Guidelines for protecting our people, information and assets

This guide outlines the Government's expectations for protective security. Effective security enables Cook Islands Government organisations to work together securely in an environment of trust and confidence. This guide covers:

WHAT IS THE PROTECTIVE SECURITY FRAMEWORK?

The Protective Security Framework is a set of best practice guidelines and principles to help you identify what your organisation must do to protect your people, information and assets.

Protective security encompasses and extends organisational practices such as health & safety, privacy, business continuity, incident management, and emergency and disaster management.

The framework has been designed with enough flexibility to be used across all organisations with differing needs and capabilities.

PROTECTIVE SECURITY **REQUIREMENTS**

The framework for protective security has four tiers and a hierarchical structure.

Security Governance

GOVSEC

Ensuring you have security management structures, procedures and culture in place to respond appropriately to security events.

1. Establish and maintain the right governance & management
2. Understand what you need to protect
3. Assess your capability
4. Build security culture
5. Develop and maintain security policies, processes and procedures
6. Manage risks when working with others
7. Manage security incidents
8. Be able to respond

Personnel Security

PERSEC

Ensuring your people are trusted to have access to official information and assets.

1. Recruit the right person
2. Ensure their ongoing suitability
3. Manage their departure

Information Security

INFOSEC

Ensuring the confidentiality, integrity and availability of your information is protected.

1. Design your information security
2. Check your security measures
3. Keep your security up to date

Physical Security

PHYSEC

Providing and maintaining a safe and secure working environment.

1. Design your physical security
2. Check your security measures
3. Maintain your security

Security Governance

GOVSEC-1

Establish and maintain the right governance and management

Establish and maintain a governance structure that ensures the successful leadership and oversight of protective security risk.

Appoint a member of the senior team as your Chief Security Officer, responsible for your organisation's overall protective security policy and oversight of protective security practices.

GOVSEC-2

Understand what you need to protect

Identify the people, information, and assets that your organisation manages. Assess the security risks (threats and vulnerabilities) and the impact of any security breach.

GOVSEC-3

Assess your capability

Use an annual evidence-based assessment process to provide assurance that your organisation's security capability is fit for purpose. Provide an assurance report to Government if requested.

GOVSEC-4

Build security culture

Provide regular information, security awareness training, and support for everyone in your organisation, so they can meet and uphold your organisation's security policies.

GOVSEC-5

Develop and maintain security policies, processes and procedures

Develop and maintain security policies and plans that meet your organisation's specific business needs. Make sure you address security requirements in all areas: governance, information, personnel, and physical.

Review your policies and plans every 2 years or sooner if there are changes in the threat or operating environment.

GOVSEC-6

Manage risks when working with others

Identify and manage the risks to your people, information, and assets before you begin working with others.

GOVSEC-7

Manage security incidents

Make sure every security incident is identified, reported, responded to, investigated, and recovered from as quickly as possible. Ensure any appropriate corrective action is taken.

GOVSEC-8

Be able to respond

Be prepared to implement heightened security levels in emergencies or situations where there is an increased threat to your people, information, or assets.

Maintain a business continuity management programme, so that your organisation's critical functions can continue to the fullest extent possible during a disruption. Ensure you plan for continuity of the resources that support your critical functions.

Personnel Security

PERSEC-1

Recruit the right person

Ensure that all people working for your organisation (employees, contractors, and temporary staff) who access Cook Islands Government information and assets:

- have had their identity established
- have the right to work in Cook Islands
- are suitable for having access
- agree to comply with government policies, standards, protocols, and requirements that safeguard people, information, and assets from harm.

PERSEC-2

Ensure their ongoing suitability

Ensure the ongoing suitability of all people working for your organisation. This responsibility includes addressing any concerns that may affect the person's suitability for continued access to classified or unclassified information, assets and locations.

PERSEC-3

Manage their departure

Manage people's departure to limit any risk to people, information and assets arising from people leaving your organisation. This may include:

- remove access rights to systems and buildings
- ensure property is returned
- ensure people understand their ongoing obligations.

Information Security

INFOSEC-1

Design your information security

Design information security measures that address the risks your organisation faces. Your security measures must be in line with:

- the Cook Islands Government Security Classification System
- the Cook Islands Security Handbook
- best practice standards
- any privacy, legal, and regulatory obligations that you operate under.

INFOSEC-2

Check your security measures

Confirm that your information security measures have been correctly implemented, are fit for purpose and meet your needs.

INFOSEC-3

Keep your security up to date

Ensure that your information security remains fit for purpose by:

- monitoring for security events and responding to them
- keeping up to date with evolving threats and vulnerabilities
- maintaining appropriate access to your information.

Physical Security

PHYSEC-1

Design your physical security

Design physical security measures that address the risks your organisation faces. Your security measures must be in line with relevant health and safety obligations.

PHYSEC-2

Check your security measures

Confirm that your physical security measures have been correctly installed and are fit for purpose.

Ensure your physical security measures are used correctly by people.

PHYSEC-3

Maintain your security

Ensure you keep up to date with evolving threats and vulnerabilities, and respond appropriately.

Ensure that your physical security measures are maintained effectively so they remain fit for purpose.

PROTECTIVE SECURITY
CLASSIFICATIONS

The Cook Islands Government has four security classifications that can be applied to confidential information depending on the sensitivity of the information.

There is a number of further markings that can be applied to confidential information to further restrict access to information.

OFFICIAL

Most of the information that is created or processed by the public sector during routine business operations and services. This information is not subject to a heightened threat profile.

RESTRICTED

Government information that could have damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen, or published in the media, but is not subject to a heightened threat profile.

SECRET

Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors. For example, where compromise could seriously damage law enforcement capabilities, international relations or the investigation of serious organised crime.

TOP SECRET

Cook Islands Government's most sensitive information requiring the highest levels of protection from the most serious threats. For example, where compromise could lead directly to widespread loss of life or threaten the security or economic wellbeing of the country or friendly nations.

Further markings can be applied to confidential information, such as...

COOK ISLANDS EYES ONLY

STAFF/PERSONNEL

RELEASABLE TO ...

CABINET

DEPARTMENT USE ONLY

COMMERCIAL

EMBARGOED

LEGAL PRIVILEGE

WITHOUT PREJUDICE

FOR YOUR EYES ONLY

NATIONAL SECURITY COMMITTEE

PROTECTIVE SECURITY

AREAS

The Cook Islands Government has three physical areas for handling information and people.

PUBLIC AREAS

These are unsecured areas including out-of-office working arrangements.

They provide limited access controls to information and physical assets where any loss of information would be unlikely to damage the security or interests of Cook Islands or the privacy of its residents. They also provide limited protection for people.

WORK AREAS

These are low-security areas with some controls. They provide access controls to information and physical assets where any loss could result in prejudice to the maintenance of law and order, impede effective conduct of government or adversely affect the privacy of residents. They also provide some protection for people.

These areas allow unrestricted access for your people and contractors. Public or visitor access is restricted.

SECURITY AREAS

These are security areas with higher levels of security measures in place. They provide access controls to information where any loss could result in serious (Secret) or exceptionally grave (Top Secret) damage to national interests. They may also provide additional protection for people.

Access should be strictly controlled with ID verification, key/card access, and logging of access. People with ongoing access should hold an appropriate security clearance. Visitors and contractors must be closely controlled and have a business need to access the area.

PROTECTIVE SECURITY
ALERT LEVELS

The Cook Islands Government has three colour coded security alert levels. The different levels trigger specific actions to be taken by government organisations based upon their specific response plans.

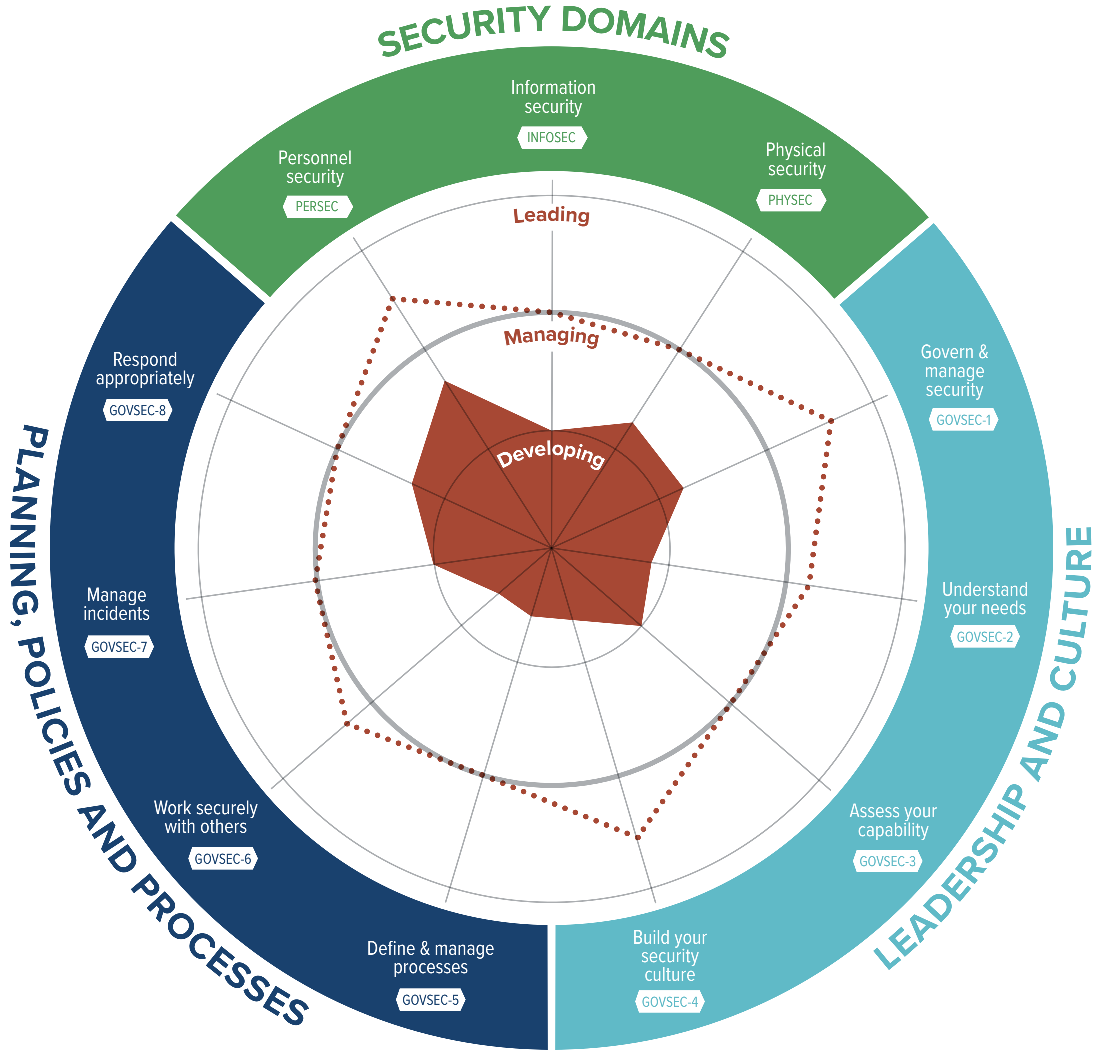
THREAT LEVEL	DESCRIPTION	RESPONSE
GREEN	**LOW RISK** **A threat event is unlikely.** No unusual activity exists beyond the normal concerns.	**Normal – Continue normal operation and awareness.** Localised incidents are managed through standard response procedures.
YELLOW	**MODERATE RISK** **A threat event is possible.** · Increased threat risk including weather, natural, physical, social, or cyber threats · Increased risk of harm to staff or the public · Risk of significant damage to critical infrastructure or IT systems.	**Heightened – Prepare for event and establish countermeasures.** Implement heightened responses for the specific threat as defined in your response plans. Example response actions are: · Doors in night mode / only allow authorised entry and exit · Plan, prepare and communicate with affected people · Issue event watch or advisory warnings to affected people · Increase monitoring of non-essential visitors or contractors · Heighten screening of mail and delivery · Increase monitoring of vulnerable infrastructure or IT systems · Address infrastructure and IT system vulnerabilities · Prepare for critical functions to transfer to alternative sites · Advise police, ambulance, or other emergency services that services may be required.
RED	**HIGH RISK** **A major threat event is imminent or has occurred and countermeasures are insufficient to prevent harm to people, information and/or assets** · Severe weather event or natural disaster · Major internal incident such as fire, flooding, or cyber attack · Potential for, or actual, loss of lives · Widespread exploit, outage, or failure of critical infrastructure or IT systems.	**Exceptional – Respond to event** Implement your exceptional responses for the specific event as defined in your response plans. Example response actions are: · Strict access control measures in place · Lock down, evacuate or close facilities · Isolate, shutdown or enact disaster recovery of affected infrastructure or IT systems · Conduct essential operations at alternative sites · Make staff aware not to come to work · Communicate and coordinate responses; people understand how to respond · Deploy police, ambulance or other emergency services · Prepare for recovery.

PROTECTIVE SECURITY ASSESSMENT TOOLS

Ongoing improvement in protective security requires a cycle of assessing and managing your risks in an everchanging environment. The self-assessment tool enables you to:

- evaluate the effectiveness of protective security practices against good practice guidance
- identify needs for protective security measures
- plan the security areas of focus and actions that will be taken to improve protective security
- report back to the National Security Director as Chair of the National Security Committee on current capability and improvement plans.

The protective security assessment radar provides a quick snapshot of your current security capability mapped against the protective security framework. There are three levels your organisation can achieve; Developing, Managing and Leading Protective Security.



● Current state ⁘ Target state

For additional information or support on the
protective security framework, please contact the
National Security Directorate, Office of the Prime Minister
at nsd@cookislands.gov.ck