



# MEETING THE Essential Eight MATURITY LEVEL ONE

Complete these tasks for each of the Essential Eight to meet the Australian Cyber Security Centre (ACSC's) Maturity Level One.



## APPLICATION CONTROL

- Develop a list of approved programs that can run on staff workstations.
- Restrict workstations from running non-approved executables.
- Restrict on-premises servers from running non-approved executables.



## PATCH APPLICATION

- Develop a process for identifying security risks in applications and drivers.
- Patch, update, or migrate applications and drivers that are identified as extreme security risks within a month.
- Update or replace applications and drivers that are no longer supported by their manufacturer.



## MACRO SECURITY

- Set policies to restrict macros from running in Microsoft Office without user approval.
- Stop regular users from changing macro security settings.



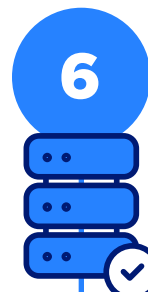
## USER APPLICATION HARDENING

- Configure workstation browsers to disable support for Flash.



## RESTRICT ADMINISTRATION PRIVILEGES

- Validate privileged access to systems, applications, and data repositories.
- Add security policies to prevent administrator accounts from reading emails, browsing the internet, and obtaining files via online services.



## PATCH OPERATING SYSTEMS

- Develop a process for identifying security risks in operating systems and firmware.
- Patch, update, or migrate operating systems and firmware that are identified as extreme security risks within a month.
- Update or replace operating systems and firmware that are no longer supported by their manufacturer.



## MULTI-FACTOR AUTHENTICATION

- Use multi-factor authentication for all remote access.
- Have at least two forms of authentication available to users. These can include passwords, security keys, physical one-time password tokens, biometrics, smartcards, mobile app one-time password tokens, SMS messages, emails, voice calls and software certificates.



## DATA BACKUPS

- Create a data backup and restoration procedure.
- Perform monthly backups of all important files, software, and configuration settings.
- Store backups for 1-3 months.
- Test backup restoration procedure annually.

Looking to boost your security posture?  
We can help, talk to us about Axient  
Managed Security Services that go  
beyond ACSC's Maturity Level One.

**axient**

[axient.com.au](http://axient.com.au) | 02 8338 3444