PASSPORT TO GOOD SECURITY

For Senior Executives

CPNI
Centre for the Protection of National Infrastructure

Key principles for a more secure organisation

Good security protects the people, reputation and profitability of your organisation.

This guide contains best practice to help you create an effective risk management strategy; one that covers the identification, assessment and mitigation of the threats your organisation might face.

CPNI
Centre for the Protection of National Infrastructure

1. GOOD GOVERNANCE

Identify who is accountable for security at board/executive level. Ensure they have clear reporting lines to all staff 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. IDENTIFY YOUR MOST VALUABLE ASSETS

Identify which assets are critical to your business success, competitive advantage and continuing operation. These will 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 company's reputation, share price or existence if sensitive internal or customer information were to be lost or stolen.

People | Products & Services | Processes | Premises | Information

3. IDENTIFY THE THREATS

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

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

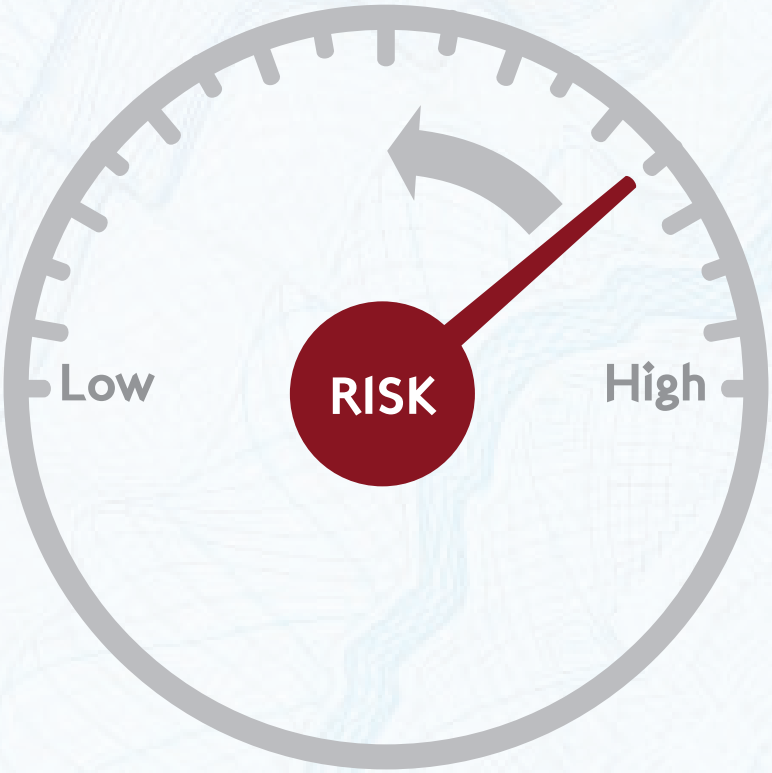
4. ADOPT A RISK MANAGEMENT APPROACH

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.

5. MITIGATE YOUR RISKS

Prioritise the risks to your organisation and put in place a range of personnel, cyber and physical security control measures that reduce your vulnerability to them and their impact.

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



6. LEGALITY, ETHICS AND TRANSPARENCY

Security principles, policies and procedures should be transparent and accessible. Taking an ethical approach, proportionate to the risk, will gain support from employees and buy-in from stakeholders.

7. CONTROL ACCESS

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

8. 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 that staff are clear on how to report a security incident, and on their responsibilities in managing and resolving security risks.

9. CREATE A STRONG SECURITY CULTURE: HARD MEASURES

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

10. PROTECT YOUR INFORMATION

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

Conduct regular reviews to incorporate changes in technology.

II. SECURE SHARING OF INFORMATION

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.

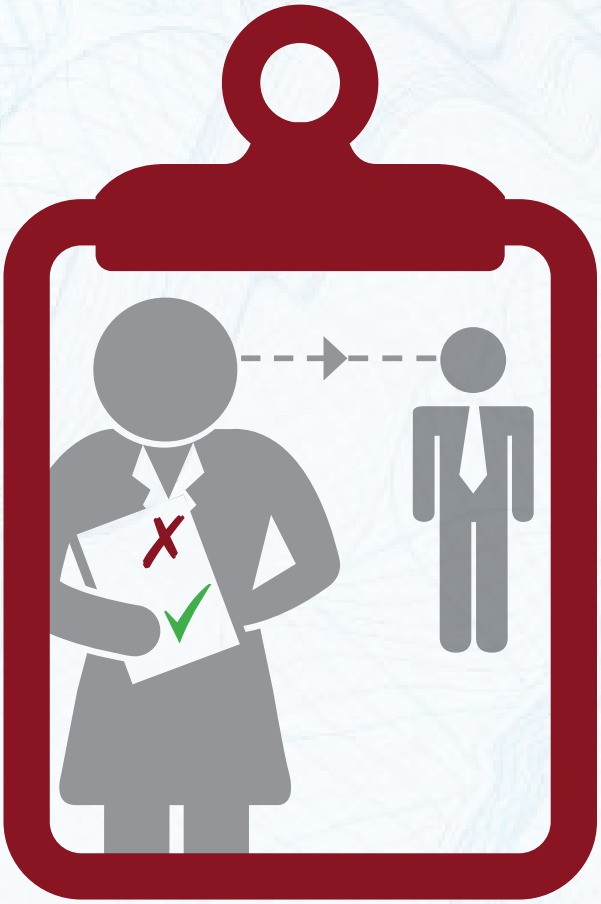
12. ONLINE SOCIAL BEHAVIOUR

Introduce staff education and training to promote safe and secure practices when using online social media to raise awareness of the risks involved (both at work and at home).

13. SECURITY PRE-SCREENING

Good personnel security begins at recruitment so ensure you make appropriate pre-employment checks on all prospective staff.

Include security checks as part of your contractor and supplier selection process.



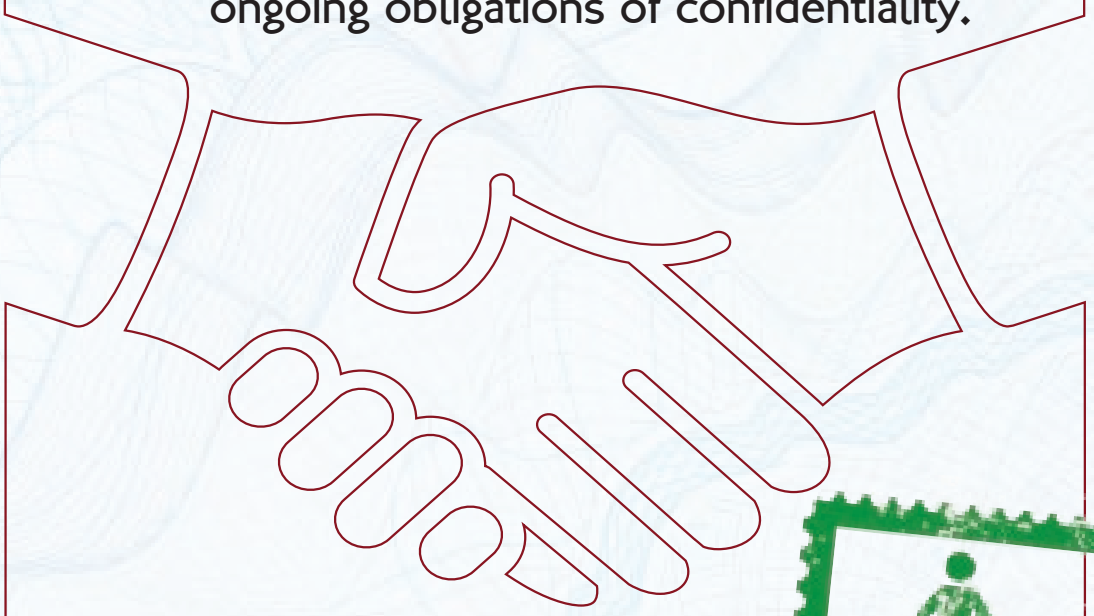
14. HOME AND MOBILE WORKING

If your staff (and contractors) work from home or travel around the UK and overseas, ensure they are briefed, trained and equipped to keep themselves and sensitive information secure at all times.

15. STAFF EXIT STRATEGY

Review access privileges for all staff when transferring roles or leaving the organisation.

Create procedures so that all staff leaving your organisation are seen and the reasons for their departure established. Remind them of their ongoing obligations of confidentiality.



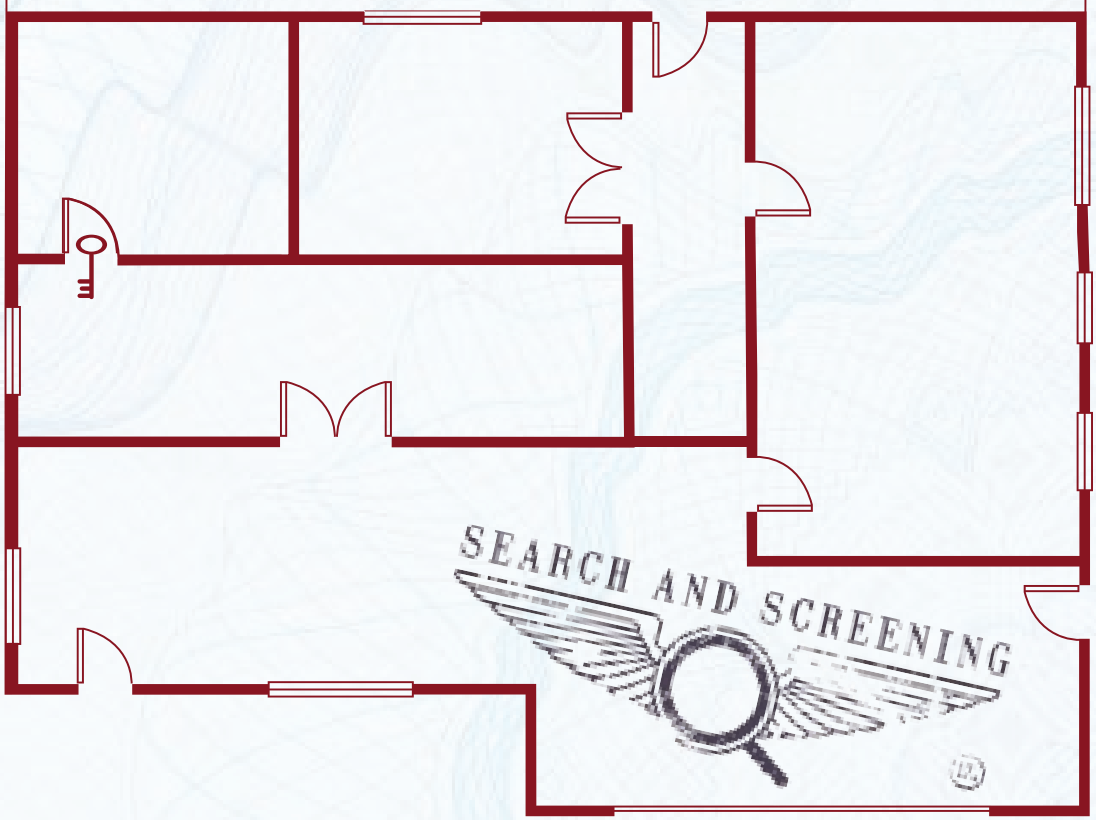
16. BUILD IT SECURE

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

17. SEARCH AND SCREENING

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.



18. BUSINESS CONTINUITY

Check the adequacy of utility supplies and standby facilities and create up-to-date response plans.

Regularly test your plans with desktop and live exercises and ensure the lessons learned are circulated and acted upon. Understand the impact on the business if your online services were disrupted for a short or sustained period.

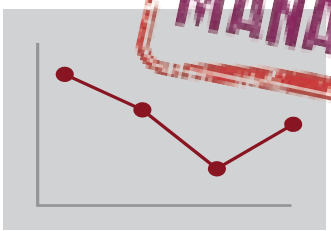
19. INCIDENT MANAGEMENT

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

NEWS

Business recovers after cyber attack

Infra Org's share price rallies with strong incident management.



INCIDENT MANAGEMENT

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 CPNI – the UK government agency responsible for giving protective security advice.

We advise on physical, personnel and cyber security.

To learn more about keeping your organisation secure, visit: www.cpni.gov.uk

CPNI

Centre for the Protection of National Infrastructure