TE OPE KĀTUA O AOTEAROA
DEFENCE FORCE

DEFENCE INDUSTRY SECURITY PROGRAMME GUIDE

Updated May 2025

02

FOREWORD

The mission of the New Zealand Defence Force (NZDF) is to secure New Zealand against external threat, to protect our sovereign interests, including New Zealand's Exclusive Economic Zone, and to be able to take action to meet likely contingencies in our strategic area of interest. This requires the NZDF to maintain disciplined combat-ready military forces that are available at short notice.[1]

Private companies, contractors and service providers engaged by the NZDF have a crucial role to support and enable this mission. Additionally, our contracted partners also directly contribute to maintaining a robust security posture, which safeguards the NZDF's people, information, facilities and capabilities from security threats.

This Defence Industry Security Programme (DISP) Guide has been compiled to assist any commercial entity that is considering a contract with the NZDF. It may also be a useful reference for companies that already hold a contract with the NZDF. It provides an overview of the New Zealand Government Protective Security Requirements (PSR) and the NZDF policies that you will need to comply with. Additionally, it outlines your security responsibilities when working with the NZDF as a member of the DISP.

The Industry Security team in Defence Security are available to provide any further advice that may be required regarding the content of this guide, or for obtaining DISP accreditation. Please feel free to contact them at IndustrySecurity@nzdf.mil.nz.

We look forward to working with you.

Group Captain Karl Harvey
Director, Defence Security
New Zealand Defence Force

28 May 2025

[1] NZDF Statement of Intent of 24 September 2024, p.10.

Contents

THE DEFENCE INDUSTRY SECURITY PROGRAMME

Introduction

If your company has a contract with the NZDF that requires access to classified NZDF information, IT systems, facilities, capabilities or equipment, you are likely to require Defence Industry Security Programme (DISP) Accreditation. DISP Accreditation provides assurance to the NZDF that contracted partners comply with the requisite security policies.

The DISP is sponsored by Defence Security and is managed by the Industry Security (INDYSEC) team. As soon as the details of your contract with the NZDF are known, the INDYSEC team will work with you to assess your DISP accreditation requirements.

If DISP accreditation is required, the INDYSEC team will guide you through the process, provide access to relevant NZDF policies, and may inspect your facilities for compliance. The INDYSEC team will also provide security advice, information and compliance checks throughout the tenure of your contract with the NZDF.

Security Policy

The New Zealand Security Intelligence Service (NZSIS) sponsor the New Zealand Government Protective Security Requirements (PSR). The PSR is a framework for managing security effectively across New Zealand Government agencies. It outlines New Zealand Government expectations for personnel, information and physical security. Alignment with the PSR is mandatory for the NZDF. See www.psr.govt.nz for more details.

In accordance with the PSR, each government agency is responsible for implementing its own security policies that are aligned to the PSR. NZDF's security policies are contained in Defence Force Orders (DFOs) and Defence Force Instructions (DFI's). All companies contracted to the NZDF are required to comply with these security policies in the conduct of their business with the NZDF. Access to relevant NZDF security policies will be provided as part of the DISP Accreditation process.

When do you need DISP Accreditation?

Your company (or other commercial entity) will need to be DISP-Accredited if your contract with the NZDF involves:

- Accessing Defence Areas or classified material for more than six months;
- Developing, storing, or handling any protectively-marked[2] material – either in hard copy or on an IT system;
- Providing a guard force or security services to the NZDF;

[2] Protectively-marked material is official information and/or equipment that requires extra protection against unauthorised or accidental disclosure or use. It is assigned a classification level under the New Zealand Government Security Classification System at either RESTRICTED, CONFIDENTIAL, SECRET or TOP SECRET (see pages 9 & 10 for more details).

- Storing, transporting, handling or managing NZDF weapons, munitions or other sensitive items; or
- Hosting any NZDF data on your own company's IT system and/or within your own company's premises.

The DISP Flow Chart at page 13 of this guide can be used to help identify whether or not your company may require DISP Accreditation.

Types of DISP Accreditation

There are three types of DISP accreditation:

- **Personnel Accreditation** – A Personnel Accreditation certifies that your employees have obtained the appropriate Security Clearance for the access that they require to fulfil their contracted business with the NZDF (see page 10 for more details on Security Clearances). A Personnel Accreditation also verifies that your company has the requisite security appointments, processes and procedures in place.

- **Facility Accreditation** – Your company will require a Facility Accreditation if your contract involves accessing, creating, handling or storing protectively-marked material at your own business premises. A Facility Accreditation ensures that your facility complies with the requisite Physical Security standards to hold material of this nature.

- **Information and Communication Technology (ICT) Accreditation** – Your company will require an ICT Accreditation if your contract requires you to:
  - Host NZDF classified data on your company's own IT system; or
  - Install a NZDF IT system within your own company premises.

- Note that obtaining a Personnel Accreditation is a pre-requisite to obtaining a Facility Accreditation, and that both are a pre-requisite to obtaining an ICT Accreditation.

DISP Eligibility Requirements

To be eligible for DISP Accreditation, your company will first need to meet the following requirements:

- Have a signed contract with the NZDF[3];
- Have a justified and valid need to access protectively-marked NZDF material in order to fulfil the requirements of your contract with the NZDF;
- Have a NZDF sponsor for your contract identified;
- Not be under foreign ownership, control or influence to the extent that granting accreditation would be against New Zealand's national interests;
- Have a company-specific security manual for staff that has been approved by Defence Security;
- Have signed a Security Agreement with the NZDF; and

[3] Note that bespoke arrangements can be made for companies that require access to classified material as part of the commercial tender process. Contact IndustrySecurity@nzdf.mil.nz if this applies.

- Have appointed a Facility Security Officer (FSO), who will be your company's point of contact for security matters.

Obtaining DISP Accreditation

The first step is for your company to secure a contract with the NZDF. The process to obtain a DISP Accreditation does not start until this occurs.[4]

Once you have a signed contract, the INDYSEC team will assess your company's DISP accreditation requirements in consultation with your appointed representatives. This will be based on the nature of your business with the NZDF and your access requirements.

You will be asked to fill out:

- A form to nominate a FSO (and a Deputy FSO if required) who will be responsible for fulfilling DISP requirements;
- A Security Agreement;
- A Security Practices and Procedures document that sets out the detailed security requirement you will need to fulfil; and
- Relevant Security Clearance forms for each employee that requires access to protectively marked NZDF material.

If a Facility Accreditation is required, a Security Risk Assessment of your premises will be conducted by the INDYSEC team. This will specify any additional security controls that you may need to install prior to storing classified NZDF material. Typical examples are installing an approved safe or approved security locks on doors.

Responsibilities Once DISP-Accredited

The Chief Executive, Managing Director or Company Principal of your company is responsible for ensuring compliance will all relevant NZDF security policies. This includes requirements to:

- Appoint and support a FSO, and where relevant, an Information Security Officer. Both roles may also need to have deputies appointed;
- Implement and maintain the security controls specified by Defence Security;
- Ensure the FSO develops, implements and continuously reviews your organisation's security policies;
- Proactively managing security and fostering a robust security culture within your organisation;
- Inform the NZDF of any proposed changes in your company, such as ownership, location, or structure to inform a re-evaluation of DISP compliance;
- Meet all costs associated with implementing the security measures specified by the NZDF;

[4] Note that bespoke arrangements can be made for companies that require access to classified material as part of the commercial tender process. Contact IndustrySecurity@nzdf.mil.nz if this applies.

- Dedicate time for regular employee security awareness education and training; and
- Ensure that protectively-marked NZDF material is not disclosed or released to any third party without the prior approval of the NZDF.[5]

Security Education and Training

Your employees need to understand why the protection of NZDF information and assets is important, and the potential wide-reaching ramifications of a security breach. Accordingly, security education and staff training is an essential part of your responsibilities under the DISP.

Staff who understand the importance of their security responsibilities, and the part they play in implementing the required security measures, are more likely to be proactive about security. It also assists in building a robust security culture within your company.

The INDYSEC team have a number of resources available to assist with security education and training. Please contact IndustrySecurity@nzdf.mil.nz to discuss your requirements further.

Access to NZDF sites

Access to NZDF sites (e.g. Camps, Bases or individual buildings) is likely to be tightly controlled. Each site has its own access procedures and security rules. Your employees will need to familiarise themselves with, and adhere to, the access requirements for the sites that they need to access.

RINGFENCE

The NZDF has a security alert system called RINGFENCE, which standardises procedures across NZDF sites in response to security threats. Your employees working at NZDF sites will need to familiarise themselves with RINGFENCE requirements, and any specific security rules and procedures pertinent to each site.

[5] There are a number of specific rules and procedures related to the disclosure or release of any classified NZDF material to third parties – particularly as it relates to disclosure to foreign nationals of foreign countries. Please contact IndustrySecurity@nzdf.mil.nz if more information is required.

ADDITIONAL INFORMATION

Elements of Protective Security

As described in the PSR (www.psr.govt.nz) and in NZDF security policies, there are four primary elements of protective security:

- **Personnel Security -** Protects NZDF resources by ensuring access to information and assets is only given to suitable people. The process of gaining a Security Clearance (see page 10) ensures your people can be trusted to safeguard classified information, assets or facilities. Obtaining a DISP Personnel Accreditation and the requisite Security Clearances directly contributes to NZDF Personnel Security.
- **Physical Security –** Relates to the security measures and controls that protect your people, information and assets from compromise. In the DISP context, this may require your company to implement physical security controls to ensure that protectively marked NZDF resources in your possession are protected. This is determined during the DISP Facility Accreditation process.
- **Information Security -** Protects NZDF information from unauthorised use, accidental modification, loss or release. The NZDF collects and receives information to fulfil its functions and expects all those who hold or access this information to protect it. Your information security measures may be assessed – particularly if a DISP ICT Accreditation is required.
- **Governance –** This ensures effective oversight and management of all elements of protective security. To successfully manage security risks organisations must ensure that security is part of their organisational culture, practices and operational plans. Specific security governance practices are required as part of DISP membership.

Security Classifications

There are two categories of official classified information:

- National Security Information; and
- Policy and Privacy Information.

National Security Information - is protectively-marked material, which if released without authorisation, could cause damage to New Zealand's national security interests. There are four classifications of National Security Information:

- **RESTRICTED** – The compromise of RESTRICTED information would damage national interests in an adverse manner.
- **CONFIDENTIAL** – The compromise of CONFIDENTIAL information would damage national interests in a significant manner.
- **SECRET** – The compromise of SECRET information would damage national interests in a serious manner.

- **TOP SECRET** – The compromise of TOP SECRET information would damage national interests in an exceptionally grave manner.

Policy and privacy information - Policy and Privacy Information is official information, which if released without authorisation, could cause damage to individuals, groups, organisations, agencies or government. There are two classifications of Policy and Privacy Information:

- **SENSITIVE** – Compromise of this information would likely damage the interests of the New Zealand Government or endanger the safety of the public.
- **IN-CONFIDENCE** – Compromise of this information would likely prejudice the maintenance of law and order, impede the effective conduct of government or adversely affect the privacy of citizens. Examples include COMMERICAL-in-CONFIDENCE or STAFF-IN-CONFIDENCE information.

Important note - NZDF information labelled 'UNCLASSIFIED' is still official information and should also be stored securely.

Security Clearances

Security Clearances are a fundamental part of Personnel Security in the NZDF. Although your company may be able to commence a contract with the NZDF prior to your employees receiving a Security Clearance, they will not be able to access classified information, assets or facilities until the requisite Security Clearance has been granted.

There are two types of security clearance in the NZDF:

- A Baseline Check; and
- A National Security Clearance.

Baseline Check - A Baseline Check is the minimum, mandatory security clearance in the NZDF. A Baseline Check is based upon a NZ Police Report, with the vetting of this report conducted by the Defence Vetting (DEFVET) team. A Baseline Check provides access to RESTRICTED NZDF information and assets, and un-escorted access to many facilities. Your employees will require a Baseline Check as a minimum if they require access to the Defence Information Exchange System (DIXS) or will be working at an NZDF facility. Obtaining a Baseline Check is also a pre-requisite to an application for a National Security Clearance.

National Security Clearance - A National Security Clearance (NSC) is required for access to classified NZDF information, assets or facilities at the CONFIDENTIAL level and above. The vetting process for all NSCs is conducted by the NZSIS. Key information about NSCs is as follows:

- **Sponsorship** - All NSCs must be sponsored by a New Zealand government agency. As a company contracted by the NZDF, the NZDF will sponsor the NSCs of your employees. All NSC applications sponsored by the NZDF are managed by the

DEFVET team in Defence Security. The DEFVET team receive all NSC applications, provide the interface between the NZDF and NZSIS, and communicate the outcomes of the vetting process.

- **Eligibility** – To be eligible for NSC vetting, a person must be a New Zealand citizen or a holder of a Residence class visa. In rare circumstances, other candidates may be eligible for security vetting. However, additional steps and checks are required. Additionally, each vetting candidate must meet the minimum checkable background requirements. As a guide, these are:
  - **CONFIDENTIAL** – five years checkable background;
  - **SECRET** – 10 years checkable background;
  - **TOP SECRET** – 10 years checkable background; and
  - **TOP SECRET SPECIAL** – 15 years checkable background.
- The PSR provides more detail on NSC eligibility.[6] The INDYSEC team can also talk through any specific concerns you may have during the DISP Accreditation process.
- **Application** – Each person applying for a NSC will need to complete an online questionnaire and provide details of both their personal and professional life, for example; previous residential addresses, employment, overseas travel, past and current relationships, and extended family. The level of detail required increases with each level of NSC. Your employees will also be required to provide referees who can attest to their trustworthiness.
- **Vetting** – Once an application is complete, the NZSIS vetting process will commence. This may involve interviews with the NZSIS for both the applicant and their referees. A range of factors can impact on the time required to complete the vetting process. A routine application may be completed in one to two months. More complex cases can take longer. Delays in the vetting process are commonly due to incorrect details in the application form, or the unavailability or unsuitability of referees.
- **Outcome –** Once the vetting process is complete, the NZSIS makes a recommendation to the NZDF on the suitability of the applicant to hold a NSC. Based on the NZSIS recommendation, the NZDF then makes the decision either grant the NSC, grant the NSC with conditions, or in rare cases, not grant the NSC.
- **NSC Responsibilities -** Once a NSC has been granted, the holder has ongoing responsibilities, which may include:
  - Reporting international travel plans;

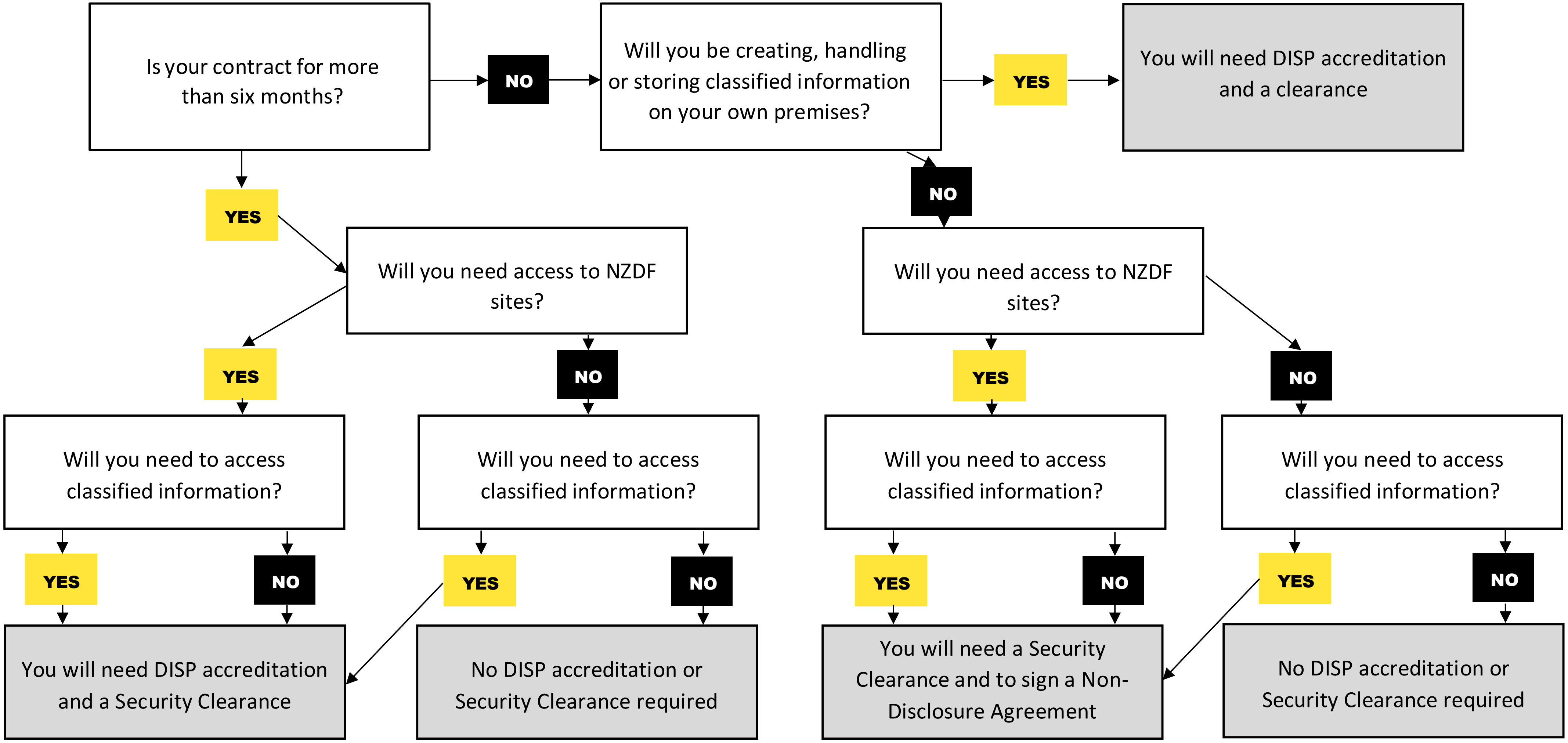
[6] https://www.protectivesecurity.govt.nz/assets/protective-security-requirements/resources/personnel-security/psr-guide-tomanaging-national-security-clearance-holders.pdf

  - Reporting significant changes in personal circumstances (note that any change in circumstance that could impact an individual's suitability to hold a NSC may initiate an assessment of their ongoing suitability);
  - Renew their NSC when required; and
  - Note that significant changes in circumstances, security breaches or instances of misconduct may prompt a review of an individual's ongoing suitability to hold a NSC.

- **NSC Renewal** – A NSC expires after five years or when the clearance holder leaves their employment. An application to renew a NSC should be initiated early enough to maintain continuity of the clearance.

- **Transfer of NSC** – In some circumstances a NSC can be transferred to another New Zealand government agency. Please contact IndustrySecurity@nzdf.mil.nz for further advice on this.

DISP Flow Chart


Is your contract for more than six months?
NO
Will you be creating, handling or storing classified information on your own premises?
YES
You will need DISP accreditation and a clearance
YES
NO
Will you need access to NZDF sites?
Will you need access to NZDF sites?
YES
NO
YES
NO
Will you need to access classified information?
Will you need to access classified information?
Will you need to access classified information?
Will you need to access classified information?
YES
NO
YES
NO
YES
NO
YES
NO
You will need DISP accreditation and a Security Clearance
No DISP accreditation or Security Clearance required
You will need a Security Clearance and to sign a Non-Disclosure Agreement
No DISP accreditation or Security Clearance required

WHO TO CONTACT FOR MORE INFORMATION

If you require further information on the subjects contained in this DISP Guide, please do not hesitate to contact the Industry Security team by emailing IndustrySecurity@nzdf.mil.nz in the first instance.

INDUSTRYSECURITY@NZDF.MIL.NZ

A11