


Protective Security Handbook





This guidance has been developed for initial consultation based on preliminary discussions with the Cook Islands National Security Directorate of the Office of the Prime Minister.

It has been designed to be scalable i.e. different agencies can apply settings which work for them and the people they serve. It will use consistent language, aid understanding across the entire public service to enable greater clarity and collaboration.

Personal responsibility

2 | **Everyone who works with government (including staff, contractors and suppliers) has a personal responsibility and duty of care to safeguard the confidentiality, integrity, and availability of Cook Islands Government information and assets that they use.**

Accidental or deliberate compromise, loss or misuse of Cook Islands Government information or assets is a security incident and may lead to damage or harm.

We must learn from security incidents to prevent or reduce the likelihood of future incidents. Repeated poor security behaviour and non-compliance to security policies can lead to disciplinary action, or in serious cases, to criminal prosecution.



Contents

What is protective security	4
<hr/>	
Why security matters	4
<hr/>	
Protective Security Framework	5
Classification System	
Security Areas	
Alert Levels	
<hr/>	
Good security behaviour	9
<hr/>	
How to protect information	15
Classifying information	
Handling information	
<hr/>	
Reporting security incidents	24
What is a security incident	
Report security incidents	



What is protective security

Protective security are the measures taken to protect your people, information, and assets. Protective security encompasses and extends organisational practices such as health and safety, privacy, business continuity, incident management, and emergency and disaster management.

4

This handbook provides people with key principles for good security behaviour and guidelines for how to keep the organisation's people, information and assets secure.

Why security matters

In today's environment, threats to security come from many directions. It is important that organisations have systems in place to reduce their vulnerabilities. Threats may include natural disasters and weather events, violence, damage to organisational property, fraud, theft, espionage and cyber-criminal attacks.



Protective Security Framework

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



SECURITY GOVERNANCE

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

1. Establish and maintain the right governance and 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

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

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

Providing and maintaining a safe and secure working environment.

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

CLASSIFICATION SYSTEM

The Cook Islands Government has four security classifications that should be applied to confidential information depending on the sensitivity of the information. All other information is considered unclassified.

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.

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 the 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.



SECURE 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.

ALERT LEVELS

The Cook Island 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.



LOW RISK

A threat event is unlikely.

- No unusual activity exists beyond the normal concerns.

8



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.



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 i.e. Cyclone
- 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.



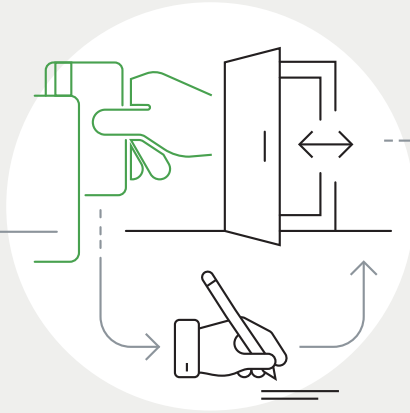
Good security behaviour

You play a vital role in helping to protect organisational assets and keeping the organisation and its people safe and secure. By following good security behaviours, you will make a big difference in reducing the organisation's vulnerability to threats.

-
- ☑ Understand and follow your organisations security policies and procedures
 - ☑ Understand what information you can and cannot share with whom
 - ☑ Be aware of your surroundings when discussing or working with sensitive material
 - ☑ Report any suspicious activity or security incidents.
-

This section describes the behaviours you should follow under different scenarios.

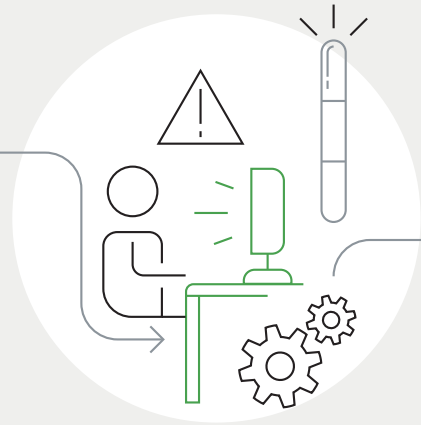




Arriving and departing your workplace

Entrances and exits are the first and last point of protection for the organisation.

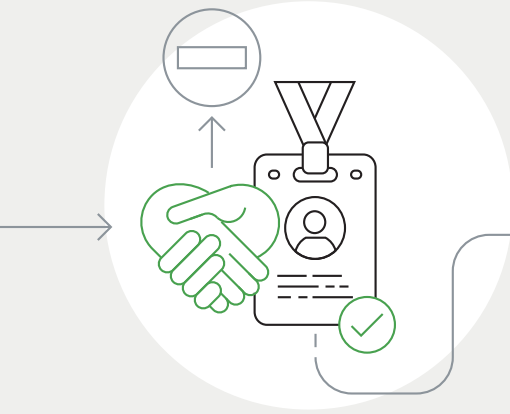
- ☑ Be alert to suspicious activity and report anything unusual
- ☑ Follow correct entry and exit procedures (e.g. swiping your pass, signing in) and ensure others do the same.



In and around the workplace

In the workplace, people need to be security conscious to minimise the chance of accidental breaches and to spot suspicious activity.

- ☑ Be observant for security incidents and report them no matter how minor you think it is – we only learn and improve through resolving incidents
- ☑ Don't discuss sensitive subjects or display sensitive information in areas where visitors are likely to be
- ☑ Clear your desk of sensitive information at the end of the day – where necessary, lock it away
- ☑ Dispose of sensitive information appropriately
- ☑ Be aware of what to do when your organisation faces an increased alert level.

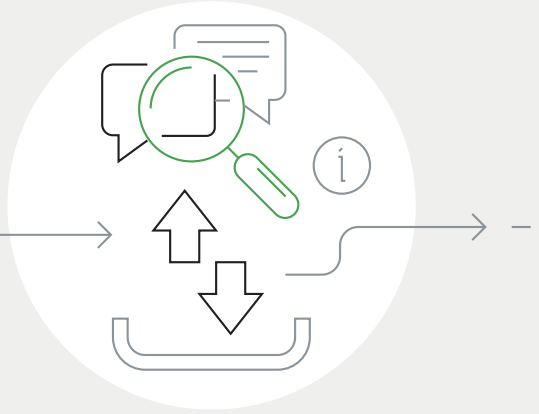


Receiving a visitor

Visitors can be a risk to your security if not managed properly. Take responsibility for your visitors when they are onsite.



- ☑ Verify the visitor's identity and confirm that their visit is expected
- ☑ Ensure your visitors are signed in, out, and accompanied when appropriate
- ☑ Ensure visitors understand your relevant security procedures
- ☑ Keep visitors away from areas they may not be authorised to go.



Handling queries

If you regularly deal with customers, partners or the public, you need to be vigilant about security, even if you know the person well.



- ☑ Verify the person's identity before sharing information or working with them – don't make assumptions about their legitimacy or credentials
- ☑ Don't give away too much detail when requested – ask yourself 'Do they really need to know this?'
- ☑ Be aware of how people may trick you to get information from you.



Using computers and devices

Organisational ICT systems hold a wealth of information which can be a target of attack. Using devices responsibly and securely can reduce the risk of cyber-attack.



- ☑ Use unique and complex passwords and change it immediately if you suspect it has been compromised. Do not share your password with others
- ☑ Lock your device or computer terminal when leaving it unattended. Protect mobile devices from loss or theft
- ☑ Be aware that electronic devices and media may contain viruses and malware that may affect your network
- ☑ Avoid using work devices and email for personal use
- ☑ Be cautious of free WiFi networks.



Your online presence

In an increasingly digital world, organisations may conduct activities online. Increased digital presence can present an increased security risk if not managed well.



- ☑ Get official approval before posting anything online
- ☑ Be aware of becoming a target if you are linking yourself with your organisation online.



Outside of work

Our work lives inevitably spill over into our personal lives such as in social situations or interacting online. These situations can put us at risk.

- ☑ Keep personal and work lives as separate as possible
- ☑ Limit communication about any details of the sensitive work you do
- ☑ Report any suspicious activity or people trying to get sensitive information from you.



Travelling overseas

You are under greater risk when travelling overseas, whether personally or professionally.

- ☑ Consult with your organisation's security team to understand the risks you face and ensure you and your devices are secure
- ☑ Be aware of your environment, ensuring all conversations are conducted in a private and secure area and your devices and documents are always kept secure
- ☑ If you suspect your device has been compromised, turn it off, and return it to your security team.



Hiring and managing others

Insiders are the biggest risk to the organisation. You must ensure that they are trustworthy to handle information securely.



- ☑ Undertake appropriate pre-engagement security checks when hiring
- ☑ Set the right behaviour expectations ensuring they attend induction, security awareness training and briefings and understand their responsibilities
- ☑ Model good security behaviour and watch out for poor security behaviour from others
- ☑ When people change roles or leave the organisation, use robust procedures to manage their departure or change.



Procuring products and services

Often organisations rely on suppliers to deliver products and services. These suppliers become an extension of your organisation and broaden the risks you're exposed to.




- ☑ Understand the risks that you could face from your suppliers – for example: insecure systems, malicious insiders, unknown supply chains, or sub-contractors with poor security practices
- ☑ Ensure suppliers understand their responsibilities to protect your information and assets
- ☑ Assess the supplier and sub-contractor capability and personnel suitability before awarding contracts
- ☑ Build assurance and continuous improvement into your contracts.



How to protect information

This section provides guidance on how to classify, protectively mark, and handle classified information. The handling guidance defines how to correctly store, file, use, copy, share, remove, transport, archive, and dispose of sensitive information.

KEY PRINCIPLES

- ☑ All information has value and requires an appropriate degree of protection
 - ☑ Access to classified information should only be granted based on a genuine 'need to know'. Don't over-classify. This will ensure those who need it, have access to it
 - ☑ Information and assets received from or exchanged with external partners should be protected in accordance with any relevant legislative, regulatory, or international agreement requirements
 - ☑ Use sound online security practices. Stay abreast of best practice online behaviours when using mobile devices and working online.
- 

CLASSIFYING INFORMATION

The classification and additional markings should be added as follows to all documents:

- Centred top and bottom of each page
- All Caps
- Bold
- In the following colours:

OFFICIAL

Marking is optional

RESTRICTED

Black

SECRET

Blue

TOP SECRET

Red

ADDITIONAL MARKINGS

Additional protective markings can be applied to warn people that the information has specific handling requirements.

Following are a small set of standard markings. Your organisation needs to define the additional set of protective marking relevant to your requirements.

COOK ISLANDS EYES ONLY

Used for material where access to information is restricted to Cook Islands residents with an appropriate security clearance and on a need-to-know basis.

CABINET

Used for material that will be presented to, and/or require decisions by Cabinet.

[DEPARTMENT] USE ONLY

Used for material intended only for use within the specified department(s).

PERSONAL

Used for material relating to an identifiable individual, where inappropriate access could have damaging consequences.

COMMERCIAL

Used for commercially sensitive processes, negotiations, or affairs.

LEGAL PRIVILEGE

Used for material that is subject to legal privilege.



CLASSIFIED DOCUMENT REGISTER

A Classified Document Register (CDR) records the creation, ownership, location, and destruction details for all TOP SECRET information produced, copied, or received by the organisation.

Your organisation may also choose to use the CDR for SECRET information and for risk mitigation of lower classified information.

HANDLING INFORMATION

Following are the requirements for storing, filing, using, transporting, and disposing of classified material.



STORE AND FILE

Below are the requirements for storing and filing sensitive information in your organisation based upon its classification.

OFFICIAL



- Stored in any area commensurate with the sensitivity of the information
- Physical folder is uncoloured.

RESTRICTED



- Stored in Work Area under single barrier and/or lock and key
- While in use, material / equipment is not left unattended – secured and/or locked away
- Physical folder should be marked RESTRICTED.

SECRET



- Stored in locked cabinet in Work Area or Security Area using approved security furniture
- Physical material is immediately placed in a folder
- Physical folder should be marked SECRET.

TOP SECRET



- Stored in a strictly controlled, locked, and monitored Security Area (e.g. strong room or safe)
- Physical material is immediately placed in a folder
- Physical folder should be marked TOP SECRET.



USE, COPY, AND SHARE

Below are the requirements for using, printing, copying and sharing sensitive information in your organisation based upon its classification.

OFFICIAL



- Clear desk and screen policy to protect against accidental or opportunistic compromise
- Obtain owner approval prior to printing, copying or sharing
- Sensitive materials should be kept to a minimum
- Social media and online sharing is not permitted except through approved communication and media authority.

RESTRICTED



Including Official requirements:

- Printing, copying or sharing may be prohibited by the originator
- Conversations and meetings are held only in approved and secured areas
- Copies should not be left unattended on printers and devices.

SECRET



Including RESTRICTED requirements:

- Consider recording copies in CDR
- Shared only with people with appropriate security clearance and valid need to know
- Secure telephones, video, conference equipment
- Material assessed for redaction before disclosure
- Printers and devices are secured before use.

TOP SECRET



Including SECRET requirements:

- Accessed only within an approved security area
- All copies in any form (e.g. physical, electronic, media) are numbered, recorded and tracked in CDR
- Disclosure assessment undertaken before approval given
- Approval authorising copying, printing, or sharing recorded in original file
- Printer and device access and use is strictly controlled and supervised.



REMOVE OR TRANSPORT

Below are the requirements for removing or transporting information from your organisation.

OFFICIAL

Authorised by the owner of the information.

In accordance with organisation policies and procedures.

RESTRICTED

Including OFFICIAL requirements:

Authorised by the originator (may be the same person as the owner).



REMOTE WORKING

- Prevent overlooking and overhearing.

Including OFFICIAL requirements:

- Stored under lock and key.



REMOVABLE MEDIA

- Can be used based upon your organisations policies.

- Appropriately encrypted.



MOVING BY HAND

- Does not requiring special enveloping or folders within physical location
- Single envelope between locations for sensitive material.

- Single envelope
- Must always be in personal custody of an authorised person.



TRANSPORTING BY POST/COURIER

- Single envelope
- Include specific addressee and return address
- Never mark classification on envelope.

- Consider reputable mail or courier with 'track and trace' service.

SECRET



Including RESTRICTED requirements:

Authorised by the CSO.

TOP SECRET



Including SECRET requirements:

Authorised by the Head of Ministry and Chief of Staff as Chair of National Security Committee.

Including RESTRICTED requirements:

- Risk assessment to determine need and identify appropriate security controls
- Approved security storage.

Including SECRET requirements:

- Exception is granted and risks have been accepted by senior management.

- Appropriately encrypted.

- Appropriately encrypted.

- Double enveloped and sealed in a tamper-evident manner
- Evidence of receipt.

- Movement recorded in CDR.

- Double enveloped and sealed in a tamper-evident manner
- Approved government or commercial courier
- Track and trace or evidence of receipt.

**Do not send by post or courier.
Transport by hand only.**

OFFICIAL

RESTRICTED



TRANSPORTING OVERSEAS

- Single envelope
 - Include return address
 - Never mark classification on envelope.
- Consider reputable mail or courier with 'track and trace' service.



ELECTRONIC TRANSFER (E.G. EMAIL, INTERNET, ONLINE APP)

- Communication of recipient's legal and destruction obligations if the incorrect party receives it.
- Risk assessed
- Password protection and encryption may be required.



ARCHIVE OR DISPOSAL

Below are the requirements for archiving and disposing of information in your organisation based upon its classification.

OFFICIAL

RESTRICTED



- Archival of public records is subject to relevant Cook Island law.
 - Dispose with care using approved commercial disposal products and services.
- Including OFFICIAL requirements:*
- Physical waste should be kept separate from unclassified waste and secured under same precautions as Filing / Storing
 - Must not be disposed by standard rubbish or recycling collection unless it has already been through an approved destruction process (e.g. shredding, pulping, burning, disintegration)
 - Disposal of electronic media should make reconstruction highly unlikely.

SECRET



- Double enveloped and sealed in a tamper-evident manner
- By authorised person only (with appropriate security clearance) or diplomatically accredited courier
- Track and trace or evidence of receipt.

- Appropriately encrypted
- Evidence of receipt.

TOP SECRET



- Security cleared diplomatically accredited courier only
- Movement recorded in CDR.

- Appropriately encrypted
- Movement recorded in CDR.

SECRET



Including RESTRICTED requirements:

- Use only approved service providers, products and destruction processes
- Media that has held SECRET information must be declassified by approved declassification and disposal processes.

TOP SECRET



Including SECRET requirements:

- Verify material is complete (all pages)
- Media that has held TOP SECRET information cannot be declassified and must be sanitised and destroyed by approved disposal process
- Supervise and witness destruction by an authorised officer
- Disposal is recorded in CDR.



Reporting security incidents

It is everyone's responsibility to report incidents. When an incident happens, act quickly to reduce any impact and prevent further harm. Follow your organisation's incident reporting and response procedures.

24

-
- ☑ Report any incident no matter how minor it may seem
 - ☑ Act quickly to reduce impact
 - ☑ Learn from repeated infringements
 - ☑ We all make mistakes, better to report incidents yourself than be reported on.



WHAT IS A SECURITY INCIDENT?

A security incident is an event, breach, or attempted breach of protective security policies or procedures.

There are three different intents that can cause security incidents, accidental, negligent, or a deliberate act. Each of these can compromise the security of the public, your organisation, its people, information or assets.

ACCIDENTAL

A failure to observe your protective security requirements or policy.

NEGLIGENT

A negligent or reckless action.

DELIBERATE

A deliberate malicious act.

IMPACT OF SECURITY INCIDENTS

The following examples highlight security incidents that might be seen to have a low impact, however, can quickly lead to incidents that have a high impact on the security of the Cook Islands Government, its people, information, or assets.



LOW IMPACT

- Key cards lost or left insecure
- Classified material left in UNCLASSIFIED waste or recycle bins
- Classified material not properly secured or stored
- Access doors wedged open for convenience without supervision that does not lead to higher impact incidents.

MEDIUM IMPACT

- Theft, attempted theft or loss of assets
- Compromise or loss of classified information
- Tampering with alarms, keys, windows, or doors
- Suspicious contact from unknown individual
- Suspicious email with attachments and links
- Computer viruses
- Information corruption
- Disruption or damage to services or equipment.

HIGH IMPACT

- Physical event – e.g perimeter, fire, water, electrical
- Social – e.g. public activity, event, protest
- Espionage
- Large scale cyber threat
- Weather or natural events.

REPORT SECURITY INCIDENTS

Your security team maintains a register of all reported security incidents. Make sure you keep them aware and informed of all security incidents.

Include the following details when you report a security incident:

- The date and time of the incident or when it was discovered
- The location of the incident
- Brief details of the incident
- What may have been compromised
- Your initial assessment of damage or harm
- What actions you have already taken
- Who was involved in the incident, if known
- Your name and contact details for follow up.

If you have reported an incident, ensure you also report any updates or changes to the situation.

For incidents requiring emergency service (i.e. Police, Ambulance, Fire) response, call 999.



For additional information or support on the protective security framework, please contact the National Security Directorate, Office of the Prime Minister by email or phone:

nsd@cookislands.gov.ck

+682 25494

