New Zealand
DEFENCE
FORCE
Te Ope Kātua O Aotearoa

DEFENCE INDUSTRY SECURITY GUIDE

JUNE 2018

A FORCE FOR
NEW ZEALAND


30
DEFENCE AREA
I.D. CARD
CHECK
30

FOREWORD

Your organisation may be considering contracting with the New Zealand Defence Force (NZDF) or may already have a contract with us.

If the work you will do with us involves accessing classified information or secure facilities or assets, you will need to meet mandatory government and NZDF security standards to safeguard them.

Private contractors and service providers employed by NZDF and other government agencies play an important role in helping us to maintain the security of our personnel, information and facilities.

This guide is intended as an overview to help you to identify what you will likely need to do to fulfil the security requirements of your contract.

It outlines what may be required of you – the processes you may need to follow and the security procedures you may need to implement.

It also summarises the policies and standards behind those requirements – primarily Defence Force Orders (DFO) 51 and the Government's Protective Security Requirements (PSR).

If at any time you need more information, please do not hesitate to contact either your NZDF Sponsor or the Defence International and Industry Security team at DIIS@nzdf.mil.nz

We look forward to working with you.

Charlie Lott
Chief Security Officer

Scott Turner
Director of Security

SECURITY POLICY AND PRACTICE – AN OVERVIEW

Several government agencies, including the New Zealand Security Intelligence Service (NZSIS) are responsible for formulating New Zealand Government security policies.

These are defined through the Protective Security Requirements (PSR) which outline the Government's expectations of managing personnel, physical and information security.

The PSR sets out what government agencies – including the New Zealand Defence Force – must and should consider to ensure we are managing security effectively. See www.psr.govt.nz for more detail.

Each government department or agency is responsible for implementing its own security policy in alignment with those in the PSR. NZDF's security policy is contained in the Defence Force Orders (DFO).

All NZDF contractors and suppliers are required to comply with the policies prescribed in the DFO 51 series and DFO 101 and 102, as well as any other NZDF security policies, orders and directives.

NZDF's mission of defending New Zealand and its national interests is a complex task, and to achieve this mission we have been entrusted with information, assets and resources that we have an obligation to protect.

The Chief of Defence Force is responsible for security and ensuring that NZDF assets and information are protected to the required standard.

THE DEFENCE INDUSTRY SECURITY PROGRAMME (DISP)

If your contract with NZDF will involve accessing secure facilities, assets or classified information, you may need to be accredited under the Defence Industry Security Programme (DISP).

If accreditation is required, there are New Zealand Government and NZDF standards you will need to meet so that our information and assets are protected to the same level we require of NZDF staff.

As soon as the detail of what you will be doing under your contract with NZDF, and where, is known, we will notify you of the exact accreditation you will need and the security requirements you will have to fulfil.

The DISP is managed by the Defence International and Industry Security (DIIS) team in NZDF's Directorate of Defence Security.

As well as accreditation of companies working with NZDF, the DIIS team provides protective security advice and information and audits compliance.

When you will need to be accredited

Your company will need to be DISP-accredited if your contract with NZDF will involve:

- accessing NZDF areas or classified material for more than six months
- developing, storing or handling any protectively-marked material – either in hard copy or via a computer system or electronic network
- providing guard force or security services to NZDF
- storing, transporting, handling or managing NZDF weapons and munitions
- hosting any NZDF website.

Protectively-marked material is official information and 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 based on a risk assessment of how much damage to New Zealand citizens, the Government or government agencies would result from its release. That system includes the levels of RESTRICTED, CONFIDENTIAL, SECRET and TOP SECRET.

Types of accreditation

There are two main types of accreditation:

- **Personnel accreditation** – this certifies that your employees have been security-cleared to the level needed.

  Your company will need this accreditation if your employees will be accessing, handling or managing protectively-marked material on an NZDF site, accessing the NZDF computer network, or working out of an NZDF facility, camp or base.

  All staff who will access information or other protectively-marked materials classified CONFIDENTIAL or above will need to hold a valid National Security Clearance.

  If your staff will only be accessing secure areas and information classified as RESTRICTED or below, they will require a Defence Site Clearance (DSC) instead. A DSC involves a New Zealand Police Check and applicants must have resided in New Zealand for six months or longer.

  Sole contractors are also accredited under Personnel Accreditation.

- **Facility accreditation** – your company will need this accreditation if your contract will involve accessing, creating, handling or storing protectively-marked material at your own business premises.

Your company may also be required to have **Information and Communication Technology Accreditation** if you will be using your own computer system or equipment for developing classified documents during your contract with NZDF.

Initial eligibility requirements

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

- Have a signed contract with NZDF.
- Have a justified and valid need to access protectively-marked NZDF material.
- Be sponsored by an NZDF employee, another New Zealand government department, an approved foreign government or a current DISP member (subject to Directorate of Defence Security approval).
- 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 the Directorate of Defence Security's approval.
- Have signed a Security Agreement with the NZDF.
- Have nominated a Facility Security Officer, who will be your company's point of contact for security matters.

Getting accredited

The first step is your company securing a contract with NZDF. You cannot be accredited under the DISP without a signed contract. The DIIS team will then establish how long your contract is for, what level of classified information or assets your employees will have access to, and where they will be located/do the work.

You will be asked to fill out three forms:

- A form to nominate a Facility Security Officer (and a deputy if required) who will be responsible for fulfilling the security requirements under the DISP accreditation.
- A Security Agreement.
- A Security Practices and Procedures document that sets out the detailed security requirements you will need to fulfil.

For Personnel Accreditation, each employee who will access or use classified information will need to be vetted for a National Security Clearance or Defence Site Clearance, as appropriate. (See the Obtaining National Security Clearance section for more information).

For Facility Accreditation, as well as filling out the three forms and staff getting security clearance as above, a risk assessment will be carried out on your premises and you will be asked to make any physical changes needed such as installing a safe or getting new security locks on doors.

Your accreditation will be processed as soon as the forms are received, verified and countersigned. Once your company is accredited, the vetting of your staff applying for security clearances can be progressed.

Your responsibilities when you are DISP-accredited

As the Chief Executive, Managing Director or Company Principal, you are responsible for ensuring your organisation complies with all relevant security policies and procedures required of you under the DISP. That includes:

- Appointing, resourcing and supporting a Facility Security Officer (FSO) and where required, an Information Communications Technology Security Officer. Both roles may also need to have deputies appointed.
- Implementing and maintaining the security controls required by NZDF's Directorate of Defence Security. If you will be accessing, creating, handling or storing protectively-marked material at your own business premises and require Facility Accreditation, you will be advised of these controls following a risk assessment of your premises.
- Ensuring the FSO develops, implements and continuously reviews your organisation's specific security policy.
- Proactively managing security and leading by example, fostering and encouraging a security culture within your organisation.
- Informing your FSO of any proposed changes to company ownership, location, structure etc so he or she can in turn inform NZDF. Such changes may affect your DISP accreditation and security clearances.
- Meeting all time and resource costs associated with implementing the security measures NZDF requires of you.
- Dedicating time for regular employee security awareness education and training.
- Not disclosing any protectively-marked material to any third party. That includes any person, institution, national or international company, contractor, public or private entity or State.

Security education and training

Providing security education and training to your staff is an essential part of your responsibilities under the DISP.

Your employees need to understand why it is so important to protect the NZDF information and assets they are accessing, and the potential wide-reaching ramifications of a security breach.

Staff who understand the importance of their responsibilities and the part they play in implementing the required security measures are more likely to be proactive about security.

Please contact the DIIS team (DIIS@nzdf.mil.nz) if you have security education and training needs, and we will work with you to meet them.

Before you release any NZDF material

You must meet certain conditions and get approval from the Directorate of Defence Security before you release protectively-marked material to a third party. That includes sub-contractors.

The person or organisation you will be releasing information to must:

- be security-cleared to the same level, or higher, as the information's security classification
- need to know the information
- have approved storage facilities and other physical security measures in place to protect the information from unauthorised access, and
- have the appropriate DISP accreditation.

You must report to the DIIS team any unauthorised disclosure of NZDF protectively-marked material.

Important note:
There are further conditions that must be met if the information is to be released to foreign nationals or foreign countries. Please contact DIIS@nzdf.mil.nz to discuss.

Access to NZDF sites

Access to NZDF sites and buildings may be controlled by security guards and/or barrier gates. Each site or building has its own security requirements that you will need to adhere to if you will be working there.

You may require an access pass and have to sign in and out of the site or building. Or you may be required to be escorted on and off the site. Security guards may also conduct random checks of access passes or vehicles.

These local security requirements are additional to the DISP accreditation requirements.

Ringfence

NZDF has a security alert system called 'Ringfence' which standardises procedures to protect our people, information and assets according to the level of threat. The security personnel at the NZDF site or facility where you will be working will keep you informed of any increase in threat level and any actions that need to be taken.

WHITE	GREY	BLACK	AMBER	RED

OBTAINING A NATIONAL SECURITY CLEARANCE

The vetting process for all National Security Clearances required by government agencies is carried out by the New Zealand Security Intelligence Service (NZSIS). NZDF does not control or affect this process.

The time the vetting process takes depends on a range of factors, but it may take some months. This needs to be factored in when planning your work with NZDF.

Your contract with NZDF can likely start without your staff having received clearance, but they will not be able to access classified information or secure sites without having received the level of clearance required to do so.

To be eligible for a National Security Clearance, you usually need to be a New Zealand citizen or be an Australian, Canadian, British or American citizen who holds a Residence Class Visa for a certain length of time.

That means that any of your employees who are not New Zealand citizens may not be eligible to be security-cleared, which may affect your eligibility to contract with NZDF.

Each person applying for National Security Clearance will need to complete an online questionnaire about their personal and professional life. The level of detail needed will depend on the level of security clearance – the higher the clearance, the more detail needed e.g. for CONFIDENTIAL clearance, five years of history is needed. For SECRET and TOP SECRET clearance, it is 10 years.

Your employees will be asked to provide information about their previous residences, employment, travel, current and past relationships and extended family.

They will also be asked to provide personal and professional referees, who will be sent an online questionnaire to fill in. For the higher clearance levels, they may also be interviewed.

It can take some time to gather the information needed to fill out the forms so you may want to suggest to your staff that they start gathering information together in preparation for filling out the questionnaire.

It is important to note that the time vetting takes can be impacted by forms not being correctly filled in, or referees not meeting the necessary criteria or being unavailable. You may want to alert your staff to the fact that the more care taken to correctly and completely provide the required information, the faster the vetting process is likely to be.

Please also note that security clearances initiated by NZDF do not take priority over those from other government agencies, and we cannot direct the NZSIS to treat one application with more urgency than others.

The NZSIS does not charge for processing National Security Clearances – so there will be no cost to you or your staff in applying for a clearance.

For more information about National Security Clearances and the vetting process, go to www.protectivesecurity.govt.nz

After you receive security clearance

The vetting and background checks carried out when someone applies for a security clearance provide assurance about a person's suitability to hold a clearance at that time.

It does not provide a continued guarantee of security, so Defence Security staff will regularly review the validity of those clearances.

They will consider if there is still a need for the security clearance held and will, as appropriate, carry out:

- **A review of circumstance** – this may be prompted by a change in personal circumstances or a security concern being raised and will address all issues needed to resolve any concerns.
- **A review of clearance** – this is usually carried out every five years to re-look at suitability, focussing on the time since the initial security clearance or last review.

Transferring a security clearance

Under some circumstances, you can transfer your security clearance between New Zealand government departments if you require either the same or lower level of security clearance. Please contact DIIS@nzdf.mil.nz for further advice on this.

THE DIFFERENT TYPES OF SECURITY AND SECURITY CLASSIFICATIONS

Personnel security

NZDF is responsible for ensuring people to whom protectively-marked material is entrusted have a justified 'need-to-know' and fully understand their responsibilities in keeping the material secure.

They must have a need to access such material in order to do their job. Being in a position of authority is not a valid justification.

Personnel security aims to determine a person's suitability to hold a security clearance by looking into their personal history, qualities and behaviour.

As a general rule, only New Zealand, Australian, Canadian, British and American citizens and residents can be granted National Security Clearances. Length of residence requirements also apply.

Physical security

Physical security controls prevent unauthorised access to protectively-marked material through measures that deter, detect, delay or respond to unauthorised access.

Your organisation will need to provide an appropriately secure physical environment for any protectively-marked material in your care.

You may be required to have NZDF-approved:

- physical barriers
- electronic or mechanical access control systems
- intruder detection systems
- security guard force
- security keys and containers.

The measures you will need to implement will depend on the level of protectively-marked material in your care and your existing physical environment. A risk assessment will be carried out at your premises and following that, you will be provided with the exact requirements you will need to fulfil.

Protectively-marked material is only to be used within areas that have been assessed and approved as suitable for that purpose. When not in use, the material is to be stored in an NZDF-approved security container within an approved area or space.

Appropriate ways of disposing of protectively-required material are also required.

Information and Computer Technology (ICT) security

Information electronically processed, stored or transmitted needs to be protected according to its security classification.

ICT security includes technology, infrastructure, hardware, software, devices and information including:

- computers and computer networks (desktops, laptops and iPads)
- all types of mobile phones
- fixed and removable storage devices (USB, CDs, DVDs, iPods, MP3 players)
- cameras (digital, video, webcams)
- telephone systems
- video and audio players and receivers
- telecommunication equipment.

If you will be using your own computer system or equipment for developing classified documents during your contract with NZDF, you will need ICT accreditation under the DISP.

Security classifications

There are two categories of official classified information:

- National security information, and
- Policy and privacy information.

National security information

National security information is protectively-marked material which if released without authorisation or accidentally could cause damage to New Zealand's national security interests.

There are four classifications:

RESTRICTED – Compromise of RESTRICTED information would damage national interests in an adverse manner e.g. it might affect the economic wellbeing of New Zealand or our allies.

CONFIDENTIAL – Compromise of CONFIDENTIAL information would damage national interests in a significant manner e.g. it might damage the internal stability of New Zealand or our allies.

SECRET – Compromise of SECRET information would damage national interests in a serious manner e.g. it might shut down or substantially disrupt significant national infrastructure.

TOP SECRET – Compromise of TOP SECRET information would damage national interests in an exceptionally grave manner e.g. it might cause exceptionally grave damage to relations with other governments or loss of life.

Important note

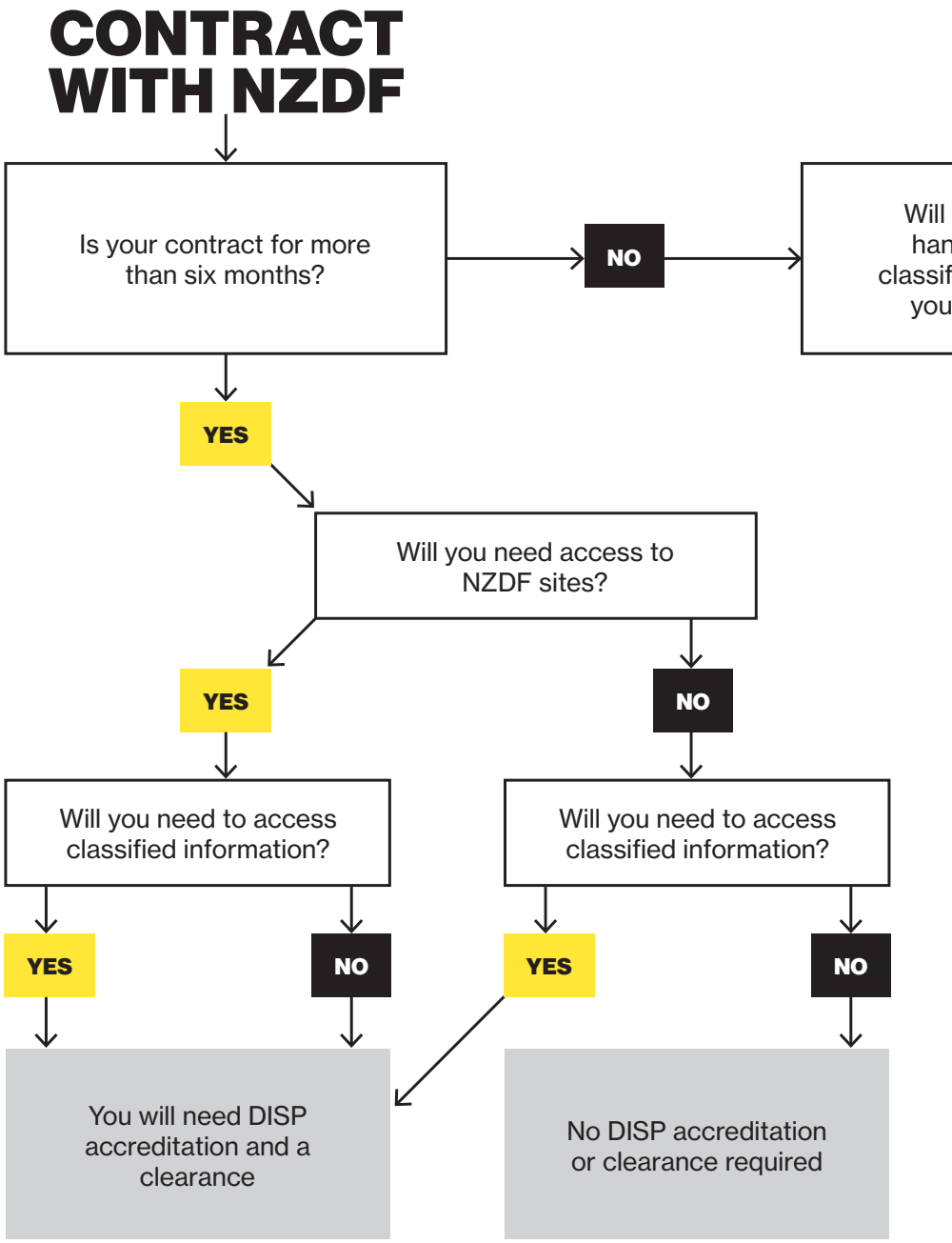
Please be aware that the information labelled as UNCLASSIFIED does not necessarily mean it is readily releasable to the public. NZDF information, even if it is UNCLASSIFIED, may be of interest and value to New Zealand's adversaries and should still be kept secure and private. For example, the number and type of army vehicles involved in a training operation is not necessarily classified information, but if the specific times and places of the vehicles' whereabouts is made public knowledge, it could bring additional risks to NZDF.

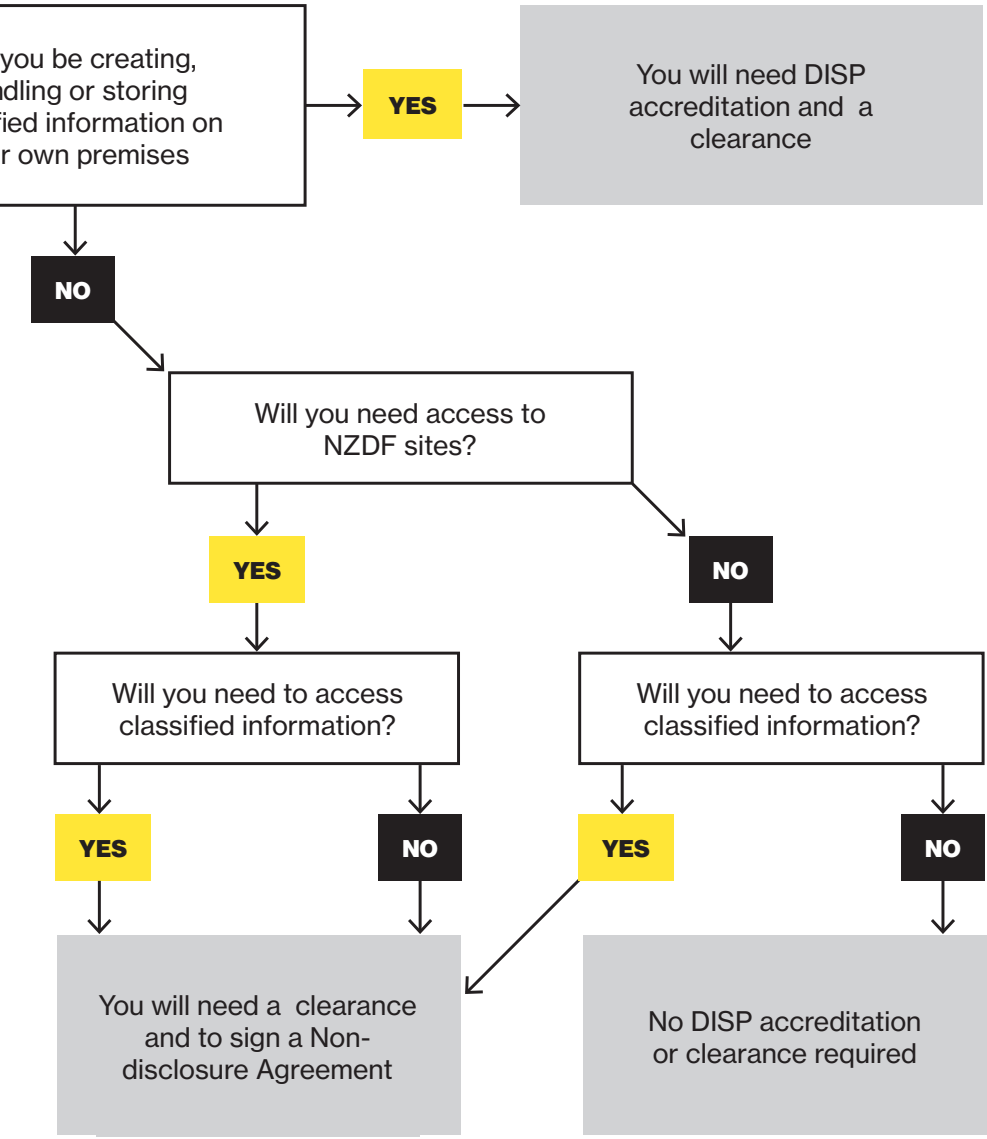
Policy and privacy information

Policy and privacy information is official information which if released without authorisation or accidentally, could cause damage to an individual, group, organisation, agency or government.

There are two classifications:

- SENSITIVE – compromise of this information would likely damage the interests of the New Zealand Government or endanger the safety of the public.
- X-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. (The 'X' is replaced by whatever interest is being protected e.g. COMMERCIAL-IN-CONFIDENCE, STAFF-IN-CONFIDENCE or SECURITY-IN-CONFIDENCE.)


CONTRACT WITH NZDF
Is your contract for more than six months?
NO
Will han classif you
YES
Will you need access to NZDF sites?
YES
NO
Will you need to access classified information?
Will you need to access classified information?
YES
NO
YES
NO
You will need DISP accreditation and a clearance
No DISP accreditation or clearance required


you be creating,
ndling or storing
fied information on
r own premises
YES
You will need DISP accreditation and a clearance
NO
Will you need access to NZDF sites?
YES
NO
Will you need to access classified information?
Will you need to access classified information?
YES
NO
YES
NO
You will need a clearance and to sign a Non-disclosure Agreement
No DISP accreditation or clearance required

WHO TO CONTACT FOR MORE INFORMATION

If you require clarification or more information about the security measures that will be required of you when you contract with NZDF, DISP accreditation or security clearances, please do not hesitate to contact the DIIS team by emailing DIIS@nzdf.mil.nz in the first instance.

DIIS@NZDF.MIL.NZ