDDs from storage and SANs and physical destroy them individually. Keep records of all physical destruction actions.
- ○ Erase individual SAN HDDs; then reconfigure the system to once again be operational (at a cost).
- ○ Risks noncompliance with key data privacy regulations.

Process with Software-Based Data Erasure:

- ○ Remotely or locally erase SANs while they are in active use.
- ○ Erase all active LUNs containing customer data.
- ○ Fulfill security policy requirements and automatically create an audit trail.
- ○ Enable resell or return of the SAN.
- ○ Potentially use the Blancco global trading network to maximize revenue.
- ○ Guarantee compliance with global data privacy regulations.

- [ ] **Step Nine:** Log any necessary information for auditing purposes, including a Certificate of Erasure if data erasure has been performed.

  Why are Blancco Data Erasure Certificates So Important?

  So you can show that the erasure was done, and done properly.

  - ✔ Digitally-signed
  - ✔ Tamper-proof
  - ✔ Automatically sent to the Blancco Management Console for audit-ready reporting
  - ✔ Data can be exported via .XLS, PDF, XML.
  - ✔ The certificate can be sent from the Management Console via API to your AMS system automatically.

- [ ] **Step Ten:** Place the server on a pallet.
- [ ] **Step Eleven**: Coordinate with your accounting department so that the fixed asset (server) is taken off the books as well as recovering all the software licenses.
- [ ] **Step Twelve:** Work with an ITAD or recycling company for the physical destruction of the server, or use internal processes to dispose of any outdated IT assets.

Decommissioning servers doesn't have to be a long and complicated process. Learn how Blancco helped a major public cloud provider erase 800+ servers overnight.