Encryption process

**This is the information for Bitlocker encryption, procedure, link to use for recovery information and future tasks.**

**About Microsoft BitLocker Drive Encryption**

BitLocker is a native encryption feature available on the Enterprise editions of Windows Operating Systems.  Microsoft BitLocker Administration and Monitoring (MBAM) software is the application Florida Polytechnic uses to centrally monitor compliance and simplify the deployment and storage of recovery keys for all encrypted devices.

**Bitlocker System Requirements**

* Operating System must be Windows 7 or above
* The computer must be joined to Florida Polytechnic's Active Directory Domain.
* Trust Platform Module 1.2 (TPM)
  + For Windows 7, a functional TPM is required
  + Windows 8 and above, a functional TPM is preferred, but not required
  + NOTE: The TPM must be enabled, activated and the Operating System must be allowed to take ownership of the TPM in the BIOS (If option available. Not all computer models have this as an option in BIOS)

**Procedure to Encrypt a laptop already assigned to a user**

|  |  |
| --- | --- |
| **Task** | **Responsible Group** |
| Schedule a day with the end user to retrieve laptop to perform the encryption | Helpdesk |
| Backup user documents to protect data | Helpdesk |
| Update BIOS to latest version (varies by manufacturer and model) | Helpdesk |
| Enable and Activate TPM chip in BIOS (varies by manufacturer and model).  Please note to enable if the option is available for the OS to take ownership of the TPM. | Helpdesk |
| Install Microsoft Bitlocker & Administration Monitoring Agent (Performed via SCCM or Manually)   * The helpdesk will need Systems group to add the computer to the "MBAM Agent Install" collection * The helpdesk can install the agent manually from the Helpdesk Archives\Client Applications\MBAM 2.5SP1 Agent   **To Do**:  The agent should be part of the base image or at least be available to all computers in SCCM | Helpdesk or Systems group |
| Verify MBAM MDOP Agent installed successfully (Check Add/Remove programs) | Helpdesk |
| Apply Group Policy for Microsoft Bitlocker Administration & Monitoring   * Helpdesk will need to provide computer name to systems group | Systems Group |
| Start Encryption Process   * The encryption process should start within 90 minutes of the group policy being applied * Alternatively, the helpdesk can manually start encrypting the Operating System drive by double clicking on the following file:   C:\Program Files\Microsoft\MDOP MBAM\MBAMClientUI.exe | Helpdesk |
| Confirm encryption process completes successfully   * The process can take from 2 hours to a day to complete depending on the size of the Operating System hard drive. * The end user can't retrieve the laptop until the process is complete. * A notification indicating the encryption process is complete is displayed when | Helpdesk |
|  |  |

**Future Task Assignments**

|  |  |
| --- | --- |
| **Task** | **Responsible Person or Group** |
| Add MBAM Agent to base Image | William Powell |
| Setup SCCM Task Sequences to work with refresh of computers that are encrypted | William Powell |
| Setup SCCM Task Sequences for Encryption to run during imaging on new computers | William Powell & Luis Luque |
| Develop processes and documentation for Imaging & Refreshing of encrypted computers | Helpdesk |

The link below allows the helpdesk (full time employees) to perform tasks required on occasions by Bitlocker by logging in with their NetID and Password.

<https://ccc-mbamweb01.floridapoly.org/HelpDesk/default.aspx>

**Drive Recovery**

The Drive Recovery option allows you retrieve drive recovery keys that can help users regain access to a computer or encrypted drives. A drive may go into Recovery mode because of a forgotten BitLocker PIN or password, an action from Windows Update, or a change to the BIOS settings of the computer.

**Manage TPM**

The Manage TPM Form can be used to help users who cannot unlock their computer because the TPM (Trusted Platform Module) will not accept their BitLocker PIN. First, use the Drive Recovery form to help the users regain access to their computer. Then, use this form to provide a TPM owner password file to help the users manage their TPM.