evidence
action

1133 Connecticut Ave, NW, Suite 200
Washington, DC 20036
USA
+1 202 888 9886

## Standard Operating Procedure for BitLocker Encryption

### Introduction

This Standard Operating Procedure (SOP) details the process for applying BitLocker encryption on Windows-based devices at Evidence Action. BitLocker, an integral full-disk encryption feature of Windows, serves to secure data by encrypting the entire hard drive, thus enhancing the protection of stored information.

### Purpose

This SOP outlines the procedures for encrypting hard drives using BitLocker to ensure the security and integrity of data on Evidence Action  computers and devices.

### Scope

This procedure applies to all employees, contractors, and third parties who use Evidence Action computers and devices that store sensitive or confidential information.

### Pre-Encryption Checklist

- Ensure that the device is running a compatible version of Windows.
- Verify that the TPM is present and activated.
- Back up all important data before starting the encryption process .

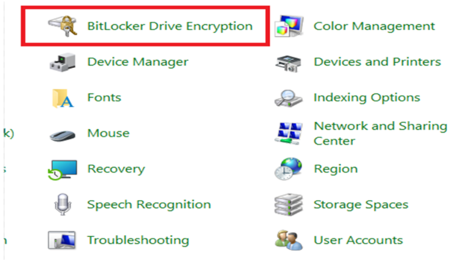
### Authorization for Disabling BitLocker

- To disable BitLocker for maintenance or troubleshooting, Global IT team members must obtain explicit permission from Allen.
- For devices in the Africa region, disabling BitLocker requires prior approval from Maria.

### Enabling BitLocker Encryption

### Open BitLocker Settings

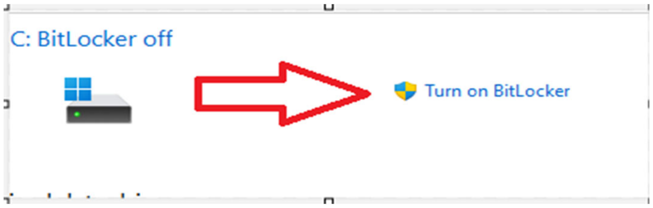
- Navigate to "Control Panel"



- Click "BitLocker Drive Encryption."

### Choose Drive for Encryption

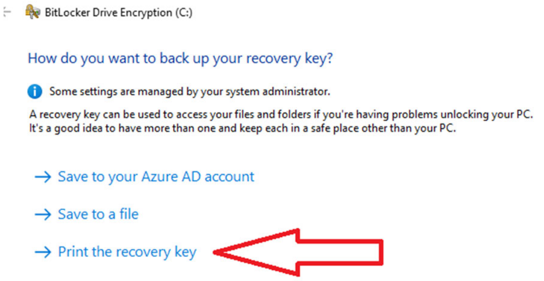
- Locate the drive you want to encrypt ( system drive, C:).



- Click "Turn on BitLocker" next to the chosen drive.

**Choose How to Backup Recovery Key**

- Choose to Print the recovery key


BitLocker Drive Encryption (C:)

How do you want to back up your recovery key?

Some settings are managed by your system administrator.

A recovery key can be used to access your files and folders if you're having problems unlocking your PC. It's a good idea to have more than one and keep each in a safe place other than your PC.

→ Save to your Azure AD account
→ Save to a file
→ Print the recovery key

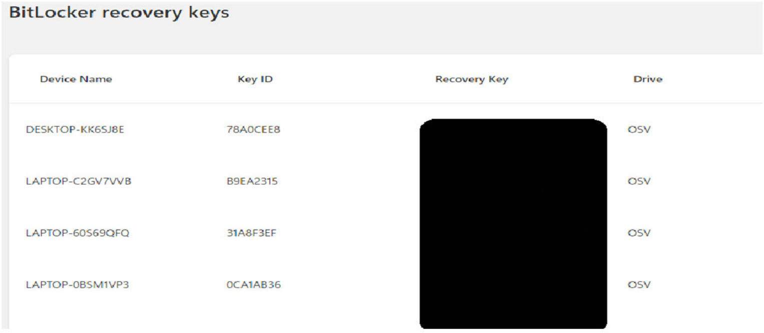
- Choose Microsoft Print to PDF
- Save into USB and name it for example US-LP-Serial Number
- Click "Next" to proceed.
- After generating the PDF, save a copy to the designated Box folder assigned for Bitlocker.

**Check BitLocker Status:**

- The "BitLocker Drive Encryption" window will display a list of all available drives with their encryption status.
- Check the status of the system drive (usually C:), and ensure it is either "BitLocker On" or "BitLocker is currently protecting this drive." This indicates BitLocker encryption is enabled.

**To recover your BitLocker key  from Microsoft Account:**

1. Go to the to this webpage https://account.microsoft.com/devices/recoverykey?refd=support.microsoft.com
2. Sign in to your Microsoft account.



BitLocker recovery keys

| Device Name | Key ID | Recovery Key | Drive |
|---|---|---|---|
| DESKTOP-KK6SJ8E | 78A0CEE8 | [redacted] | OSV |
| LAPTOP-C2GV7VVB | B9EA2315 | [redacted] | OSV |
| LAPTOP-60S69QFQ | 31A8F3EF | [redacted] | OSV |
| LAPTOP-0BSM1VP3 | 0CA1AB36 | [redacted] | OSV |

3. Copy the BitLocker key and save it in a safe place.

**Steps to Disable Secure Boot:**

1. **Restart Your Computer:**
    - Begin by restarting your computer.
2. **Access the BIOS/UEFI for Lenovo Settings:**
    - As your computer starts up, press the ENTER key to enter the BIOS/UEFI settings and then F1.

i.

    - Within the BIOS/UEFI menu, use the arrow keys to navigate. Look for a tab or section 'Security'.
    - Select the Secure Boot option and change its setting to 'Disabled'.
    - Note: The exact steps may vary depending on your computer's make and model.
3. **Access the BIOS/UEFI for Dell Settings:**
    - As your computer starts up, press F12 key to enter the BIOS/UEFI settings andBIOS Setup.

.

    - Within the BIOS/UEFI menu, use the arrow keys to navigate. Look for a tab or section 'Boot Configuration'.
    - Select the Secure Boot option and change its setting to 'Disabled'.
    - Note: The exact steps may vary depending on your computer's make and model.
4. **Save and Exit:**
    - After disabling Secure Boot, save the changes.
    - Exit the BIOS/UEFI settings. Your computer will restart.
    - To save changes, you often need to press F10 or select an option like 'Save and Exit'.

Record of Changes

| Date | Title/Brief Description of Change | SECTION/PAGE |
|---|---|---|
| January 29, 2024 | Initial | All |
| | | |
| | | |
| | | |