# Lifecycle+

# ASSET DISPOSAL

## REMOTE MANAGEMENT & ASSET SECURITY

## MOBILE DEVICE MANAGEMENT

Globally many companies are rapidly moving towards a mobile workforce. Devices such as phones, tablets and laptops more often than not are managed under a Mobile Device Management (MDM) solution.

Lifecycle+ assists our customers to deploy new hardware to end users, as well as in the value recovery of existing equipment managed within these MDM environments. With this experience we have released this guide to better assist customers in avoiding the pitfalls that can lead to the increased administration of assets, asset value reduction and increased time between return and final reporting.

## WHAT ARE SOME OF THE MOST COMMON ISSUES?

**Remote Management Lock for Apple Devices**

iOS based devices managed under an MDM will have this feature enabled. It is important to remove the device completely from your respective MDM and Apple Business Manager prior to returning to Lifecycle+. Though our software tests for the presence of remote management, it will require additional touch time from the client and delay the final reporting processes if left to be completed post return.

**iCloud Management for Apple Devices**

It is our experience there is often a mixture of both corporate iCloud and personal accounts used on iOS devices. This is especially prevalent within the education sphere. Once a device is locked to a particular iCloud account it remains unusable unless removed by the respective owner of that account. Unlike remote management, the reliance on the account holder removing the device may mean an asset is devalued completely if unremoved.

**Microsoft Intune**

Your organisation may be using Microsoft Intune, a cloud-based service that manages and secures corporate data on various devices. If your device was used to access corporate resources, Intune's management policies often remain active until the device is explicitly removed from the system by an administrator. To ensure a smooth process and complete transfer of accountability, please contact your IT administrator to have the device officially 'retired' or 'unenrolled' from Microsoft Intune (and related services like Microsoft Entra ID or Autopilot) before you ship it to us.

**BIOS Passwords for All Devices**

There are three common passwords applied to a system that will need to be removed either prior (preferred), or a password provided to us to do so on your behalf.

**EXPLORE OUR SERVICES + CONTACT OUR EXPERTS**

sales@lifecycle.plus | +61 2 9620 5313 | www.lifecycle.plus

# ASSET DISPOSAL

# REMOTE MANAGEMENT & ASSET SECURITY

## BIOS PASSWORDS FOR ALL DEVICES

1. **Power on Passwords (POP)**
   This password is set to appear when a device is booted and will stop the machine from posting into the operating system. A screen prompt to enter a password will appear prior to booting to your OS.

2. **BIOS Password**
   This password is set on a device's BIOS to ensure that no settings can be changed by a third party. This password will not be evident at the time of bootup, however if you enter the BIOS you will not be able to make changes without being prompted to enter this

3. **Hard Drive Password**
   This can appear similar to the POP password as it will prompt the user to enter a password before the device can access the HDD and boot to the OS. Often it is represented as a different icon showing a picture of HDD. This will vary depending on make and model.

## ENTRUSTING PASSWORDS

The safekeeping of passwords is paramount to ensuring the safe operation of today's businesses. The handing-over of passwords to third party agents for the purposes of business continuity, means trust. Trust is a privilege earned through transparent processes and the consistent delivery of services. For Lifecycle Plus, your continued security is the cornerstone of our business. We would like to show you how we secure the passwords you give us to better protect your assets.

## IMPORTANT

Please ensure all of the above-mentioned devices are removed from your remote management or device management platform, immediately. Failure to do so could inadvertently give unwarranted access to your systems or profiles, subject to how your individual remote management platform is configured. Please contact your Remote Management provider for further information.

**EXPLORE OUR SERVICES + CONTACT OUR EXPERTS**

sales@lifecycle.plus | +61 2 9620 5313 | www.lifecycle.plus