FOREWORD

Your organisation may be considering entering into a contractual relationship with the New Zealand Defence Force (NZDF), or may already have entered into such a relationship. Should that relationship require access to sensitive or classified information or materiel, your organisation will be required to meet New Zealand Government and NZDF security standards to safeguard that information or materiel. This is a mandatory requirement.

This booklet outlines the rationale behind the security polices, standards and processes applicable to NZDF. These policies, standards and processes are also applicable to your organisation and the work it undertakes as a result of your organisation’s contractual relationship with NZDF. This booklet provides a broad introduction to the protective security arrangements for organisations that have not previously dealt with classified information or materiel. Comprehensive detail on NZDF security policy is contained in the Defence Force Orders 51 series (DFO 51). Advice and assistance can be obtained from the Defence Security Division (DSyD).

The application of security measures, whilst mandatory, need not be onerous. Early identification of issues and communication are key elements in the smooth implementation of security measures. For that reason, you are encouraged to contact your NZDF sponsor, or DSyD staff to discuss any security issues you may encounter.

I hope that you will find the information in this booklet to be helpful, straightforward and that it will assist you to identify and implement the necessary security aspects that are relevant to your relationship with the NZDF.

S.G. TURNER
Deputy Director of Security
For Chief of Defence Force
SECURITY POLICY

The New Zealand Government is responsible for the security of the nation. Several Government Departments, including the New Zealand Security Intelligence Service (NZSIS), are responsible for the formulation of New Zealand Government security policies. These policies are promulgated in several manuals, including Security in the Government Sector (SIGS) 2002 and the New Zealand Government Protective Security Manual (PSM). The SIGS 2002 prescribes the minimum standards and best practice guidelines which are applicable to all New Zealand Government departments and agencies.

Each department or agency is responsible for implementing its own security policies in alignment with those promulgated in the PSM. Accordingly, NZDF’s security policy is contained in the Defence Force Orders (DFO) series. The DFO 51 series sets out policies and procedures for the application of protective security measures in NZDF and Defence Industry, while DFO 101 & 102 detail the Communications and Information Systems (CIS) requirements. These policies also provide guidance to assist managers to determine the security measures that may exceed the minimum standards prescribed in SIGS 2002 or the PSM.

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

PROTECTIVELY-MARKED MATERIEL

In this booklet, the term protectively-marked materiel refers to any information, equipment, ammunition, weapon, system or asset provided to a DISP member by the New Zealand Defence Force or any other foreign government which has a minimum security requirement.
The Chief of Defence Force (CDF) is responsible for security in the NZDF and to ensure that protectively-marked materiel, provided to Defence Industry, is protected to the required standard. The Deputy Director Security (DDSy) manages this responsibility for Defence Industry on a day-to-day basis.

DDSy is responsible for ensuring that NZDF security policy reflects not only New Zealand Government policy direction, but also meets NZDF’s unique business and operational requirements. DDSy’s responsibilities include, but are not limited to:

- Developing and reviewing NZDF security policy and standards;
- Investigating or contributing to the investigation of significant security incidents; and
- Ensuring that industry and consultants who are granted access to protectively-marked materiel implement and maintain security standards in accordance with NZDF policy.

IMPLEMENTATION OF SECURITY POLICY

The NZDF mission of defending New Zealand and its national interests is a complex task. In order to achieve this mission, the NZDF has been entrusted with assets and resources that we are obliged to protect. Our actions to protect these assets and resources comprise the management of security risks.

The effective management of security risks requires a combination of tangible and intangible measures. This methodology is known as Defence-in-Depth. Defence-in-Depth works on the premise that a series of protective barriers (physical, procedural and psychological) are more robust than a single line of defence. Some of these barriers may include:

- Only providing access to protectively-marked materiel to those that require it for their job;
- Ensuring that all protectively-marked materiel is classified appropriately;
- Implementation of security procedures; and
- The use of electronic security devices where required.
DEFENCE-IN-DEPTH

Laws, security policies, perimeter fencing

Access control, security alarms

Initial security vetting, escorting

Clear desk, secure login

Education & Training

Need-To-Know

Asset

Need-To-Hold

Classification, settings

Key control

Restricted areas, secure rooms

Security guards, patrols

Lighting, geographical surrounds
The Defence Industry Security Programme (DISP) is designed to provide its members with information and direction to protect protectively-marked materiel. The DISP requires its members to be familiar with and adhere to NZDF security policies and procedures.

If your organisation is accredited under the DISP, it will be provided with relevant copies of, or extracts from, the DFO 51 series. DSyD staff can also provide ongoing security advice and guidance.

WHEN IS ACCREDITATION REQUIRED?

Accreditation is required if, at any time, your organisation:

- Accesses, stores, or handles any protectively-marked materiel, either hardcopy or via a computer system or electronic network;
- Stores, transports or controls the handling of NZDF weapons, ammunition or explosives; and/or
- Hosts any NZDF website.

WHAT ARE THE TYPES OF ACCREDITATION?

**Personnel Accreditation (PA)** – certifies that DISP members’ employees have been security cleared to the identified level.

**Facility Accreditation (FA)** – granted to your organisation if it accesses, handles or stores protectively-marked materiel at your business premises.

**Communications & Information Systems Accreditation (FA: CIS)** – granted to your organisation for the use of electronic storage or processing devices used for viewing, processing or storing classified information.

**Consultant Accreditation (CA)** – granted to an individual contracted directly to NZDF who has a sponsored requirement to access protectively-marked materiel.

DISP accreditations of FA and FA: CISA are granted to specific facilities. If additional facilities require accreditation, contact your sponsor.
INITIAL ACCREDITATION

Your organisation must meet the following requirements in order to be eligible for any accreditation:

• Have a justified and approved requirement to access protectively-marked materiel;
• Be sponsored by a member of the NZDF, another New Zealand Government Department, an approved Foreign Government, or a current DISP member (subject to DSyD approval and acceptance);
• Not be under foreign ownership, control or influence to the extent that the granting of an accreditation would not be in New Zealand’s national interest;
• Have developed an organisation specific security manual for staff involved; and
• Have signed a security agreement for the protection of protectively-marked materiel.

ACCREDITATION STARTS EARLY

Contact DSyD as soon as possible when you are considering tendering or if you have already been awarded a contract. Security requirements are easier to integrate the earlier they are identified. Early advice may save you time and money.
RESPONSIBILITIES FOR A DISP MEMBER’S MANAGEMENT

Management (Chief Executive Officers, Managing Directors or Company Principals) is responsible for ensuring that the organisation complies with all relevant security policy as prescribed by DSyD. A DISP Member’s Management must:

• Appoint, resource and support a Facility Security Officer (FSO) and a Communications and Information System Security Officer (CISSO) where required;
• Implement and maintain security controls as required by DSyD;
• Ensure the FSO develops, implements and continuously reviews the organisation’s specific security policy;
• Be pro-active towards security and by example, foster and encourage a positive security culture throughout the organisation;
• Inform the FSO of any proposed changes to ownership, location, structure, etc);
• Meet all time and resource costs associated with implementing required security measures;
• Dedicate time for employee security education and training activities;
• Not disclose any protectively-marked materiel to any third party;*
• Identify and manage all security risks in consultation with DSyD staff; and
• Not advertise DISP membership or any accreditation for promotional reasons.

*“Third Party” means any person, institution, national or international organisation, public or private entity or State other than the NZDF and the organisation. This includes any third country government, any national of a third country or any Contractor whether or not owned or influenced by the organisation.

SUBCONTRACTING

Before releasing or allowing access to any protectively-marked materiel to any subcontractor (NZ or foreign born) you must contact DSyD to confirm that appropriate security measures are in place.
Security Education and Training is the most important aspect of your responsibilities to the NZDF. This ensures that everyone in your company understands the reasoning behind the security measures that have been put in place. Staff who know that they play an important part in security are likely to be proactive about these security measures. We have created a variety of educational materials that are freely available to you. The posters, brochures and briefings are updated as necessary to evolve with new security threats and policy.

You are welcome to attend any of the training courses we run on a regular basis throughout the country. Please contact DSyD for further information.
Security is a condition achieved through the establishment and maintenance of a variety of measures designed to protect our personnel, information, and assets (materiel and installations).

Protective security encompasses Information, Personnel, Physical, and CIS security, underpinned by an appropriate threat assessment.

**INFORMATION SECURITY**

Information security (INFOSEC) is the protection of information against unauthorised access or modification (irrespective of whether in storage, transit or processing). INFOSEC spans all areas of protective security and encompasses all information stored or processed by any means. It is not limited to documents or information processed on computers. In this context, information includes, but is not limited to:

- Documents and papers;
- Electronic data;
- Software, systems and networks used to store, process or communicate information;
- Knowledge gained by individuals in the course of their work for NZDF; and
- Physical items from which information about design, components or use could be obtained.

**OFFICIAL INFORMATION**

All information generated by NZDF employees and contractors to NZDF is official information which may require some level of protection. Legislation governing the general protection and disclosure of official information includes:

1. Crimes Act 1961;
2. Defence Act 1990;
3. Official Information Act 1982;
4. Privacy Act 1993; and
SECURITY CLASSIFICATIONS

The process that enables the identification and application of appropriate levels of security to information. It also defines the degree of damage that unauthorised release of the information may cause to New Zealand. There are two categories of official information:

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

* Note: UNCLASSIFIED does not necessarily mean the information is readily releasable to the public. Using the “UNCLASSIFIED” marking may be helpful in certain situations although not mandatory.

NATIONAL SECURITY INFORMATION

National security information is protectively-marked materiel where, if compromised, could cause damage to New Zealand’s national security interests. There are four classifications of national security information:

**TOP SECRET:** Compromise of information would damage national interests in an exceptionally grave manner.

*Ex. Compromise of **TOP SECRET** material may cause exceptionally grave damage to relations with other governments.*

**SECRET:** Compromise of information would damage national interests in a serious manner.

*Ex. Compromise of **SECRET** material may shut down or substantially disrupt significant national infrastructure.*

**CONFIDENTIAL:** Compromise of information would damage national interests in a significant manner.

*Ex. Compromise of **CONFIDENTIAL** material may damage the internal stability of New Zealand or friendly countries.*

**RESTRICTED:** Compromise of information would damage national interests in an adverse manner.

*Ex. Compromise of **RESTRICTED** material may adversely affect economic well being of New Zealand or friendly countries.*
POLICY AND PRIVACY INFORMATION

Policy and privacy information is official information where, if compromised, damage could be caused to an individual, group, organisation, agency or government. There are two classifications of public and privacy information:

SENSITIVE: compromise of information would be likely to damage the interests of the New Zealand Government or endanger the safety of its citizens, and

X-IN-CONFIDENCE: compromise of information would be likely to prejudice the maintenance of law and order, impede the effective conduct of Government or affect adversely the privacy of its citizens.

The X is replaced by whatever interest is being protected, e.g. COMMERCIAL-IN-CONFIDENCE, STAFF-IN-CONFIDENCE, SECURITY-IN-CONFIDENCE.

CONDITIONS FOR THE RELEASE OF NZDF MATERIEL

Several conditions must be met before any protectively-marked materiel can be released to any party (there are further conditions for the release of information to foreign nationals or foreign countries).

The party to whom the information will be released must:

- Be security cleared to a level equal to, or higher than, the security classification of the information;
- Have a need-to-know the information;
- Have approved storage facilities and other physical security measures to protect the information from unauthorised access; and
- Have the appropriate DISP accreditations.

You must obtain DSyD approval to release protectively-marked materiel to any third party. Additionally, you must report to DSyD staff any unauthorised disclosure of NZDF protectively-marked materiel as soon possible.
The NZDF is responsible for ensuring that people to whom protectively-marked materiel are trusted, have a justified need-to-know the materiel, and fully understand their responsibilities and obligations. The need-to-know principle requires a person to have a justifiable need to access protectively-marked materiel in order to perform their official duties. Positions of authority or convenience are invalid justifications.

Personnel security aims to determine a person’s suitability to hold a security clearance through an examination of their personal history, personal qualities and behaviour. The person is assessed to determine whether they are honest, trustworthy, mature, tolerant, loyal, and have an appreciation of their protective security responsibilities and obligations.

As a general rule, only New Zealand, Australian, Canadian, British and American (US) citizens can be granted New Zealand security clearances.

THE SECURITY CLEARANCE PROCESS

A security clearance must be obtained prior to access to protectively-marked materiel.

The three levels of security clearance which can be processed are:

CONFIDENTIAL, SECRET, and TOP SECRET.

As the level of security clearance increases, so does the level of background checking required. The vetting process becomes more expensive, time consuming and intrusive. The best outcomes are achieved when the requirement is identified early and the process initiated with adequate lead time. DSyD processes all security clearances for NZDF and Defence Industry.

Although not a security clearance, a Defence Site Clearance may be granted if DISP employees, contractors or consultants, do not require access to any protectively-marked materiel CONFIDENTIAL or above, are to be employed on a NZDF site.
AFTERCARE

Background checks and vetting enquiries provide certain levels of assurance about a person’s suitability at the time the security clearance was granted. It does not provide a continuing guarantee of suitability. The effective management of personnel in the workplace is an integral aspect of security.

DSyD staff conduct regular aftercare processes for security clearances. The first stage in each of these processes is to determine whether the requirement for the security clearance held still remains. The two aftercare processes conducted are:

**Review of circumstance:** This may be triggered by a change in personal circumstances or a security concern being raised, and will address all issues considered necessary to resolve any concerns;

**Review of clearance:** A periodic process (normally conducted every five years) involving a complete review of suitability, focussing on the period of time since the initial security clearance or last review.

TRANSFERRING A SECURITY CLEARANCE

Under some circumstances, security clearances may be transferable between New Zealand Government departments on the basis that the individual requires the same or a lower level of security clearance.

DSyD advice on this point should be sought.
PHYSICAL SECURITY

Physical security contributes to a safe and secure environment through the prevention of unauthorised access to protectively-marked materiel by deterring, detecting, delaying and responding to unauthorised access.

Your organisation will need to provide an appropriately secure physical environment for any protectively-marked materiel it deals with.

Physical security measures include NZDF approved:

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

SECURITY RATINGS OF SITES

There are three security ratings applicable to a site, categorised by the degree of security protection they provide. Security ratings can be applied to a site such as a single room, a building or a complex consisting of a number of buildings.

Protectively-marked materiel is only to be used within areas that have been assessed and approved as suitable for that purpose. When not in use, the materiel is to be stored in a NZDF approved security container within an approved area. The type of security controls required will depend on the classification of protectively-marked materiel, and the security rating of the site.

*Note: Appropriate methods of disposal for protectively-marked materiel is also required.

Protectively-marked materiel must not be taken home in any form unless approved by DSyD. Appropriate and accredited protective security arrangements must be in place.

Contact DSyD as soon as the requirement for a facility to be accredited becomes known.
Increasingly, data is processed, stored and transmitted electronically. This data requires protection commensurate to its security classification. The broad objective of CIS security is to apply an effective and consistent level of security to all CIS that process NZDF information.

**DEFINITION OF CIS**

CIS includes technology hardware, software, data, infrastructure and devices. For example:

- computers (i.e. desktops, laptops, and mobile computing devices);
- fixed and removable storage devices (i.e. USB, CDs, DVDs, iPods, MP3 players);
- cameras (i.e. video, digital, webcams);
- telephone systems;
- all types of mobile phones (i.e. Blackberry and iPhones);
- video and audio players/receivers (i.e. CD and DVD players);
- telecommunication equipment; and
- networks.

**ACCREDITATION**

NZDF uses an accreditation framework to ensure that CIS are effectively protected. All CIS processing or storing NZDF protectively-marked materiel must attain certification and accreditation before they can be used. CIS that require accreditation include, but are not limited to:

- NZDF CIS or Defence Industry CIS (including applications and databases) that process NZDF protectively-marked materiel;
- CIS that are deemed critical to NZDF business continuity or requirements.

These CIS are to be accredited to a minimum of **RESTRICTED**.

CIS are not to operate or process protectively-marked materiel until accreditation is granted.
ACCESS CONTROL TO NZDF SITES

Access to NZDF establishments and buildings may be controlled by security guards and/or barrier gates. The security guards may conduct random checks of access passes or vehicles. Therefore, personnel may be stopped for inspection upon entry or exit to NZDF premises.

RINGFENCE

NZDF has a security alert system, named ‘RINGFENCE’ which standardises procedures to protect NZDF personnel, assets and resources according to the level of threat, including those with potential for violence. RINGFENCE procedures are defined in several levels which increase commensurate to the identified threat. The most obvious indication of an increased RINGFENCE alert level is the application of more intensive inspection regimes and access controls.

GREY  BLACK  AMBER  RED
For more information contact:

**The Defence & International Industrial Security Team**

+64 (0)4 496 0007  
diis@nzdf.mil.nz