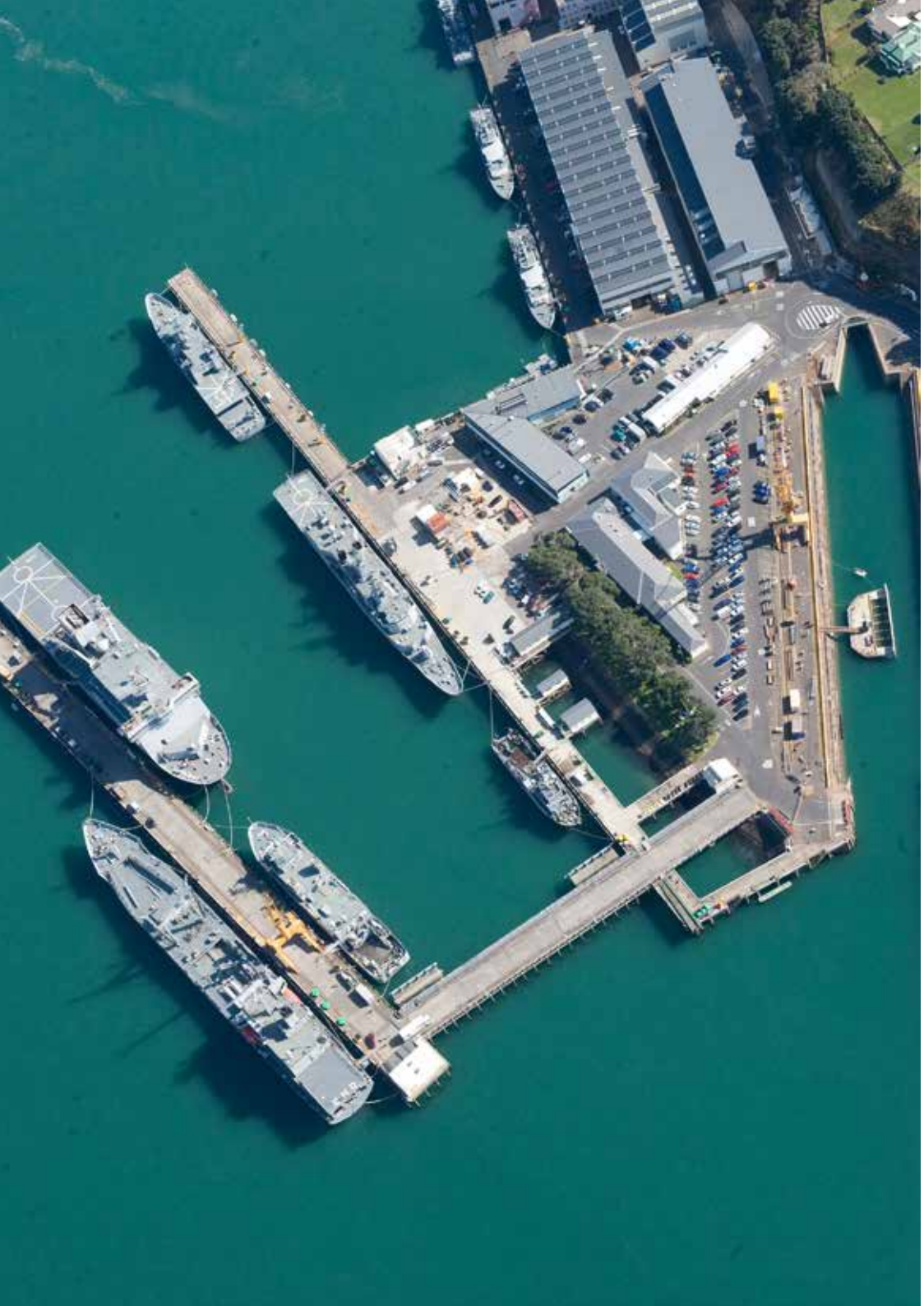
New Zealand
DEFENCE
FORCE
Te Ope Kātua O Aotearoa

Defence Security

Facility Security Officer Guide

Version 2.0 | October 2019



Introduction

Having a contract with the New Zealand Defence Force (NZDF) comes with a legal obligation to safeguard all classified information and assets.

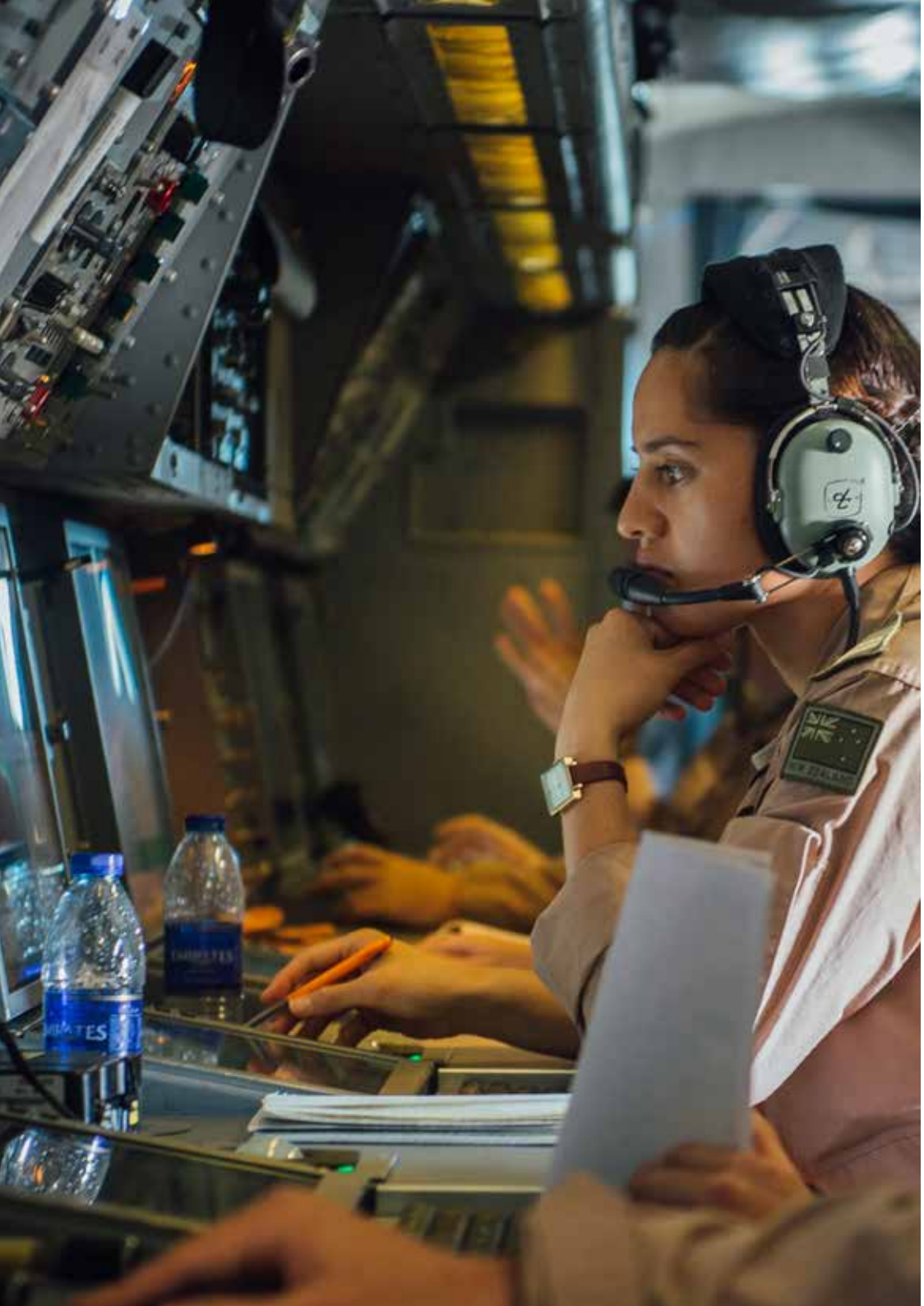
Every Defence contractor plays an important role in helping us to maintain the security of Defence personnel, information and facilities, and in most cases they will need to be accredited under the Defence Industry Security Programme (DISP).

This accreditation requires you to meet New Zealand Government and NZDF standards so that Defence information and assets are protected to the same level we require of NZDF staff.

As part of that accreditation, every DISP company is required to appoint a Facility Security Officer (FSO) to work with NZDF to ensure the security requirements that come with the individual contract are fulfilled.

This guide outlines the responsibilities of the FSO role and Deputy FSO, as needed.

The contents of the guide are UNCLASSIFIED.



The importance of your role

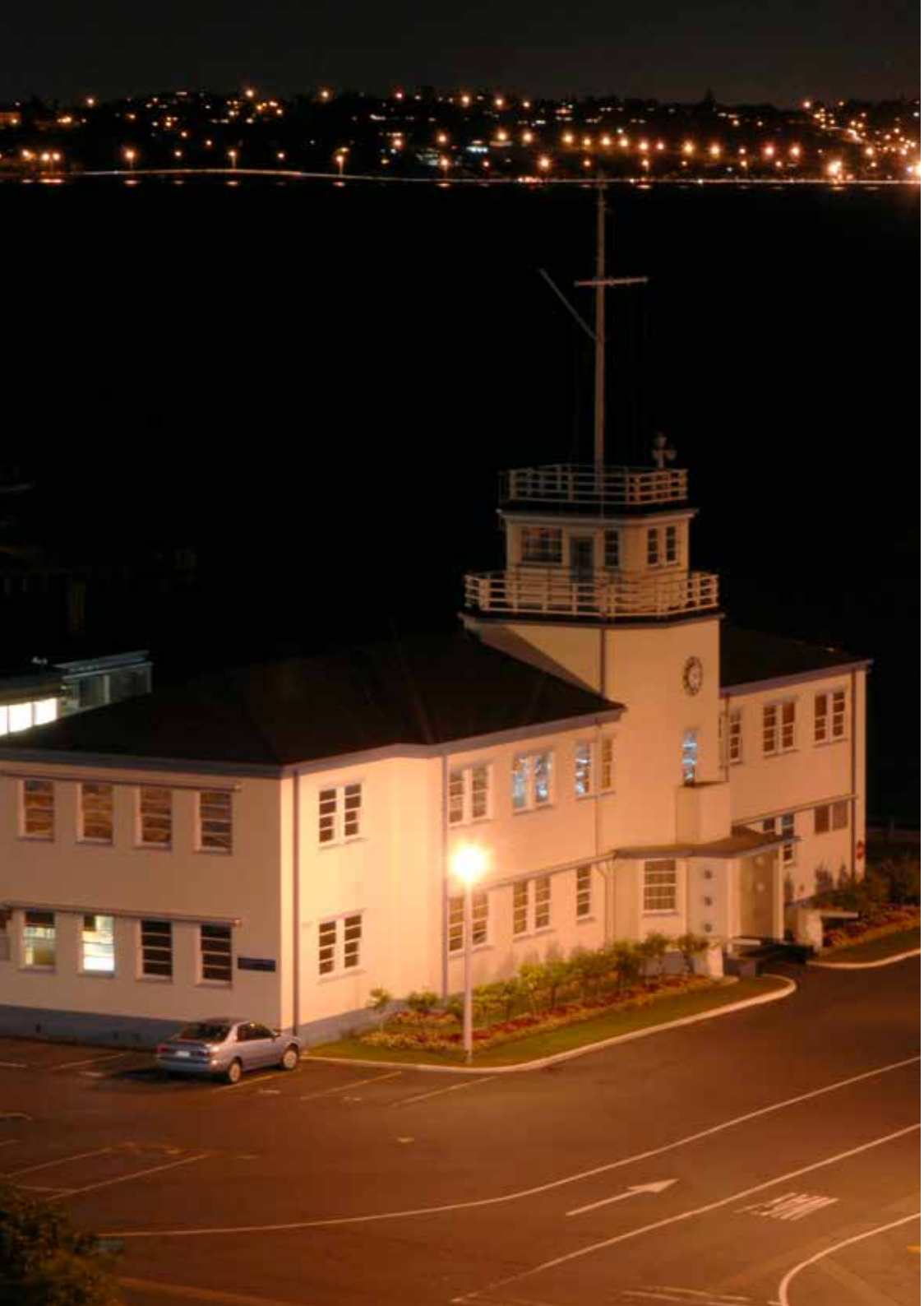
As your company's FSO/Deputy FSO, you are required to manage or oversee the security functions and activities related to the NZDF contract or contracts, on behalf of your company's management.

It's an important role. You are NZDF's key security contact and we rely on your help to ensure the mandatory government requirements under your contract are met.

We appreciate that being appointed your company's FSO/ Deputy FSO will likely add extra responsibilities to your already busy work-life, and we want to provide you with as much support as possible.

A lot of your responsibilities are about putting processes and systems in place to ensure you can easily complete the individual tasks required of you.

We have produced resources to support you in that, which are available through our Dropbox link listed in Resources near the end of this guide.



Your responsibilities as FSO/Deputy FSO

1. Ensure all company employees know their security responsibilities

It is your role as FSO/Deputy FSO to provide security-cleared employees with a briefing on their individual responsibilities under the DISP.

We have prepared a two-part PowerPoint presentation – both slides and presenter notes – to guide you on the content and delivery of this. You are able to tailor the briefing to the group you are presenting to, and to add in specific company information.

Once cleared staff members receive their Security Clearance they will need to receive their initial security briefing. Security-cleared employees are to read the "Summary of Offences Related to Wrongful Disclosure or Use of Official Information" contained in your Security Practices and Procedures (SPP) document that your company signed as part of the DISP accreditation process.

Employees must complete the Briefing Acknowledgement within the SPP, which will need to be kept with your DISP accreditation documents before any access to classified material can be granted.

Employees must receive a security briefing every 12 months, and a record of who has been briefed must be kept by you in a Facility Security Register (FSR).

See page 11 for more information on the FSR.

2. Inform NZDF of any changes that could affect your company accreditation

Your company's management is required by their contract to inform you as FSO/Deputy FSO of any proposed changes that could affect the company's accreditation, or its ability to safeguard Defence material.

You are required to advise the NZDF DIIS team, as soon as possible, of any changes to:

- Company ownership
- Major shareholders
- Business or operating name and address
- The personal circumstances of any security-cleared employees (using the 'Change of Circumstance' form)

All security-cleared employees are to report to you as FSO/ Deputy FSO:

- Any changes to their personal circumstances (such as marriage, divorce, de-facto relationships starting or ending, or any name change)
- Any situation, incident, or change of condition that may affect the company, or directly or indirectly place classified information or equipment at risk
- Any unusual contact of potential security significance (such as a persistent friend request on Facebook from someone they don't know)
- Any confirmed or suspected sabotage, espionage or subversive activities
- Any loss, compromise or suspected compromise of classified information or equipment

- Any industrial espionage, fraudulent or other criminal activity
- Any loss or theft of commercially sensitive material and/or important items
- Any evidence of tampering with or improper transmission of classified information or equipment
- Any other suspected or confirmed security breaches, incidents or perceived security deficiencies

3. Provide security advice to management and employees

It's your responsibility to provide advice to all cleared company personnel regarding your company's security responsibilities and to make sure everyone is abiding by the rules of your DISP accreditation.

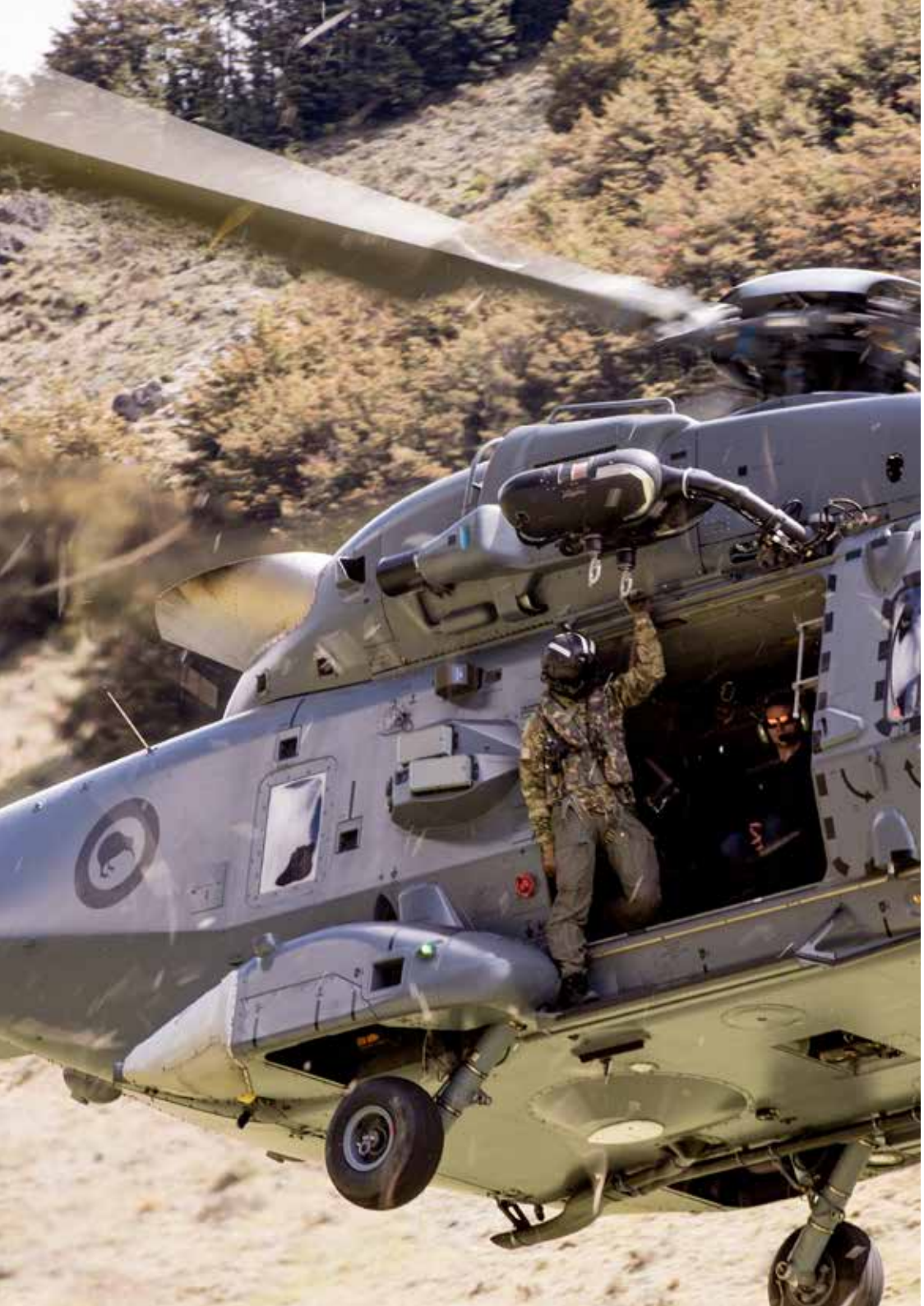
This can include, but is not limited to:

- Personnel clearances
- Facility standards
- Accreditation limitations
- Travel advice
- Managing/disposing of classified documents
- Security incidents

4. Develop, implement and review the Security Practices and Procedures (SPP) document

The SPP MUST be maintained and updated annually by the FSO/ Deputy FSO to ensure that it reflects:

- Employee responsibilities and appointments
- Current Defence security policy and procedures
- Security conditions relevant to classified activities the DISP member is involved in



5. Develop and maintain a Facility Security Register (FSR) detailing all records

The Facility Security Register template is available on request from DIIS in digital copy or via our Dropbox link listed in Resources.

The FSR is to contain, at a minimum:

- FSO/DFSO and any other security appointment details
- Changes to your company Security Practices and Procedures document
- Security surveys and self-inspections
- Employee personnel security clearances
- Any overseas travel by staff security-cleared to CV or higher
- Security briefings and de-briefings to employees
- Security incidents
- Security education and training conducted
- Other items of security importance, depending on your accreditation, should be attached to the FSR document, for example; Security Container checks, Security Key musters, and Electronic Security System services

6. Develop and implement a security education programme

You will need to develop and implement an ongoing programme of security education and awareness for all security-cleared employees.

You must maintain a record of any security seminars or presentations delivered to DISP members for each employee in the FSR (at minimum 1 hour annually).

7. Security breach/Incident reporting

You will be responsible for promptly advising DDS of any security incidents and conducting a preliminary inquiry, including initial interviews, into suspected or confirmed security breaches. Details of the preliminary inquiry must be recorded in the FSR.

8. International travel reporting

You must advise DIIS, via email, the dates and locations of all international travel (this includes both private and business) to be taken by staff members cleared to CV or higher. DIIS will provide an overseas travel briefing to the FSO/Deputy FSO if the destinations include any Country Representing a Special Security Risk (CRSSR), and advise if any further actions are required.

9. Advise NZDF of visits

You will be responsible for preparing visit notifications for security-cleared employees requiring entry to sensitive or controlled areas of Defence or Defence Contractor establishments, both in New Zealand and overseas.

10. Disposal of classified waste

You will arrange for the disposal of classified waste by secure means, as prescribed by NZDF. DDS or the NZDF Unit Security Officer (USO) responsible for your company's area of work will be able to provide advice on this.

11. Manage access to security containers and keys

You must maintain a register of all lock combinations, keys to security containers and classified work areas, and key holders.

12. Security inspections and checks

If your company has a Facility Accreditation, you must conduct:

- Regular security inspections
- Regular security key musters
- Random security checks

13. Personnel security clearances

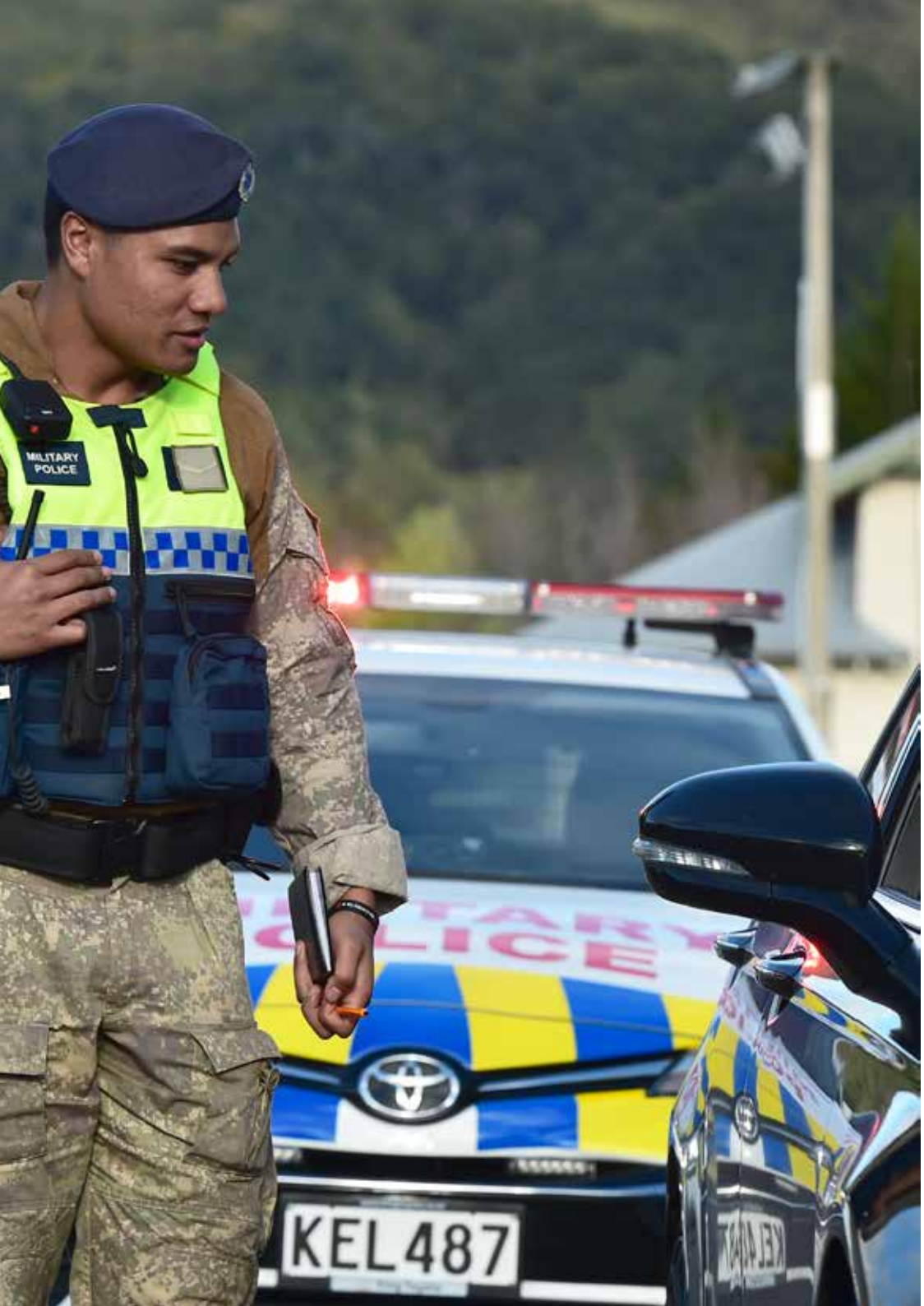
You will be responsible for facilitating personnel security clearances and associated actions with the Industry Vetting department at DDS (email: IndyVet@nzdf.mil.nz).

14. Approach DDS to arrange a specific threat assessment for a particular facility or project.

Example: A threat assessment may be necessary in situations such as an exhibition, open day or other event when the threat to the DISP member may be increased.

15. Security self-assessments

You will be required to conduct a self-inspection survey of security matters annually. DIIS will provide you with the survey template and the results of this survey are to be sent back to DIIS upon completion.



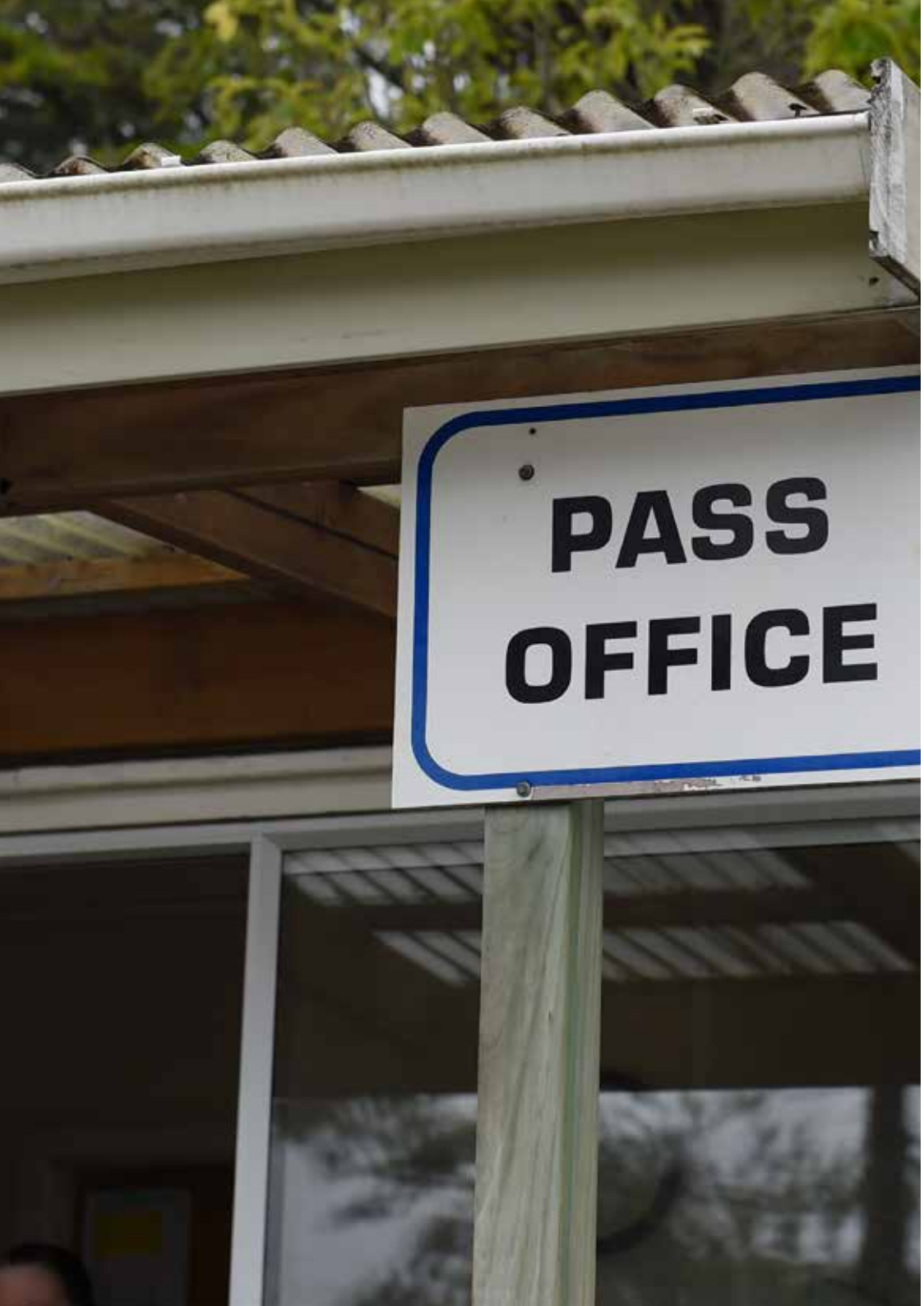
Why Security matters

Security threats to both the NZDF and New Zealand are real and increasing.

In today's connected world, our geographic isolation and small size no longer protect us from being of interest to foreign intelligence agencies and other adversaries.

Not every security risk is within our control, but we can mitigate potential risks by being vigilant – not just in terms of our own behaviours but also the behaviour of others.

Security matters because poor security practices can have serious ramifications. They not only can put classified Defence information at risk, they can also put people at risk.



Resources

We have been able to put information and forms into a Dropbox, accessible through the following link:

https://www.dropbox.com/sh/1fjpau1gq266jzh/AAD42CoNxI2nVi2UYU8JJNgWa?dl=0

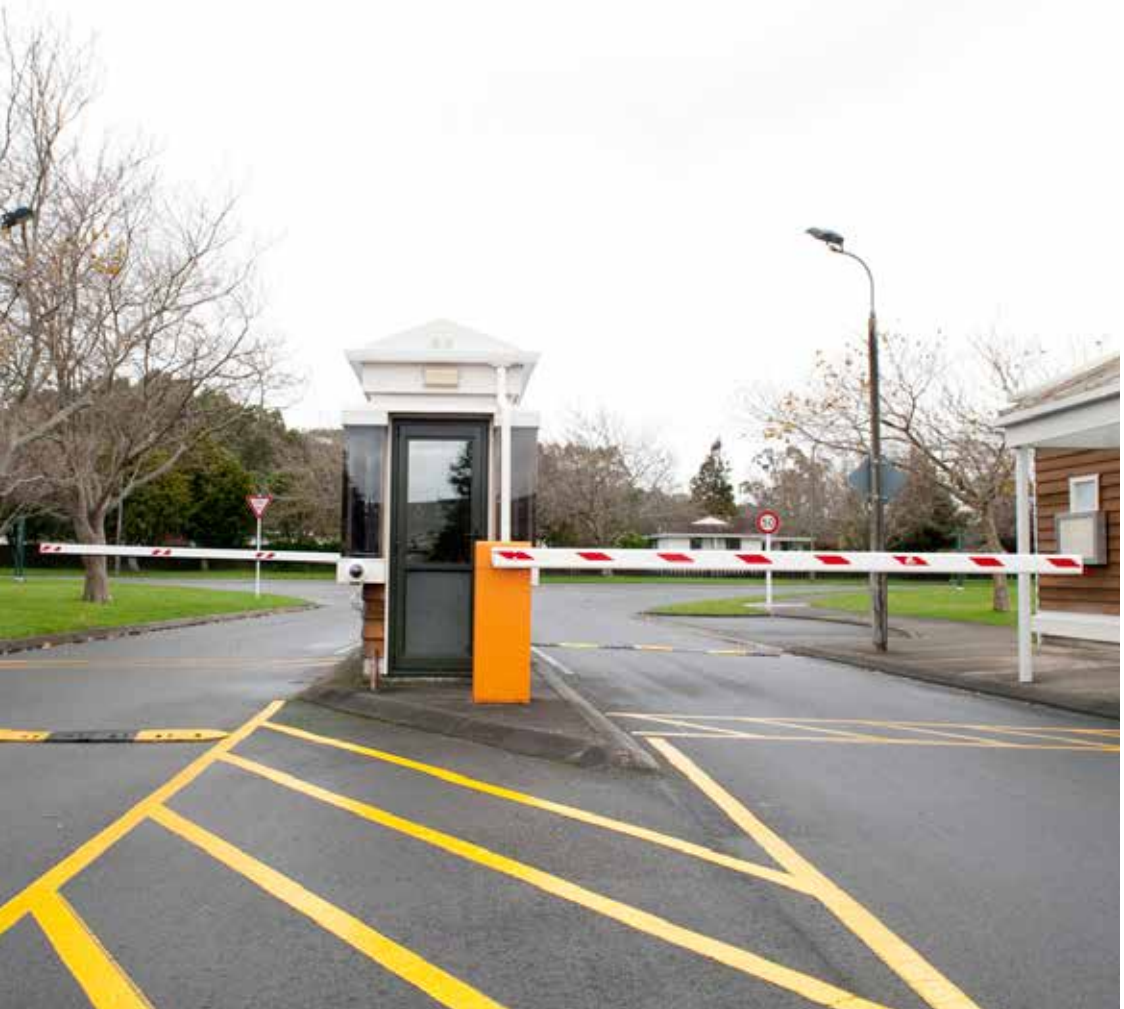
or this short URL:

http://bit.ly/DISP-0219

You will find it divided into three sections – Information, Forms and Resources.

Please note that you will not be able to access this through DIXS – you will need to use your own company's internet.

We hope this makes it much easier for you to access the security information, resources and forms you need, which will be kept up to date with anything new that DIIS creates or that may be useful to you as FSO/Deputy FSO.



How we can support you

Please do not hesitate to contact the DIIS team by emailing DIIS@nzdf.mil.nz with any queries you may have. We are here to support our company FSOs/Deputy FSOs in any way we can.

Please remember to report any suspicious behaviour or activities by calling military or civilian Police first, then contacting DIIS.

A FORCE FOR
NEW ZEALAND