

Australian Government
Australian Security Intelligence Organisation

Protective Security Top 10

The essential components of a complete security framework to protect people, places, technology and information

1. Know the **threat** to your workplace
2. Establish a security **governance** framework
3. Build a strong security **culture**
4. Install and maintain **physical** security systems
5. Implement robust **ICT** systems
6. Implement a **personnel** security framework
7. Protect **information**
8. Be secure **online**
9. Recognise and **respond** to suspicious behaviour and security incidents
10. Regularly **review** your settings

Protective Security Top 10

The essential components of a complete security framework to protect people, places, technology and information

1 Know the threat to you and your workplace so you can prepare accordingly

- Identify the threats to—and vulnerabilities of—staff, key functions, critical systems, data, assets and facilities. And know that you may also be targeted.
- Conduct a risk assessment to identify your unique risks and risk tolerance.
- Apply a risk-based approach to security: focus your attention and resources where it will achieve the best outcomes.
  - **Threat** = intent and capability of an adversary.
  - **Vulnerability** = a flaw or weakness which could be exploited.
  - **Risk** = likelihood and consequence of an attack.
  - **Risk tolerance** = an informed decision to accept a certain level of risk.

2 Establish a security governance model to support oversight, control and decision-making

- Develop a security plan and establish a corporate body responsible for overseeing security matters and decision-making.
- Security is a shared responsibility: assign security responsibilities to trained personnel and collaborate—no single person or area can manage security alone.
- Establish sound and tested policies and procedures that are easy to follow and access and update them regularly—make doing the right thing, the right way, as easy as possible.
- Include policies and procedures to manage any risks posed by external visitors, contractors, managed service providers, staff working remotely and staff travelling overseas.

3 Build a strong security culture to enable, encourage and educate employees towards security-savvy behaviours

- Regularly assess the culture for trends that require attention.
- **Enable:** leadership, compliance and correction.
- **Encourage:** ownership, reporting, discipline, innovation and confidence.
- **Educate:** communicate and deliver security awareness training to all staff.

4 Install and maintain physical security systems to protect people, places, technology and information

- Provide secure and reliable infrastructure for all staff, including those working remotely.
- Ensure highly secure areas have systems that are auditable and can control access to sensitive information and assets, detect breaches or attempted breaches of access and provide real-time alerts about unauthorised access.
- Keep an inventory of all physical assets assigned to personnel (passes, tokens, laptops) and update the inventory regularly.
- Ensure physical and ICT supply chain risks are considered and addressed.

5 Implement robust ICT systems to protect your critical systems, devices and data from cyber threats

- Implement the ACSC's *Essential Eight*.
- Secure your accounts, devices and email—patch regularly and use complex passwords, multi-factor authentication and protection software.
- Manage the connectivity of systems and devices—**anything connected to the internet is vulnerable** (this includes PROTECTED networks).
- Secure all electronic devices: maintain physical control of them at all times; switch them off daily; limit the information stored on them; and sanitise them before destruction or disposal.
- Carefully consider the potential risks of using the cloud or data centres.
- Regularly back up devices, data and systems.



6 Implement a personnel security framework to ensure employees are suitable to have access to your people, key functions, critical systems, data, assets and facilities

- Implement appropriate and proportionate personnel screening procedures during pre-employment, throughout employment and at the conclusion of employment.
- Include external providers, managed service providers, contractors, consultants and business partners.
- Implement a counter insider threat program.
- Remember security clearance holders have additional obligations.

7 Protect information that is unique, privileged, sensitive and national-security classified

- Hold sensitive activities and discussions in secure areas (for example, recently swept spaces, device-free areas, Security Zones and SCIFs).
- Handle, use, store and destroy sensitive material appropriately.
- Control information access to only those with an appropriate security clearance and/or need to know.
- Restrict mobile devices in secure areas or near sensitive discussions.
- Protect your research and intellectual property by collaborating with care.
- Conduct technical security countermeasures sweeps if required.

8 Be secure online

- Restrict, limit or securely manage the connectivity of systems and devices.
- Regularly check the security settings of online accounts and delete or deactivate accounts no longer in use.
- Periodically review, update or remove information available online or on social media that could compromise the safety of your employees, workplace and assets, or be of interest to adversaries.

9 Recognise and respond to suspicious behaviour and security incidents

- Establish a reporting mechanism that is confidential, accessible and timely.
- Educate employees on what to report and how.
- Educate security teams to recognise and respond to possible reconnaissance activities.
  - Reconnaissance is the purposeful observation of people, places, vehicles and locations to gather information; it may be undertaken through physical and/or technological means.
- Educate employees to Think Before You Link when connecting online and to report suspicious approaches or persistent questioning.
- Establish emergency and security incident investigation and response procedures and know when referral to external agencies is required.

10 Regularly review your settings for effectiveness

- Regularly review your security governance and controls for effectiveness and adjust if required.
- Review security incidents to assess if there were missed opportunities to intervene earlier, if additional or different measures or training could have assisted, and if it was an isolated incident or part of a trend.
- Review and test incident response and investigation procedures for effectiveness.

This document provides broad advice on the actions government and industry security managers can take to protect their workplaces from various threats. This document is not comprehensive and security managers should refer to the source materials for detailed information.

Resources

ASIO and partner intelligence reporting and protective security products available to eligible subscribers of the Outreach portal—**www.asio.gov.au/outreach**—including:

- *Countering the insider threat: a security manager's guide*
- *Security manager's handbook: introduction to protective security measures*
- Security Managers Guides on *Supply chain security, Working from home, Data centre security* and *Electronic access control systems*
- Products on mobile device and travel security
- *Technical surveillance countermeasures inspections*
- *Think Before You Link* campaign materials
- *Protect your research; collaborate with care* campaign materials
- *Report prying minds* campaign materials
- *Secure your success* campaign materials

Australian Cyber Security Centre (ACSC) cyber threat reporting and mitigation advice available at **www.cyber.gov.au** including:

- *Information Security Manual*
- *Essential Eight*
- *Strategies to mitigate cyber security incidents*
- *System hardening and administration*
- *Remote working and secure mobility*
- *Cloud security guidance*

Protective security policy framework (PSPF)—
www.protectivesecurity.gov.au

Department of Defence, Australian Government Security Vetting Agency (AGSVA) security clearances information—**www.defence.gov.au/security/clearances**

Standards Australia—**www.standards.org.au**

- Australian Standard AS ISO 31000:2018 *Risk management guidelines*
- Standards Australia Handbook HB167:2006, *Security risk management*

24-14802