ACSC Essential Eight Security Solution

Need help securing your IT?

With the growing complexity of cyber-attacks, a severe shortage of IT security professionals, and increasing legislation against data breaches, it can be more difficult than ever to get and stay secure.

By leveraging the Australian Cyber Security Centre (ACSC) Essential Eight security model, our solution provides a three-step process to get and keep your IT secure, giving you peace of mind, saving you time and money, and reducing the risk of data loss and security breaches.

Peace of Mind

- **ACSC Essential Eight compliant –** We support all three maturity levels of the Australian Cyber Security Centre (ACSC) Essential Eight model.
- **Ongoing protection** – Our managed service ensures your IT stays secure month after month, allowing you to focus on your business.

Save …

- **Time** – Your most valuable resource is your staff. By leveraging our security experts, we free up your IT staff to focus on higher business value activities.
- **Money** – According to IBM, the average cost of a data breach in 2018 was A$5.2M. And this doesn't consider the loss in customer trust that can dramatically impact sales.

Reduce …

- **Risk of data loss** – EU GDPR and Australian Notifiable Data Breaches (NDB) Scheme are placing increasingly strong penalties around customer data losses.
- **Risk of security breach –** The longer an attacker is in your system (2018 advanced hacker average was 99 days), the more damage they can do to your business.

What you get

- *Assessment* – 2-day engagement, which is complimentary if you use our remediation services.
- *Remediation* – tailored to suit your current and desired security maturity levels – see next page.
- *Managed service* – let our security experts keep your IT secure through our fixed price offering.

Why Vigilant.IT?

- The first Australian Partner to achieve Microsoft's Gold Security competency.
- Over a decade of experience securing IT environments.
- Qualified security architects and Microsoft MVPs (Most Valued Professionals).

ACSC - Essential Eight Maturity Levels

High level summary

For more details, visit cyber.gov.au

Mitigation Strategy	Level One	Level Two	Level Three
Application control	Restrict workstation executables	Also restrict libraries, scripts, installers + servers.	Also rules to prevent app control bypasses
Patch applications	Monthly (extreme risk), don't use unpatched apps	Fortnightly (extreme risk)	48hrs (extreme risk), automated confirmation
Office macro settings	Macros require user approval, users can't change settings	Also macros must be signed, block Word macros from Internet	Also macro must be in Trusted Location
User application hardening	Web browsers prohibit Flash content	Also block ads and Java from Internet	Also Office disables Flash, prevents OLE packages
Restrict admin privileges	Privileges validated initially, not allowed to read emails, browse web, or access online files	Also privileges regularly validated	Also unable to read emails etc, access to systems, apps, & data limited to "as needed"
Patch operating systems	Monthly (extreme risk), don't use unpatched OS or ICT equipment	Fortnightly (extreme risk)	48hrs (extreme risk), automated confirmation
Multi-factor authentication	All remote users, two methods	Also privileged users or positions of trust	Also when accessing important data
Backup	Performed monthly, stored 1-3 months, partial restore annually	Weekly. Also stored offline or read only online, full restore tested once, partial biannual	Daily. Also stored more than 3 months, full restore tested regularly, partial quarterly

NOTE: Level 1 = partially aligned with overall strategy, level 2 = mostly aligned, level 3 = fully aligned