

The IRS requires every tax professional to implement these six minimum security controls before filing season. Each item below must be in place and documented in your Written Information Security Plan (WISP).

1 ANTIVIRUS / ANTI-MALWARE

- ✓ **Installed on every device**
Workstations, laptops, and any server
 - ✓ **Set to auto-update**
New threats emerge daily — manual updates are not enough
 - ✓ **Scheduled full scans**
At least weekly; daily on devices that touch client data
- **TIP:** Free options: Windows Defender (built-in), Malwarebytes Free. Paid... recommended for offices: Malwarebytes Business, Bitdefender.

2 SOFTWARE FIREWALL

- ✓ **OS firewall enabled on all devices**
Windows Firewall or macOS Firewall — never disabled
 - ✓ **Hardware firewall on router**
Most business routers include this; verify it is active
 - ✓ **Default router password changed**
Never leave factory credentials in place
- **TIP:** Check: Windows Security > Firewall & network protection. All three... profiles (Domain, Private, Public) must show "On."

3 MULTI-FACTOR AUTHENTICATION (MFA)

- ✓ **IRS e-Services — MFA required**
Mandatory since 2022; EFIN can be suspended without it
 - ✓ **Tax software logins — MFA on**
Drake, ProSeries, Lacerte, UltraTax — enable in settings
 - ✓ **Email accounts — MFA on**
Microsoft 365, Google Workspace — highest risk if breached
- **TIP:** Use an authenticator app (Google Authenticator, Microsoft... Authenticator) rather than SMS when possible — it is more secure.

4 STRONG, UNIQUE PASSWORDS

- ✓ **Minimum 12 characters per account**
Longer is always better — 16+ recommended
 - ✓ **No reuse across sites or accounts**
One breach exposes every reused password
 - ✓ **Use a password manager**
Bitwarden (free), 1Password, or Keeper recommended
- **TIP:** A password manager means staff only needs to remember one strong... master password. It also flags reused and weak passwords.

5 DRIVE ENCRYPTION

- ✓ **BitLocker on Windows (Pro/Enterprise)**
Control Panel > BitLocker Drive Encryption > Turn On
 - ✓ **FileVault on macOS**
System Preferences > Security & Privacy > FileVault
 - ✓ **Encrypt all portable devices**
Laptops, USB drives, external hard drives
- **TIP:** If a laptop is lost or stolen, encryption means the data is unreadable... without the password. This may exempt you from breach notification in some states.

6 ENCRYPTED BACKUPS

- ✓ **Backups performed at least weekly**
Daily recommended during filing season
 - ✓ **Backup stored off-site or in cloud**
Not on the same device or same physical location
 - ✓ **Backups are encrypted**
Use a backup solution with built-in encryption
- **TIP:** IRS recommends the 3-2-1 rule: 3 copies of data, on 2 different media... types, with 1 stored off-site.