

Small business IT | Medium | 2 min read

Encrypting laptop drives with BitLocker or FileVault

If a laptop is lost or stolen, **encryption** stops a thief from reading the files on it. It is one of the simplest ways to protect customer and business data.

What these tools are

- **BitLocker** is Microsoft's drive encryption for Windows. It is available on Pro and higher editions, and some PCs use a simpler version called device encryption.
- **FileVault** is Apple's built-in drive encryption on Mac.

Before you start

- Make a **current backup**.
- Plug the laptop into power.
- Make sure you can sign in as the account owner or administrator.

Turn it on

Windows:

1. Open Settings, then Privacy and security, then Device encryption, or search for Manage BitLocker.
2. Follow the prompts to turn it on.
3. When asked how to back up the **recovery key**, choose your Microsoft account, work account or a printed copy, and keep it safe.

Mac:

1. Open System Settings, then Privacy and Security, then FileVault.
2. Turn it on and choose how to unlock your disk if you forget your password.
3. Store the recovery key safely, or use your iCloud account.

Warnings about recovery keys

- **Without the recovery key, you may never get your data back.** Store it somewhere other than the laptop.
- Do not save it only on the encrypted drive itself.
- Record which key belongs to which device. A password manager or secure shared admin folder works well.
- Windows may ask for the key after hardware or update changes, so make sure someone can find it.

Also remember

Encryption protects a switched-off or locked device. You still need a strong sign-in password, a screen lock, and updates.

When to get more help

Get help if the option is missing, if you are managing many laptops, if you are asked for a recovery key you cannot find, or before encrypting an older computer.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.