Decommissioning assets

How to retire digital assets (such as data, software, or hardware) from operation.

This guidance describes why it's important for organisations to decommission digital assets, and how to do so securely. It's aimed at technical staff and risk owners. For advice dealing specifically with decommissioning hardware, please refer to our guidance on discontinuing obsolete products or network devices.

What is decommissioning?

Decommissioning involves retiring digital assets - such as data, software, or hardware - from operation. It is a critical phase in the lifecycle of any asset. Decommissioning can be highly expensive and complex, with potentially severe repercussions if not executed properly.

Outdated or unsupported assets can pose an unacceptable risk to the organisation. As the NCSC guidance on asset management explains, assets that are no longer required become liabilities because they can open up vulnerabilities or expose information. Decommissioning helps to reduce unnecessary risks, which can include:

- unauthorised individuals accessing sensitive data
- lost data, services or functions
- disruption to the organisation
- inability to roll back to a known safe state
- exploitation of services or devices

Planning decommissioning

Although decommissioning typically occurs at the end of an asset's lifecycle, it is crucial to consider decommissioning at the start of the procurement process of the asset.

Asset discovery and valuation

A crucial first step is **identifying** all the assets in your organisation, which is described in the NCSC guidance on asset management. You should also be aware of the risks posed by 'shadow IT', the unknown assets that are used within an organisation for business purposes. Since these are not accounted for by asset management, nor aligned with corporate IT processes or policy, they're a particular risk to your organisation.

You will also need to validate the accuracy of your records, which should include the asset's purpose, and (where appropriate) what data it processes, stores or transmits. The goal is to understand the potential impact of the asset's decommissioning, and ensure that all associated components are accounted for. This is because decommissioning can have broader impacts than are immediately apparent. For example, decommissioning a temperature control asset initially might seem to only affect temperature regulation. However, it could lead to overheating of all digital assets in that space due to unregulated temperatures.

Your work should encompass other assets that may become redundant once the primary asset is decommissioned. For instance, a test or pre-production server will need to be decommissioned if the related production server is slated for decommissioning. Viewing the organisation as a holistic system (rather than as isolated parts) will help with this.

Backup, archiving and recovery plans

If decommissioning does not go as planned, or if only part of an asset needs decommissioning, then having backup, archiving, and recovery plans is critical. For example, if a server is being decommissioned, you'd need to make a backup of the data so that it can recovered onto the new server. In this case, 'data' includes all information required to execute a rollback plan, such as

configuration data, firewall rules, and network diagrams. You should maintain backups for a certain period to cope with any unexpected events that may necessitate a rollback, or for legal or compliance purposes.

Where possible you should test your rollback plan or at least key aspects of it prior to starting the decommissioning process. Your recovery plans should include:

- description of software or data that may need to be reinstalled on assets, and where this is stored
- ways to notify both the individuals and teams most likely to be making the rollback changes (and the users or teams likely to be impacted by the rollback)
- ways to protect critical functions should the rollback plan take longer than is expected
- checks in place to confirm the rollback has been successful

For more information, refer to the NCSC's guidance on creating ransomware-resistant backups.

Decommissioning assets

A common requirement during decommissioning is the sanitisation of storage media. This can be done for many reasons:

- **Re-use:** if you want to allocate a device to a different user, or repurpose equipment within your organisation.
- **Sell:** you might want to sell (or donate) equipment that no longer meets your organisation's needs.
- **Repair:** you may need to return a faulty device to the vendor for repair or replacement.

Sanitisation is the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level. Some forms of sanitisation will allow you to re-use the media, while others are destructive in nature and render the media unusable.

Once the appropriate data has been backed up (if required), the original asset including data within it should be sanitised in line with the NCSC's Secure sanitisation of storage media guidance.

> Note that the NCSC has also published separate guidance on the secure removal of data or malware from smartphones, tablets, laptops and desktop PCs, which is aimed at users wishing to sell or dispose of their own personal devices.

Once the actual decommissioning of assets begins, you'll need to ensure that:

- the coordination of decommissioning activities is in place, such as the introduction of replacement assets
- there are effective communications so that everyone who is impacted (including end users) is aware of what is happening
- assets are stored securely whilst they are awaiting their next stage of decommissioning; assets holding potentially sensitive data should not be stored in insecure environments
- replacement assets are in place and working as expected before performing irreversible actions (such as the permanent destruction of configuration data)
- third parties are appropriately certified and vetted if they are carrying out sensitive activities
- appropriate tracking is in place for any assets that are transferred between individuals or teams; this may require a more stringent, detailed, chain-of-custody type of tracking for sensitive or valuable assets

---

Post decommissioning

Once the decommissioning of an asset is complete, its effectiveness must be verified. If a device is decommissioned for repurposing, such as for reuse or resale, you should ensure that the appropriate sanitisation process has been followed.

You might have delegated certain decommissioning tasks (like asset destruction) to external parties. In such instances, it's crucial to confirm and keep evidence that these tasks were carried out properly and with the necessary rigor. This evidence typically comes in the form of certificates. Similarly, any decommissioning activities conducted internally should be well-documented.

During and after the decommissioning process, you should update your asset inventories to accurately reflect the changes in your environment. This ensures a dependable source of truth is available for those who may need to implement changes or manage risks in your environment.

Even after completing the decommissioning process, it is important to continue monitoring for any unforeseen impacts that may not have been immediately apparent. In such cases, your backup, archiving, and recovery plans will be critical.

PUBLISHED

20 May 2025

REVIEWED

20 May 2025

VERSION

1.0

WRITTEN FOR

Small & medium sized organisations

Public sector

Cyber security professionals

Large organisations