The Essential Eight—at a glance

A simple view of the eight strategies and how they apply at different maturity levels.

Patch applications

Keep applications up to date to reduce exposure to known vulnerabilities.

Patch operating systems

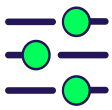
Apply security updates to operating systems, drivers, and firmware within defined timeframes.

Multi-factor authentication (MFA)

Require more than a password for access.

Restrict administrative privileges

Limit who has elevated access and define justifiable accounts.



Application control

Allow approved applications to run and block unauthorised software.

Microsoft Office macro settings

Reduce the risk of malicious macros by limiting how and where they can run.

User application hardening

Harden browsers, PDFs, and scripting tools to reduce attack paths.

Regular backups

Maintain tested backups protected from unauthorised changes.

How the Essential Eight applies at different maturity levels

Level 1
Foundation

Establish a baseline

At this level, the focus is on putting all eight controls in place to reduce common attack paths.

Level 2
Consistency & Visibility

Apply controls consistently

At this level, organisations are expected to apply controls consistently, with greater visibility and oversight.

Level 3
Detection & Response

Prove maturity & respond to threats

At this level, organisations must detect, log, and respond to malicious activity across all eight controls.

Based on guidance from the Australian Cyber Security Centre (ACSC)