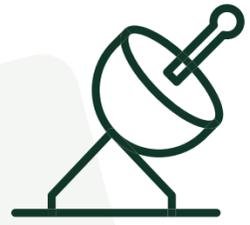


# What is the Essential 8?

Cybersecurity strategies recommended by the Australian Government, published in 2017.

- > Prevent Cyberattacks
- > Limit the impact of cyberattacks
- > Retain Data Recovery options and System Availability



Application Control



Admin privileges



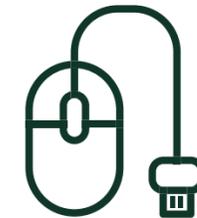
Patching Applications



Patching operating systems



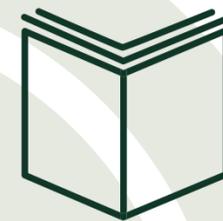
Configuring Microsoft Macro Settings



Multi-factor authentication



User application hardening



Regular backups

# Why should you use the Essential 8

- > Easy to set up
- > Cost-efficient
- > Reduces risk of getting hacked

# 1) Application Control

**WHAT:** Preventing all non-approved applications from running on managed devices

**WHY:** Enabling Application Control prevents users or malicious actors from running potentially harmful or inappropriate applications on managed devices

**HOW:** Application Control is available via most anti-virus programs including Sophos Advanced Intercept X. Microsoft Intune also offers AC for customers with Business Premium or E5 licensing

## 2) Patching Applications

**WHAT:** Updating security vulnerabilities in applications within 2 weeks of a regular update or 48 hours if an exploit exists

**WHY:** Keeping your applications up to date prevents malicious actors from exploiting known weaknesses within your systems

**HOW:** Many applications such as Adobe products, web browsers and Microsoft Office have regular automated maintenance. Subscribing to update notification emails and rolling out manual updates (PaperCut, Avaya)



# 3) Configuring Microsoft Office Macro Settings

**WHAT:** Deploying Microsoft's recommended Office Macro settings

**WHY:** Disabling these settings prevents malicious users from running code through trusted Office programs

**HOW:** You can manually disable Office Macro settings from the Trust Centre settings inside ANY Office app



## 4) User Application Hardening

**WHAT:** Disabling Advertisements, Flash and Java from an Internet browser. Preventing Office from running un-required processes

**WHY:** Ads, Flash & Java are popular ways to deliver and execute malicious code on systems. Disabling them prevents these sources from being interacted with by users

**HOW:** You can manually disable Flash, Java & Office processes from the respective app's settings. Can be deployed via registry keys

# 5) Restrict Administrative Privileges

**WHAT:** Restricting Admin privileges to only required admin staff and services

**WHY:** Administrator accounts provide the 'Keys to the Kingdom.' Adversaries can use these accounts to gain full access to your data and/or systems

**HOW:** Setup 'User' accounts on Windows devices for non-admin staff, limit the number of staff with admin permissions in online environments and most importantly don't share passwords for admin accounts

# 6) Patching Operating Systems

**WHAT:** Keeping your devices operating systems up-to-date

**WHY:** Keeping your devices up to date prevents malicious actors from exploiting known weaknesses within your systems

**HOW:** Windows devices have monthly auto-deployed patches and weekly security updates. Prevent users from disabling windows updates and remind them to Restart their devices

# 7) Multi-Factor Authentication

**WHAT:** Adding an additional verification method to user accounts prevents them from being breached. This typically includes text confirmations and authenticator app codes

**WHY:** Adding additional verification requirements prevents malicious actors from accessing accounts as the actor requires access to the additional method of verification

**HOW:** System admin staff can enforce user accounts to enrol in MFA for systems such as Microsoft 365 or Google Workspace. Azure joining devices and activating Windows Hello for business

# 8) Daily Backups

**WHAT:** Backing up company and user data to a secure cloud-based location

**WHY:** Backing up data to the Cloud enables you to recover important data in the case of a geographic emergency a malicious actor deleting files or a member of staff accidentally deleting an entire SharePoint site

**HOW:** Acronis Cyber Cloud Backup provides a Cloud backup service that can be linked to your Microsoft 365 tenant (or Google Workspace)