

PASSPORT TO GOOD SECURITY

PSR | Protective Security
Requirements

Key principles for a more secure organisation

Good security protects your organisation's people, reputation, and profitability.

This guide contains best practice to help you create an effective risk management strategy – one that covers identifying, assessing, and mitigating the threats your organisation might face.

1. CREATE GOOD GOVERNANCE



Identify who is accountable for security at board or executive level. Ensure they have clear reporting lines to all people with security responsibilities.

Monitor the effectiveness of security management across your organisation. Review and update at regular intervals. Seek regular briefings on the threats to your organisation.

2. CREATE A STRONG SECURITY CULTURE: SOFT MEASURES

Lead by example. A good security culture relies on visible endorsement and engagement from the top.

Develop clear and fit-for-purpose security policies (particularly on how to report security incidents) supported by training and regular communication.

Ensure your people are clear on how to report a security incident, and on their responsibilities in managing and resolving security risks.



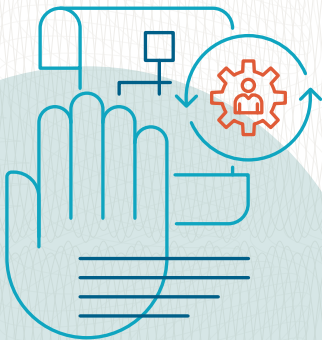
3. BUILD BUY-IN THROUGH TRANSPARENCY

Security principles, policies, and procedures should be transparent and accessible. To gain support from your people and buy-in from stakeholders, take an ethical approach that is proportionate to the risks.



4. CREATE A STRONG SECURITY CULTURE: HARD MEASURES

Establish robust procedures for dealing with poor security behaviour. Enforce security policies visibly and quickly when your people, contractors, or suppliers do not comply.



5. ADOPT A RISK MANAGEMENT APPROACH

Establish your organisation's appetite for security risk. Choose a risk management approach that suits your organisation and business activity – one that integrates security into your business but does not inhibit it.



6. IDENTIFY YOUR MOST VALUABLE ASSETS

Identify which assets are critical to your business success, competitive advantage, and continuing operation. Include people, products, services, processes, premises, and information.

Look beyond your organisation to suppliers and contractors. Establish a full and accurate picture of the impact on your organisation's reputation, share price or existence if sensitive internal or customer information was lost or stolen.



People



Products & services



Processes



Premises



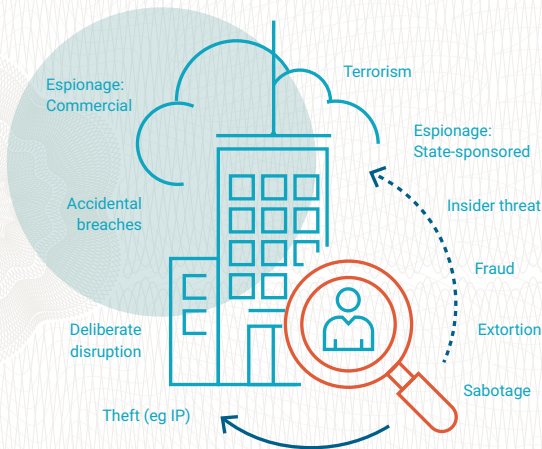
Information



7. IDENTIFY THE THREATS

Identify the security threats to your most valuable assets. Threats are diverse, may exist in physical or cyberspace, and may change over time.

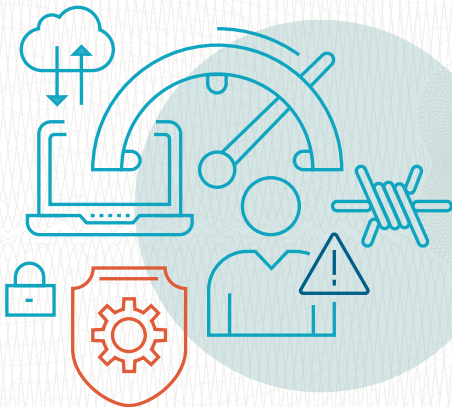
Consider exchanging information with other organisations to help you identify emerging threats and learn from others. Work on the premise that you and your peers are also likely to be key targets.



8. MITIGATE YOUR RISKS

Prioritise the risks to your organisation.
Reduce your vulnerability to them and their impact by putting a range of personnel, cyber, and physical security measures in place.

Accept that you cannot protect everything.
Build an effective, professional and competent security team with clear, well-defined, and rehearsed procedures.



9. PLAN FOR BUSINESS CONTINUITY

Identify your organisations' priorities for business continuity. Identify what's needed to keep your critical functions running or to restore them promptly if disrupted.

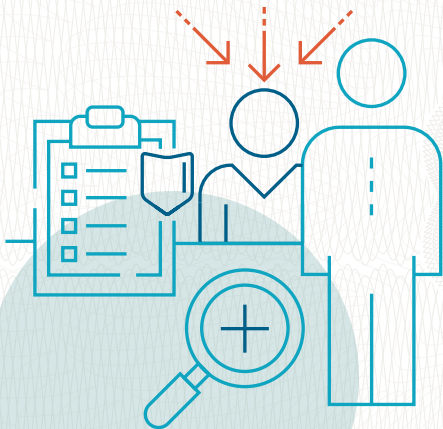
Create up-to-date response plans. Regularly test your plans with desktop and live exercises. Ensure the lessons learned are circulated and acted on. Understand the impact on the business if your online services were disrupted for a short or sustained period.



10. RECRUIT THE RIGHT PEOPLE

Good personnel security begins at recruitment, so ensure your pre-employment checks on all prospective employees are robust.

Include security checks in your selection process for contractors and suppliers.



11. KEEP REMOTE AND MOBILE WORKING SECURE

If your people and contractors work from home or travel around New Zealand and overseas, ensure they are briefed, trained, and equipped to keep themselves and sensitive information secure at all times.



12. GUIDE BEHAVIOUR ON SOCIAL MEDIA

Introduce security awareness training to promote safe and secure practices for social media that raise awareness of the risks involved (both at work and at home).



13. MANAGE DEPARTURES

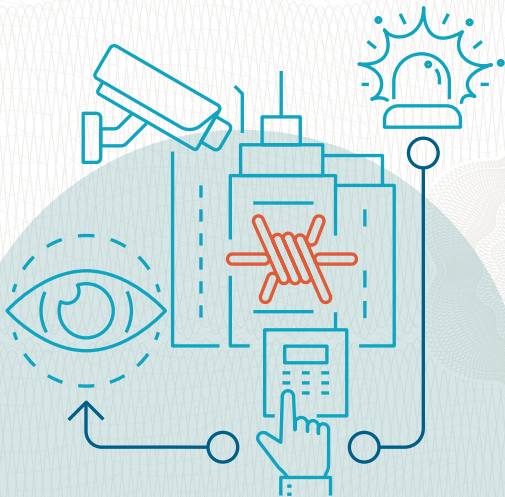
Review access privileges for all people transferring roles or leaving your organisation.

Create procedures to ensure all people who leave are seen and the reasons for their departure established. Remind them of their ongoing confidentiality obligations.



14. BUILD IT SECURE

Ensure your buildings, physical barriers, and surveillance equipment are fit for their specific purpose. Make sure they are built, installed, and used correctly to prevent unauthorised entry and enable early detection.



15. CONTROL ACCESS

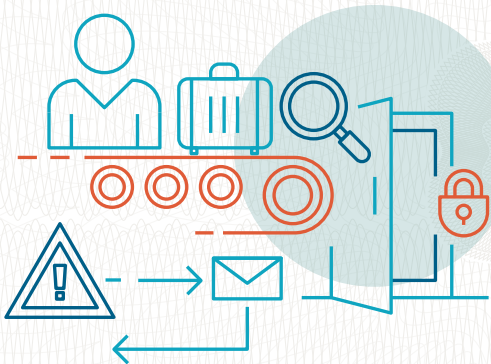
Introduce control measures and monitoring systems to ensure your people, contractors, suppliers and the public only have access to buildings, information, and people necessary for their role.



16. SEARCH AND SCREEN

Consider creating more secure zones within your site. Use search and screening procedures to stop prohibited people and items entering or leaving.

Consider whether to have mail delivered and screened off-site, and whether to have other deliveries made off-site too.



17. PROTECT YOUR INFORMATION

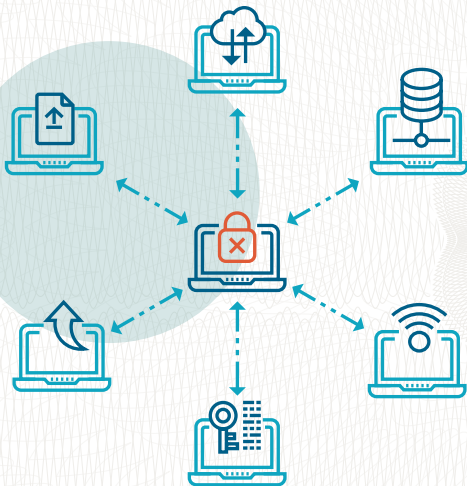
Establish an information and cyber security policy that identifies the information risks across your organisation and applies appropriate security measures.

Conduct regular reviews to incorporate changes in technology.



18. SHARE INFORMATION SECURELY

Ensure contractors, suppliers, and other organisations that handle (send, receive, or store) your information are clear on their legal responsibilities to protect it securely – now and in the future.



19. MANAGE INCIDENTS

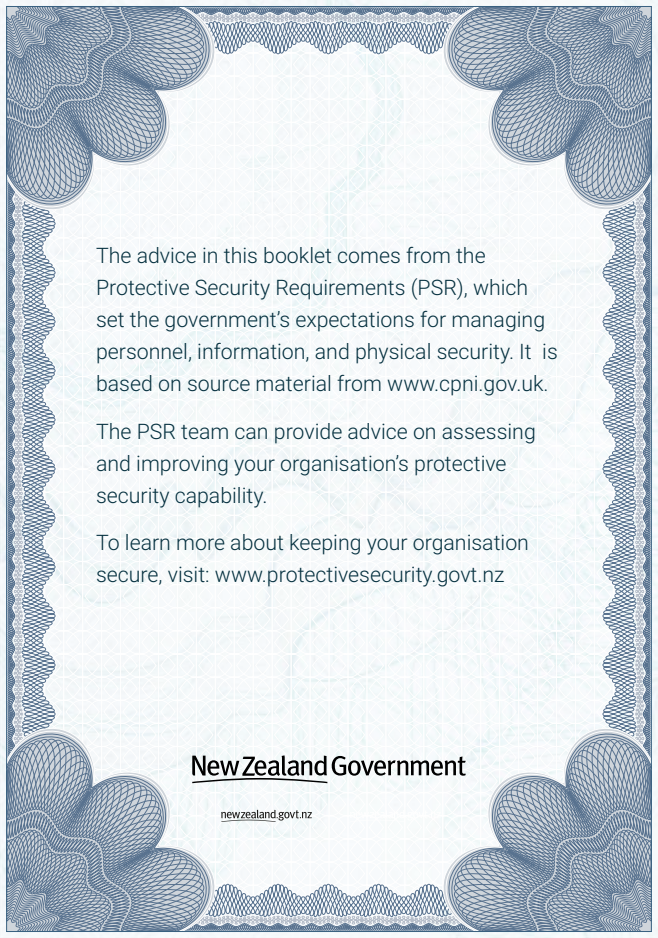
When drawing up incident management plans, consider damage to critical assets, reputation and confidence, financial standing, employee morale, and the time needed to recover business as usual.



20. EMERGE STRONGER

Learn from internal and external security incidents. Use the knowledge to anticipate new vulnerabilities, threats, and risks and to remain compliant with evolving regulatory requirements.





The advice in this booklet comes from the Protective Security Requirements (PSR), which set the government's expectations for managing personnel, information, and physical security. It is based on source material from www.cpni.gov.uk.

The PSR team can provide advice on assessing and improving your organisation's protective security capability.

To learn more about keeping your organisation secure, visit: www.protectivesecurity.govt.nz

New Zealand Government

newzealand.govt.nz

New Zealand Government