# Proper Device Reuse and Recycling for Devices Used in the Covered Entity

This article outlines the necessary steps to securely configure a device for reuse that was previously used in Yale's Covered Entity. This article has been broken down into the following scenarios:

- Proper device reuse process for devices staying in the Covered Entity
- Proper device reuse process for devices leaving the Covered Entity

***Note**: If you are looking to dispose of a device that was used in the covered entity, dispose of the entire device in accordance with the Yale Environmental Health and Safety Process. For more details, see the KB article "Disposal of Computers and Equipment". (KB0000315).

## Proper device reuse for devices staying in the Covered Entity

1. Ensure the device is whole disk encrypted
2. Re-image the device to meet the Minimum Security Standards for High Risk Data.

***Note:** the ITS Chain of Custody document is not required.

## Proper device reuse for devices leaving the Covered Entity

### When a device is being re-used by another Yale department:

This section outlines the steps to take when a device is leaving the covered entity and being repurposed in a department outside of the covered entity.

*Example: A Device is leaving Internal Medicine to be reused in the Math department.*

1. Ensure the device is whole disk encrypted.
2. Re-image the device and configure it to meet the Minimum Security Standards.
3. Complete the ITS Chain of Custody Document.

### When the device is being configured for personal use:

This section outlines the steps to take when a device that was being used within the covered entity and is being reconfigured for personal use.

**For Windows Devices with a TPM Chip:**

1. Ensure the device is whole disk encrypted.
2. Clear the TPM chip per the instructions in the article below, "How to Clear the TPM security chip on Yale Supported Hardware" (KB0022199).

3. You can verify that this sanitization process worked by rebooting the device after making the change. You should be at the BitLocker recovery screen.
4. Perform a fresh OS install using manufacturer provided media. The MW image may not be used for this use case.
5. Complete the ITS Chain of Custody Document.

**For Mac Devices:**

1. Ensure the device is whole disk encrypted.
2. Repartition the hard drive per the instructions in the article, "How to Repartition a Fusion, FileVaulted, or APFS-formatted Macintosh Hard Drive" (KB0004772).
3. Perform a fresh OS install using manufacturer provided media. The MW image may not be used for this use case.
4. Complete the ITS Chain of Custody Document.

**For All Other Devices:**

***Note:** the following instructions pertain to both a Mechanical and Solid State Drive (SSD).

**Option 1:**

1. Ensure the device is whole disk encrypted.
2. Perform a fresh OS install using manufacturer provided media. The MW image may not be used for this use case.
3. Complete the ITS Chain of Custody Document.

**Option 2:**

1. Ensure the device is whole disk encrypted.
2. Remove the hard drive and shred in accordance with the Yale Environmental Health and Safety Process. The hard drive will need to be replaced and the MW image may not be used for this use case.
3. Complete the ITS Chain of Custody Document.