Client Learning Resources:

The Essential 8

Background

The Essential 8, are a set of technical control strategies targeted at preventing cyber intrusions, ransomware and other malicious events, limit their damage and enable organisations to recover if they occur.

Essential 8 mitigation strategies **What?**	**Why?**
Mitigation Strategies to Prevent Malware Delivery and Execution	
Application control to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers	All non-approved applications (including malicious code) are prevented from executing
Configure Microsoft Office 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	Microsoft Office macros can be used to deliver and execute malicious code on systems
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	Security vulnerabilities in applications can be used to execute malicious code on systems
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	Flash, ads and Java are popular ways to deliver and execute malicious code on systems
Mitigation Strategies to Limit the Extent of Cyber Security Incidents	
Restrict administrative privileges Admin accounts are the 'keys to the kingdom'. Adversaries use these accounts to gain full access to information and systems	Admin accounts are the 'keys to the kingdom'. Adversaries use these accounts to gain full access to information and systems
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	Stronger user authentication makes it harder for adversaries to access sensitive information and systems
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	Security vulnerabilities in operating systems can be used to further the compromise of systems
Mitigation Strategies to Recover Data and System Availability	
Daily backups of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes	To ensure information can be accessed following a cyber security incident (e.g. a ransomware incident)

Victorian Managed Insurance Authority (VMIA) acknowledges the Traditional Custodians of the land on which we do business and we pay our respects to Elders past, present and emerging. We acknowledge the important contribution that Aboriginal and Torres Strait Islander peoples make in creating a thriving Victoria.