

# THE ESSENTIAL

## Strategies to Mitigate Cyber Security Incidents

### 01 Application Control...

To prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.

**Why:** All non-approved applications (including malicious code) are prevented from executing.

### 02 Patch Applications...

e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.

**Why:** Security vulnerabilities in applications can be used to execute malicious code on systems.

### 03 Patch Operating Systems...

Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.

**Why:** Security vulnerabilities in operating systems can be used to further the compromise of systems.

### 04 Restrict Admin Privileges...

To operating systems and applications based on user duties. Regularly revalidate the need for privileges. Don't use privileged accounts for reading email and web browsing.

**Why:** Admin accounts are the 'keys to the kingdom'. Adversaries use these accounts to gain full access to information and systems.

### 05 Configure Office 365 Macro Settings...

To block macros from the internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.

**Why:** Microsoft Office macros can be used to deliver and execute malicious code on systems.

### 06 User Application Hardening...

Configure web browsers to block Flash (ideally uninstall it), ads and Java on the internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.

**Why:** Flash, ads and Java are popular ways to deliver and execute malicious code on systems.

### 07 Multi-factor Authentication...

Including for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive/high-availability) data repository.

**Why:** Stronger user authentication makes it harder for adversaries to access sensitive information and systems.

### 08 Daily Backups...

Of important data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.

**Why:** To ensure information can be accessed following a cyber security incident (e.g. a ransomware incident).