Proper Device Reuse and Recycling for Non-Covered Entity Devices That Store High Risk Data

This article outlines the necessary steps to securely configure a device that previously stored high risk data. This article has been broken down into the following scenarios:

*__Note__: For devices that were used in the covered entity, please follow the steps outlined in KB0022724.

- Proper device reuse when the device is being reused at Yale University.
- Proper device reuse when the device is being configured for personal use.

Note: If you are looking to dispose of a device that stored high risk data, 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 being reused at Yale University

This section outlines the steps to take when a device is being re-purposed for a new role at the University. This process should be followed whether the device is staying within the department of origin or being used by a different department.

*__Note__: For devices that were used in the covered entity, please follow the steps outlined in KB0022724.

1. Ensure the device is whole disk encrypted.
2. Properly sanitize the device and configure it to meet the Minimum Security Standards for the data classification that device is now used for.

When the device is being configured for personal use:

This section outlines the steps to take when a device that stored high risk data is being reconfigured for personal use.

*__Note__: For devices that were used in the covered entity, please follow the steps outlined in KB0022724.

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.

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.

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.

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.