SECURITY POLICIES AND PLANS

Level 1 – Level 3

INSERT BUSINESS NAME

Insert address of Entity

**This template is designed to cover a range of security aspects. Please complete the fields that apply to your Entity and delete those that do not apply.**

The Defence Industry Security Program (DISP) team can assist you with the development of your Security Policies and Plans. Please contact DISP.info@defence.gov.au for assistance.

**ISSUED BY THE AUTHORITY OF:**

CHIEF SECURITY OFFICER: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

SIGNATURE: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

DATE: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**WITNESSED BY:**

SECURITY OFFICER: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

SIGNATURE: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

DATE: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**DOCUMENT STATUS**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Review Number** | **Author** | **Reviewer** | **Approver** | **Date** |
| **Name** | **Signature** | **Name** | **Signature** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**EMPLOYEE AGREEMENT WITH THESE SECURITY POLICIES AND PLANS**

**(2 options delete as required)**

**Option 1. Add a reference to an internal file that captures employees engaged on Defence’s agreement with the SPPs.**

**Example:** Employee agreement with these Security Policies and Plans are documented in the Security Register and also in the Personnel Security Folder.

**Option 2. Have all employees engaged on Defence read the SPPs and sign below (to be completed annually).**

|  |  |  |
| --- | --- | --- |
| **Name** | **Signature** | **Date** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Contents**

[1. Defence Industry Security Program 5](#_Toc202882102)

[2. BUSINESS DETAILS AND DESCRIPTION 5](#_Toc202882103)

[3. POINTS OF CONTACT 6](#_Toc202882104)

[3.1 Defence, DISP 6](#_Toc202882105)

[3.2 Entity Name 6](#_Toc202882106)

[4. RESPONSIBILITIES 6](#_Toc202882107)

[4.1 Chief Security Officer Responsibilities 6](#_Toc202882108)

[4.2 Security Officer Responsibilities 7](#_Toc202882109)

[5. SECURITY POLICY DOCUMENTATION 8](#_Toc202882110)

[5.1 Protective Security Policy Framework 8](#_Toc202882111)

[5.2 Defence Security Principles Framework 8](#_Toc202882112)

[5.3 Australian Government Information Security Manual 9](#_Toc202882113)

[6. GOVERNANCE 10](#_Toc202882114)

[6.1 Security Policies and Plans (SPP) 10](#_Toc202882115)

[6.2 Security Register 10](#_Toc202882116)

[6.3 Designated / Industry Security Assessed Positions Register 11](#_Toc202882117)

[6.4 Report Changes in Foreign Ownership Control and Influence 11](#_Toc202882118)

[6.5 Ongoing Assurance and Uplift Program 11](#_Toc202882119)

[6.6 Security Risk Assessment 12](#_Toc202882120)

[6.7 Annual Security Awareness Training 12](#_Toc202882121)

[6.8 Insider Threat Program 13](#_Toc202882122)

[6.9 Overseas Travel 13](#_Toc202882123)

[6.10 Official Overseas Travel 14](#_Toc202882124)

[6.11 Change of Circumstance Reporting 14](#_Toc202882125)

[6.12 Contact Reporting 15](#_Toc202882126)

[6.13 Security Incident Reporting 16](#_Toc202882127)

[6.14 Security Officer Training 17](#_Toc202882128)

[6.15 Defence Online Security Dashboard (DOSD) 17](#_Toc202882129)

[6.16 Close of Business Security Check 18](#_Toc202882130)

[6.17 Emergency Situations 18](#_Toc202882131)

[7. PERSONNEL SECURITY 19](#_Toc202882132)

[7.1 Employment Screening 19](#_Toc202882133)

[7.2 Personnel Security Clearances 19](#_Toc202882134)

[7.3 Security Clearance After-Care 19](#_Toc202882135)

[7.4 Identification (ID) and Access Passes 20](#_Toc202882136)

[7.5 Visitors 21](#_Toc202882137)

[7.6 Cleaners and Ancillary Staff 21](#_Toc202882138)

[8. PHYSICAL SECURITY 22](#_Toc202882139)

[8.1 Physical Certification of Zones 22](#_Toc202882140)

[8.2 Security Containers 23](#_Toc202882141)

[8.3 Use of Security Construction and Equipment Committee Approved Products 23](#_Toc202882142)

[8.4 Keys and Combinations 24](#_Toc202882143)

[8.5 Security Alarm System 24](#_Toc202882144)

[8.6 Security Guards 25](#_Toc202882145)

[9. INFORMATION AND CYBER SECURITY 26](#_Toc202882146)

[9.1 ICT Networks Standard Operating Procedures 26](#_Toc202882147)

[9.2 Portable Electronic Devices (PED) 26](#_Toc202882148)

[9.3 Audio-Visual Security 27](#_Toc202882149)

[9.4 Classified Document Register 28](#_Toc202882150)

[9.5 Classified Document Muster 28](#_Toc202882151)

[9.6 Security Caveats 29](#_Toc202882152)

[9.7 Official Information 29](#_Toc202882153)

[9.8 Transfer of Classified Information/Security Protected Assets 30](#_Toc202882154)

[9.9 Copying and Reproduction of Protectively Marked Information 30](#_Toc202882155)

[9.10 Disposal and Destruction of Protectively Marked Information and Assets 31](#_Toc202882156)

[10. CONCLUSION 32](#_Toc202882157)

[10.1 SECURITY IS EVERYONE’S RESPONSIBILITY 32](#_Toc202882158)

**ABBREVIATIONS**

|  |  |
| --- | --- |
| AGSVA | Australian Government Security Vetting Agency |
| ASR | Annual Security Report |
| BIL | Business Impact Level |
| CDR | Classified Document Register |
| COMSEC | Communication Security |
| CSO | Chief Security Officer |
| DISP | Defence Industry Security Program |
| DOSA | Directorate of Security Assurance |
| DOSD | Defence Online Security Dashboard |
| DPN | Defence Protected Network |
| DSAP | Designated Security Assessed Position |
| DSPF | Defence Security Policy Framework |
| FIS | Foreign Intelligence Services |
| FOCI | Foreign Ownership Control and Influence |
| ISM | Australian Government Information Security Manual |
| PED | Portable Electronic Devices |
| PSPF | Protective Security Policy Framework |
| PSZ | Physical Security Zones |
| SAS | Security Alarm System |
| SCEC | Security Construction Equipment Committee |
| SCIF | Sensitive Compartmented Information Facility |
| SIA | Security of Information Agreement or Arrangement  |
| SO | Security Officer |
| SOP | Standard Operating Procedures |
| SPP | Security Policies and Plans |
| SR | Security Register |
| SRA | Security Risk Assessment |
| SRR | Security Risk Register |

# Defence Industry Security Program

The Defence Industry Security Program (DISP, the Program) assists in securing Defence capability through strengthened security practices in partnership with industry, and enhances Defence’s ability to manage risk in the evolving security environment. DISP manages the Program to support Defence Groups and Services, and defence industry in managing security risks.

Following Defence’s assessment of their eligibility and suitability, < Entityname> <insert Entity address> will be granted a DISP Membership at the following levels:

 **Governance Security:** <Enter Membership Level>

 **Personnel Security:** < Enter Membership Level>

 **Physical Security:** < Enter Membership Level>

 **Information & Cyber Security:** < Enter Membership Level>

<Entity name> must continue to meet the ongoing eligibility and suitability requirements, as outlined in the Defence Security Principles Framework (DSPF) *Principle 16* and *Control 16.1* *Defence Industry Security Program* to maintain their DISP membership.

< Entity Name> has agreed to abide by the security provisions stated in the DSPF, and reflected in these Security Policies and Plans (SPP). The SPP provides a ***‘working guide’*** for < Entity Name> management and all personnel to implement security measures required by the DSPF.

# BUSINESS DETAILS AND DESCRIPTION

A current SPP is required in every facility used by < Entity Name>. *Please ensure this template is updated for each facility accordingly.*

**<ENTITY NAME>**

<*Entity* *name*> is located at <*enter Entity address*>.

<*Give a brief description on the role of each the Facility/Entity* >.

*Please provide the following details:*

*Your Entity’s registered ASIC address:*

*Does your Entity’s postal address differ from its registered ASIC address?*

*List the physical addresses of all your Entity’s facilities, including any located outside of Australia.*

# POINTS OF CONTACT

Defence, DISP

### The DISP Team can be contacted via DISP.info@defence.gov.au.

### The DISP Team can assist you or request a local DOSA representative as required in providing local security advice or services. Please contact the DISP team if you require these services.

### Please call Defence for all non-DISP related matters on 1800 DEFENCE (1800 333 362).

Entity Name

### <*Entity name*> **Chief Security Officer** is <insert CSO name>.

Business Hours: <insert phone number>

After Hours: <insert phone number>

### <*Entity name*> **Security Officer** is <insert SO name>.

Business Hours: <insert phone number>

After Hours: <insert phone number>

### IF OTHER <Entity name> **Security Officer** is <insert SO name>.

Business Hours: <insert phone number>

After Hours: <insert phone number>

# RESPONSIBILITIES

Chief Security Officer Responsibilities

### The CSO must be a member of the entity’s board of directors (or similar governing body), executive personnel, general partner, or senior management official with the ability to implement policy and direct resources. The CSO **must** be able to obtain and maintain a Personnel Security Clearance commensurate with the Industry Entity’s level of DISP membership.

### <*Name of CSO>* as the CSO is responsible for oversight of, and responsibility for, security arrangements and championing a security culture in <*Entity* *name*>.

### <*Name of CSO>* is accountable for ensuring:

1. all obligations contained in the DISP principle and control policy documents for their level of membership are met;
2. an appropriate system of risk, oversight and management is maintained;
3. DISP reporting obligations are fulfilled;
4. any sensitive and classified materials entrusted to the Entity are safeguarded at all times;
5. Security Officer(s) are appointed to develop and implement the Entity’s security policies and plans, on the CSO’s behalf;
6. The DISP Annual Security Report is agreed by the executive (Board equivalent), and all recommendations are implemented within agreed timeframes; and
7. any change in Foreign Ownership Control and Influence (FOCI) status of <Entity name> is reported to Defence via the DISP Member Portal here - [DISP Member Portal | Business & Industry | Defence](https://www.defence.gov.au/business-industry/industry-governance/industry-regulators/defence-industry-security-program/resources/disp-member-portal).
8. *Please insert any additional CSO responsibilities set by the Entity, if applicable.*

Security Officer Responsibilities

### The SO is responsible for the development and implementation of the security policies and plans and acts on behalf of the CSO. An SO **must** be able to obtain and maintain a Personnel Security Clearance commensurate with the Industry Entity’s level of DISP membership.

### <*Name of SO>* as the SO is responsible for:

1. the development and application of security policies and plans within <*Entity* *name*>;
2. ensuring sensitive and classified materials entrusted to <*Entity* *name*> are safeguarded at all times;
3. maintaining the Designated/Industry Security Assessed Position (DSAP) list, which is to be made available to DISP at their request;
4. maintaining a Security Register (SR);
5. the management of personnel security clearance requests;
6. reporting change of circumstances and vulnerabilities of clearance holders;
7. facilitating annual security awareness training of personnel:
8. reporting security incidents and fraud incidents, and contact reports, in accordance with Defence policy; and
9. yearly assurance activities to support the CSO.
10. <*Include additional SO responsibilities as directed by the CSO>*

***\*****Where an Industry Entity holds Level 1- 3 DISP membership, SOs with limited security responsibilities may hold lower level Personnel Security Clearances however the specific roles and responsibilities need to be clearly outlined in the SPPs to justify why a lower level of security clearance is appropriate*.

Industry Entities **must** document in their security policies and plans the roles and responsibilities of SOs that hold lower level Personnel Security Clearances.

Additionally, in order to obtain authority to sponsor and manage Personnel Security Clearances within the Industry Entity, an SO **must** have a minimum Negative Vetting 1 (NV1) Personnel Security Clearance. SOs cannot sponsor Personnel Security Clearances at a level higher than the Personnel Security Clearance level they hold (e.g. an NV1 clearance holder cannot sponsor NV2 clearances).

### **Additional Security Officer Appointments**

*Delete if not applicable*

### <*Entity* *name*> management have appointed the following personnel to additional SO positions and will support all security appointments in accordance with the DSPF:

1. Information Technology Security Manager (ITSM);

 <*insert ITSM name and contact details (if applicable)*>

1. Information Technology Security Officer (ITSO);

 <*insert ITSO name and contact details (if applicable)*>

1. COMSEC Custodian Officer (CCO);

 *<insert CCO name and contact details (if applicable)>*

1. Classified Document Register (CDR) Responsible Members;

 i. Custodian(s) <*insert name(s)*>

 ii. Maintaining Member(s) <*insert name(s) here>*

 iii. Supervising Member(s) *<insert name(s) here>*

# SECURITY POLICY DOCUMENTATION

Protective Security Policy Framework

### The Protective Security Policy Framework (PSPF) provides the appropriate controls for the Australian Government to protect its people, information and assets at home and overseas. The PSPF can be found at: [PSPF Annual Release | Protective Security Policy Framework](https://www.protectivesecurity.gov.au/pspf-annual-release).

Defence Security Principles Framework

### The Defence Security Principles Framework (DSPF) is available from the SO and provides information on security requirements, which are specific to Defence, and DISP members. The DSPF can be located on the DISP website, DOSD, or on the Defence website [here](https://www.defence.gov.au/business-industry/industry-governance/defence-security-principles-framework).

Australian Government Information Security Manual

### The Australian Government Information Security Manual (ISM) is the standard, which governs the security of government Information Communications Technology (ICT) systems and complements the PSPF. The ISM can be found at <https://www.cyber.gov.au/ism>.

# GOVERNANCE

Security Policies and Plans (SPP)

### The Security Policies and Plans (SPP) are developed and maintained by the SO to provide all personnel with a guide to their individual security responsibilities.

### All employees are required to read the SPP annually as a reminder of their individual responsibilities. New security-cleared personnel mustread the SPP at the time of their introductory security briefing by the SO.

### While working at Defence establishments, or facilities, security cleared personnel must abide by the applicable local security instructions.

Security Register

### A Security Register (SR) should capture all matters of security interest relevant to <*Entity* *name*>. and is maintained by the SO.

### An SR template is located on the DISP website.

### The SR is a living document and should be updated regularly. Contents may include, but is not limited to:

* Governance
	+ Record of sighting of register by CSO (*Section A1*)
	+ Record of Security Officers (Section A2)
	+ Record of Assistant Security Officers (*Section A3*)
	+ Record of other security appointments (*Section A4*)
	+ Record of current governance documentation (*Section A5*)
	+ Inspections and random spot checks (*Section A6*)
* Physical Security
	+ Record of security containers and door (combination operated) (*Section B1*)
	+ Record of security containers (key operated) (*Section B2*)
	+ Record of security alarm systems (SAS) (*Section B3*)
	+ Security key register (*Section B4*)
	+ Building patrol listing (*Section B5*)
	+ Certifications & Accreditations of PSZ, Armouries & Licensed EO facilities (*Section B6*)
* Personnel Security
	+ Record of temporary access to classified material (*Section C1*)
	+ (Industry) Required Security Assessed Positions (DSAP) register (*Section C2a*)
	+ Record of personnel travelling overseas (*Section C3*)
* Security Education and Training
	+ Record of security education/training (*Section D1*)
	+ Record of new starter briefings/departure briefing (*Section D2*)
* Information Security
	+ Master record of Classified Document Registers (*Section E1)*
* Security Incidents
	+ Record of security incidents (*Section F1*)
* Armouries
	+ Record of innocuous and sectionalised weapons (*Section G1*)
	+ Innocuous weapon certificate (*Section G2*)
	+ Record of Arms Checks (*Section G3*)
	+ Record of privately owned weapons in Defence armouries check (*Section G4*)

Designated / Industry Security Assessed Positions Register

### The CSO or SO is to maintain a Designated / Industry Security Assessed Position list nominating all positions relevant to <*Entity* *name*> that require the occupant to have a security clearance.

### A DSAP is compulsory for all DISP membership levels.

### Personnel are to be security cleared to the level commensurate with the level of classified information or assets they are required to access, or the responsibilities they hold.

### <*Entity* *name’s*> Security Officer is responsible, through direction from the Defence contract manager/s and/or capability manager/s, for identifying positions and assuring those, personnel are suitable to access:

* classified information, materials and assets;
* Defence/Industry Entity ICT systems; and
* classified areas.

### A DSAP Register template is located within the Security register template located on the DISP website.

### *You may wish to include local arrangements about the DSAP in <Entity Name>.*

Report Changes in Foreign Ownership Control and Influence

### DISP members are obligated to report all potential or actual changes to their Foreign Ownership Control and Influence status.

### The CSO and/or SO are to report all FOCI changes by submitting a change in the [DISP Member Portal](https://www.defence.gov.au/business-industry/industry-governance/industry-regulators/defence-industry-security-program/resources/disp-member-portal).

Ongoing Assurance and Uplift Program

### The Annual Security Report (ASR) is a declaration by the CSO, under the authority of the Executive (Board equivalent), that an Entity is continuing to meet the eligibility and suitability requirements of the DISP.

### The ASR is to be submitted to Defence annually on the date DISP membership is granted <insert ASR due date / anniversary of DISP membership grant date>.

### Submit the ASR on the [DISP Member Portal](https://www.defence.gov.au/business-industry/industry-governance/industry-regulators/defence-industry-security-program/resources/disp-member-portal).

### *You may wish to include local arrangements, or where the ASR is kept in <Entity Name>.*

### Ongoing Suitability Assessments (OSA) and Deep Dive Audits are a part of the DISP assurance and uplift program. DISP members must engage with uplift and assurance activities including provision of requested security artefacts to support assurance activities and implementation of recommendations from uplift activities within a mutually agreed timeframe.

Security Risk Assessment

### DISP Members are to maintain Security Risk Assessments (SRA) to identify and manage risks. Additionally, a more specific SRA should be maintained relating to any Defence contract the business is working on.

### Further information on Defence’s policy on SRA’s can be located in the *DSPF Governance and Executive Guidance* document, paragraph 31, and 40-41.

### A *Comprehensive Security Risk Management Guide* is located on the DPN, the DOSD and is available from your Defence contract manager. Further information on SRAs, including the Basic and Comprehensive SRA templates, are available upon request from your Defence contract manager, on the DPN and the DOSD.

### *You may wish to include where the SRA are kept in <Entity Name>.*

Annual Security Awareness Training

### DISP members are to implement annual security awareness training for all personnel. It is the DISP member’s responsibility to determine the best format and content for their business needs.

* Defence engaged personnel are required to complete all training using a Defence-endorsed platform *ADELE (O) Open* (Replaced Campus Anywhere), *Learn eXcel Perform (LXP)* (Replaced Campus) on the DPN or *SCORM package* available through the DOSD for your Learning Management System (LMS).

### Security Awareness training records are to be retained in the Security Register.

### *You may wish to include details about local arrangements for the Annual Security Awareness training within <Entity Name>.*

Insider Threat Program

### DISP members are to implement an Insider Threat awareness program, and make it available to all staff. The following resources are available to assist in the creation of this program. *Insider Threat Template* and *Countering The Insider Threat,* available on the DOSD or by emailing DISP.info@defence.gov.au.

### The Insider Threat Awareness training program completion by staff must be recorded in the Security Register.

### *You may wish to include details about local arrangements for the Insider Threat Program within <Entity Name>.*

Overseas Travel

### All security-cleared personnel contemplating business or private overseas travel are to notify the SO. The traveller must complete an AB644 form as soon as travel is confirmed, and provide the form to the SO. The SO must brief the employee prior to travel and enter details in the SR.

### It is recommended that personnel familiarise themselves with the Department of Foreign Affairs and Trade (DFAT) travel advisory *(Smartraveller website – www.smartraveller.gov.au)* for information relevant to the planned destinations. Classified intelligence advice and information is available on the DOSD and can be used to support an overseas travel brief. If you witness any suspicious activity whilst traveling, please report to your SO.

### On return from overseas travel, the employee will need to complete the second half of the AB644 form and a debrief is to be conducted by the SO. The traveller will also need to submit a change in circumstance for the overseas travel via MyClearance.

### More information concerning overseas travel can be located in the *DSPF Control 44.1 Overseas Travel*, and in the Security Toolkit on the DISP Portal. A copy of the AB644 is available upon request from your Defence contract manager, on the DPN or the DOSD.

### *You may wish to include details about local arrangements for Overseas Travel within <Entity Name>.*

Official Overseas Travel

### It is the responsibility of travelling personnel to advise the SO of any official overseas travel.

### Form AA062 *Overseas Visit Authority* must be completed for all official overseas travel in addition to the AB644*.* The AA062 form is available upon request from your Defence contract manager, on the DPN or the DOSD.

### If travelling to any country with which Australia has a Security of Information Agreement or Arrangement (SIA), or for overseas travel that may involve classified discussions, the traveller, visit organiser or Security Officer must complete and submit to AGSVA, a Request for Visit or Posting Security Clearance Advice form (XP090), which is required to be completed and submitted to securityclearances@defence.gov.au.

### *You may wish to include details about any local arrangements for Official Overseas travel within <Entity Name>.*

Change of Circumstance Reporting

### <*Entity name*> personnel holding security clearances are required to report any changes in circumstance to AGSVA via the [myClearance website](https://www.agsva.gov.au/about/myclearance).

### Changes that may affect suitability to hold a security clearance must be reported, including:

* Change of name or identity, including gender.
* Change in citizenship or nationality.
* Change in significant relationships, including entering into, or ceasing, a marriage, domestic partnership or significant personal relationship.
* Involvement or association with any group, society or organisation.
* Involvement with any individual that may be a security concern.
* Suspicious, unusual, persistent, regular or ongoing contact with foreign nationals.
* Relatives residing in a foreign country.
* Changes of address or share-housing arrangements.
* Residence in a foreign country.
* Change in financial circumstances, including entering into a mortgage, incurring a significant debt, significant change to household income, receiving a lump sum payment or other financial windfall.
* Change of employer.
* External business interests, including business activities with overseas individuals and entities.
* Change in health or medical circumstances.
* Change in criminal history, police involvement and association with criminal activity.
* Disciplinary procedures.
* Illicit or illegal drug use or alcohol problems.
* Changes in religious beliefs.
* Security incidents.
* Overseas travel.
* Identity document replacement following a cyber-hack, including driver’s licence, passport and Medicare card.

Contact Reporting

### A contact is any suspicious or nefarious activity where an employee communicates with representatives of foreign countries; extremist or subversive groups; criminal groups; or political or issue motivated groups or individuals, including the media.

### Espionage represents a threat to the security of Defence and Defence industry. Foreign Intelligence Services (FIS) personnel are skilled in the exploitation of relationships and aim to recruit people with legitimate access to their target area. Private and official contacts, particularly social contacts, are used by foreign representatives to glean information of possible intelligence value or to make character studies of Australian official or business people. Therefore, persons employed within the DISP need to be aware of the possibility of such contacts being made and report them to the SO.

### Any contact, either in Australia or overseas, which is considered to have security significance, is to be reported immediately by completing and submitting Form XP188 **-** *Security Report* to the SO and sent to the Security Incident Coordination Centre – security.incidentcentre@defence.gov.au

### If the DISP member does not have access to the DPN, they may send an email to the Security Incident Coordination Centre at security.incidentcentre@defence.gov.au, providing all details of the contact.

### The Security Incident Coordination Centre manages Contact reporting and can be contacted by emailing security.incidentcentre@defence.gov.au.

### The XP188 form is located on the DOSD or on the DPN at <http://drnet.defence.gov.au/AssociateSecretary/security/services/Pages/incidents-reporting.aspx> .

### *You may wish to include details about any additional local arrangements for Contact Reporting within <Entity Name>.*

Security Incident Reporting

### <*Entity name*> personnel are responsible for reporting security incidents in accordance with *DSPF Principle 77 Security Incidents and Investigations*. The SO should report all security incidents using the online form XP188 - *Security Report* in accordance with the DSPF.

### There are a range of events that are Security Incidents. Below are some examples (please refer to [DSPF Control 77.1 Security Incident Management and Investigation](http://intranet.defence.gov.au/home/documents/home/publications/policy-documents/defence-security-principles-framework.htm) for more):

* Unauthorised access to and/or use of Defence facilities, information and communications equipment or systems;
* Inappropriate handling, storage, loss, theft, or unauthorised access to classified information, weapons, associated equipment, and explosive ordnance;
* Security contacts where Defence personnel are approached by, or communicate with, representatives of foreign interests, extremist or subversive groups, criminals, or commercially, politically or issue motivated groups whose purpose appears to be to obtain official information;
* Any investigation or other action by civil police, that involves Defence people or property and
* Events of actual or suspected espionage and/or sabotage.

### All security incidents must be recorded in the SR. The SO must take necessary action to immediately correct any security deficiencies or any matters which are likely to pose a direct security risk to Entity personnel or classified material, or which threaten to reduce the level of protection being afforded to classified material in <*Entity name*> custody. If you are a part of a criminal act or if a life-threatening situation emerges please call the Police.

### If the DISP member does not have access to the DPN, they may send an email to the Security Incident Coordination Centre at security.incidentcentre@defence.gov.au, providing all details of the incident.

### The Security Incident Coordination Centre manages Security Incident Reports and can be contacted by emailing security.incidentcentre@defence.gov.au.

### The XP188 form is located on the DISP Portal or on the DRN at <http://drnet.defence.gov.au/AssociateSecretary/security/services/Pages/incidents-reporting.aspx>.

### *You may wish to include details about any additional local arrangements for Security Incident Reporting within <Entity Name>.*

Security Officer Training

### Chief Security Officers and Security Officers are required to undertake the Security Officer Training course provided by DISP. The course provides a general understanding of the security environment and responsibilities of an SO. The training has evolved into a self-paced modularised e-learning program, making it more accessible, flexible, and comprehensive. Please email DISP.info@defence.gov.au for an access key to the course.

### Security Officer Training course completion details must be recorded in the Security Register and renewed every three years.

Defence Online Security Dashboard (DOSD)

### Chief Security Officers and Security Officers for DISP members may apply for access to the DOSD.

### The DOSD provides access to the DISP Toolkit, a declassified version of the DSPF, and other security tools and advice via the internet rather than via the Defence Protected Network.

### The DISP team will facilitate DOSD access for the CSO and/or SO at the time of their DISP membership being granted.

### Further access to the DOSD can be requested by emailing the DISP membership management team at disp.info@defence.gov.au.

### The CSO and SOs with Personnel Security membership Level 1 to Level 3 may apply for access to the MyClearancePortal. The myClearance Portal is used for all security clearance related processes, including:

* Updating Chief Security Officer and Security Officer contact details.
* Requesting and removing sponsorship of security clearances.
* Submitting notifiable information reports.
* Requesting priority processing of security clearance assessments.
* Checking progress of security clearance assessments.

### Access to the myClearance Security Officer Portal can be requested by submitting the *SVA 016* myClearance portal request form to DISP.info@defence.gov.au. Find the SVA016 on the DOSD, the DPN or the [AGSVA website](https://www.agsva.gov.au/security-officers/administrative-responsibilities).

Close of Business Security Check

*Delete if not applicable*

### A security check should be conducted at <*Entity name*> at close of business daily, to ensure that all classified material is secured in approved security containers and the Physical Security Zones perimeter(s) is/are secure.

### An optional template for the *Close of Business Security Checklist* is located on the DOSD.

### *You may wish to include details about any additional local arrangements for Close of Business checks within <Entity Name>.*

Emergency Situations

*Delete if not applicable*

### In the event of a fire, civil disturbance or other occurrence that requires evacuation from the facility, where practicable security cleared staff should, prior to leaving:

a. take action to secure all classified material in security containers; or

b. assume personal charge of the classified material and retain it until relieved of the responsibility by the custodian or SO.

### It may be necessary to grant access to the facility for emergency responders while under escort by appropriately security cleared staff.

### *You may wish to include details about any additional local arrangements for emergencies within <Entity Name>.*

# PERSONNEL SECURITY

Employment Screening

### All personnel engaged on Defence will undergo employment screening in line with AS4811-2022.

### *Include details about local arrangements for employment screening within <Entity Name> including reference to supporting policy and/or procedures outlining screening requirements.*

Personnel Security Clearances

### Once a security clearance is granted, the security-cleared personnel must meet their ongoing responsibilities. See the Australian Government Security Vetting Agency (AGSVA) website at <http://www.defence.gov.au/agsva> for responsibilities, including reporting of any change of circumstances.

### <*Entity name*> SO is responsible for the management and ongoing support of personnel holding security clearances. The SO acts as a single point of contact with Australian Government Security Vetting Agency.

### Prior to personnel gaining access to classified material, they are to be briefed by the SO on concerning their responsibilities.

### It is important that once granted a security clearance and access to classified information and material, that personnel meet their ongoing responsibilities as clearance holders. See the AGSVA website at <http://www.defence.gov.au/agsva> for responsibilities.

Security Clearance After-Care

### <*Entity name*> SO is responsible for managing the separation process through a debrief. During the separation debrief, the SO will cover the following requirements:

1. Completion of the XP101 *Declaration of Secrecy on Cessation of Duties* form for departing Defence engaged personnel (a copy of the XP101 is available upon request from your Defence contract manager, on the DPN or the DOSD);
2. report to AGSVA any security concerns arising from the separation;
3. administer or organise debriefs for personnel who have had access to CODEWORD or other compartmented information;
4. notify the compartment controller of the separation and withdraw sponsorship of any compartmented briefings;
5. advise AGSVA:
* that an employee or contractor with a security clearance is separating/has separated;
* if known, which agency or contracted service provider the employee is transferring to; and
1. remind the separating employee of her/his continuing personal obligations under the *Crimes Act 1914* and other relevant legislation.

### The SO will record the details of induction briefings and termination debriefings in the SR.

### Personnel with supervisory responsibilities must advise the SO when there are indications that security cleared personnel have undergone significant changes of personality, attitudes, behaviour, financial or domestic circumstances.

### *You may wish to include details about any additional local arrangements for security clearance aftercare within <Facility Name>.*

Identification (ID) and Access Passes

*Delete if not applicable*

### ID and Access passes are to be used at this <*Facility Name>* within the Physical Security Zones (PSZ). <Facility/*Entity* name> personnel are responsible:

a. to ensure their safekeeping;

b. to wear them visibly at all times within the workplace, ensuring the photograph can be clearly seen;

c. report it to the SO in the event of loss;

d. to ensure that no other person has possession, use or access to their ID or access pass;

e. to challenge anyone not known to them in the facility that is not wearing a pass;

f. to return the ID or access pass to the SO on expiration of the pass, cessation of the requirement to enter any premises requiring the pass, or termination of employment; and

g. personnel are to surrender any Defence access pass to their SO during their debriefing, when ceasing employment.

### Electronic access cards are to be considered a “Security Key” and will be recorded in the SR by the SO. The SO will conduct an annual audit to account for all <*Entity name*> access cards.

### <*Entity* name> personnel who visit Defence premises must wear their Defence Visitor or Defence ID Common Access Card (DCAC), and must be clearly visible at all times.

### *You may wish to include details about any additional local arrangements for ID and Access Passes within <Facility Name>.*

Visitors

### Visitors to <*Entity* name> are not permitted access to classified material until their identity, security clearance and “Need‑to‑Know” has been established.

### *Delete if not applicable:* All visitors to <*Entity* name> must be issued a Visitor’s Pass, which is to be retained and displayed on their person during their visit. The Visitor’s Pass is only valid for the duration of the visit and must be returned upon departure from the site. All visitors are to sign the Visitors Register and are to be escorted by an appropriately security cleared Entity employee at all times. It is the responsibility of the escorting officer to ensure that the visitor’s pass is returned when the visitor leaves the facility.

### *You may wish to include details about any additional local arrangements for visitation access within <Entity Name>.*

Cleaners and Ancillary Staff

*Delete if not applicable*

### Cleaner(s) and other ancillary staff are usually not security cleared and must be escorted at all times within <*Entity name*> by appropriately security-cleared personnel.

### Cleaner(s) and other ancillary staff who are appropriately security cleared may work within the <*Entity name*> PSZ unsupervised. They are not to be given custody of Security Keys under any circumstances and appropriate measures should be taken to ensure they do not have access to classified material.

### *You may wish to include details about any additional local arrangements for cleaners and ancillary staff within <Entity Name>.*

# PHYSICAL SECURITY

*Delete if not applicable*

Physical Certification of Zones

### Level 1 – Level 3 Physical Security DISP members are required to have their facilities certified and accredited in accordance with the DSPF to receive, handle, store and destroy the appropriate level of classified information and material. Certification and accreditation is coordinated by the DISP Team (please contact DISP.info@defence.gov.au).

### **Zone 1**: Self-Certification and Accreditation is required for a Security Zone 1.

### A Security Zone 1 is a public access area within a space or area that has access control measures in place at the perimeter.

### **Zone 2**: entities are recommended to conduct a self-assessment of their Zone 2 facilities through completion of the AE995 - *Physical Security Certification and Accreditation*. The self-assessment template is located upon request from your Defence contract manager, on the DPN or the DOSD. Once completed, the form is to be returned to the appropriate Directorate of Security Assurance (DOSA) regional office or Service Executive Security Adviser for review and endorsement via the DISP team at DISP.info@defence.gov.au.

### Zone 2 can store up to certain levels of classified information and assets in accordance with the PSPF. Refer to the relevant Zone 2 certificate for handling and storage permissions.

### Entities seeking certification or accreditation of **Zone 3 – Zone 5** facilities (not including Zone 5 SCIF), are to email the DISP team at DISP.info@defence.gov.au.

### **Zone 3**: Limited employee and contractor access with visitors escorted within the security zone. Ongoing employees to hold the security clearance at the highest level of the material they access within the Security Zone. Storage of information up to SECRET (and equivalent Security Protected Assets) permitted, provided they are stored within security containers specified within the DSPF/PSPF for the level of material held within the Security Zone.

* As of the 1st of January 2025 Portable Electronic Devices (PEDs) are no longer permitted in security Zone 3s. Contact your Defence contract manager or email DISP.info@defence.gov.au for further information.

### **Zone 4**: Strictly controlled employee access with personal verification as well as card access.  Only contractors and visitors with a need-to- know that are closely escorted are provided access. Where security classified information is stored within the zone, all employees with ongoing access are to hold a security clearance at the highest level of the information held within the zone.

### **Zone 5**: Strictly controlled employee access, with personal identity verification as well as card access (dual authentication access).  Visitors and contractors with a need to know are closely escorted at all times.  Employees with ongoing access to the area are to hold a security clearance and briefings at the highest level of the information held within the Security Zone. Zone 5 areas are where information classified at TOP SECRET, codeword information or large quantities of SECRET information is stored and used or where the aggregate of information would have a catastrophic business impact if compromised.

### **Zone 5 SCIF**: Companies seeking certification or accreditation of Zone 5 Sensitive Compartmented Information Facility (SCIF) are to email the DISP team (DISP.info@defence.gov.au) requesting a site visit. Applicants will then need to submit the *AE851 Request for T4 Certification of a Defence Top Secret or Sensitive Compartmented Information Facility (SCIF)* form, available upon request from your Defence contract manager, on the DPN, or the DOSD.

### *You may wish to include information about the physical certification of <Facility Name>.*

Security Containers

*Delete if not applicable*

### All official and classified material must be stored in approved security containers. Access to the container/s shall be limited to the approved custodian/s.

### *DSPF Principle 72* *Physical Security* outlines the appropriate types of security containers applicable to the various levels of classified material in the various types of PSZ within Australia.

### The SO is to record details of the security containers, their locations and their custodians in the SR.

### *You may wish to include details about any security containers within <Facility Name>, if applicable.*

Use of Security Construction and Equipment Committee Approved Products

*Delete if not applicable*

### The Security Construction and Equipment Committee (SCEC) is responsible for evaluating security equipment for their suitability for use by the Australian Government. The SCEC determines which products will be evaluated, and the priority of evaluation. Evaluated security products protect classified information of which the compromise would result in a bustiness impact level of high or above.

### Approved items are to be listed in the SCEC Security Equipment Evaluated Product List (SEEPL), which is only available to Australian Government security personnel and as well as Defence Industry Security Program members and can be obtained from the [*SCEC website*](https://www.scec.gov.au/application-form)with a copy of your DISP membership certificate.

### For further information, please refer to the [*PSPF* website](https://www.protectivesecurity.gov.au/pspf-annual-release).

### *You may wish to include details about local arrangements of SCEC endorsed equipment at <Facility Name>.*

Keys and Combinations

### The SO maintains a register of all facility keys, security containers, combinations and keys. Each security container must have a custodian appointed who is responsible for the contents and controlling access to the security container.

### Security keys to security containers are to be held only by authorised and appropriately, security cleared personnel. Keys to containers holding classified material are to be regarded as having the same classification as the material held in the containers and must be protected accordingly.

### The SO must maintain a key register. Duplicate keys are not to be made except on the authorisation of the SO and recorded in the key register. An audit of your facility’s keys must be performed at least every six months. The loss or compromise of a security key must be reported in accordance with *DSPF Principle 77* *Security Incidents and Investigations*.

### In the event of a compromise or suspected compromise of a security container, the SO must be informed immediately and an XP188 submitted to Defence (see section 6.13 Security Incident Reporting).

### *You may wish to include details about any additional local arrangements for keys and combinations within <Facility Name>.*

Security Alarm System

*Delete if not applicable*

### <*Facility/Entity name*> utilises a <*enter details of Security Alarm System*> Security Alarm System (SAS) within the PSZ(s).

### The SO will ensure that the SAS is installed, operated, maintained and monitored in accordance with the manufacturer’s specifications and, where applicable, Australian Government specifications.

### The SO shall ensure that detailed instructions are provided to the monitoring station and the contracted response force. Staff responsible for operating the system and responding to call outs will be briefed by the SO on their role and the reporting actions required of them in the event of an alarm, or of any incident which threatens to reduce the effectiveness of the SAS.

### All alarm incidents and response actions are to be reported to the SO. The SO shall investigate all reported incidents, provide advice and take necessary action to correct any security deficiencies immediately. Details of alarm incidents and response actions will be recorded in the SR.

### For further information, Please liaise with your local DoSA office and/or your SCEC consultant for Security Alarm guidance.

### *You may wish to include details about any additional local arrangements for security alarm systems within <Facility Name>.*

Security Guards

*Delete if not applicable*

### < Entityname> has contracted <*insert Guard Entity name*> to provide protective security services at *<Facility Name>*.

### The SO will ensure that detailed guarding instructions are provided to <*insert Guard Entity name*> guards, that they are maintained, and that a backup procedure is in place. The SO will also ensure that the guards and other members of the response team are briefed on their role, and the response and reporting actions required of them in the event of an emergency or other reportable incident.

### For further information, please liaise with your local DoSA office and/or your SCEC consultant for Security Alarm guidance.

### *You may wish to include details about any additional local arrangements for security guards at <Facility Name>.*

# INFORMATION AND CYBER SECURITY

ICT Networks Standard Operating Procedures

### DISP entities with Information and Cyber Security Entry Level membership must meet or exceed the [Australia Signals Directorate’s Essential Eight (E8) at Maturity Level Two](https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model), across all of the corporate ICT systems used to correspond with Defence.

### DISP entities with an Information and Cyber Security Level 1 membership must have a PROTECTED ICT system, with an active accreditation status, in accordance with the Cyber Security Assessment and Authorisation Framework (CSAAF).

### DISP entities with an Information and Cyber Security Level 2 membership must have a SECRET ICT system, with an active accreditation status, in accordance with the CSAAF.

### DISP entities with Information and Cyber Security Level 3 membership must have a TOP SECRET ICT system, with an active accreditation status, in accordance with the CSAAF.

### *If applicable, insert system details of accreditation for the ICT systems, (including AS number and Accreditation expiration date), otherwise delete this point.*

### The ITSO <*insert name and contact details*> is responsible for maintaining the system specific Standard Operating Procedures applicable to ICT systems for <*Entity name*>.

### *If not already included in another ICT policy or procedure document, you may include in this section of the SPPs or in a supporting Annex, details about how security controls are being implemented for the following Mitigation Strategies:*

1. *Patch applications,*
2. *Patch operating systems,*
3. *Multi-factor authentication,*
4. *Restrict administrative privileges,*
5. *Application control,*
6. *Restrict Microsoft Office macros,*
7. *User application hardening, and*
8. *Regular backups.*

Portable Electronic Devices (PED)

*Delete if not applicable*

### <*Facility/Entity name*> has a designated Portable Electronic Device (PED) prohibited area/s. <identify area/s>.

### The authorisation from the SO must be obtained in writing prior to using any PED equipment in the vicinity of classified activities, material or asset/s or within the designated PED prohibited area at <*Facility/ Entity name>.*

### The following items are not to be taken into PED Prohibited Area:

**(The list below can be updated to suit and is provided as an example only)**

* + 1. Laptops
		2. Personal Digital Assistants (PDA)
		3. Mobile Phones
		4. Digital Camera
		5. Audio Recorders
		6. Digital Media i.e. USB and External Hardrives
		7. Cordless Telephone

Car Key Fobs

* As of the 1st of January 2025, Portable Electronic Devices (PEDs) are no longer permitted in security Zones three through five. Contact your Defence contract manager or email DISP.info@defence.gov.au for further information.

### *You may wish to include details about any additional local arrangements for PED at <Facility Name>.*

Audio-Visual Security

*Delete if not applicable*

### It is important to consider audio-visual security to protect classified information from compromise by unauthorised persons through surveillance or other technical collection methods.

### The first line of defence is appropriate protective security. Ensuring that classified information has been communicated appropriately within accredited facilities is the primary measure taken to mitigate audio-visual security risks.

### Access to rooms with audio security measures should be strictly controlled. Access should be limited to authorised persons with the appropriate security.

### For more information, please see the *DSPF Principle 14 and Control 14.1 Audio-Visual Security.*

### *Include the audio-visual security arrangements in place at* *<Facility/Entity name>*

Classified Document Register

*Delete if not applicable*

### All material classified SECRET and above must be registered in a CDR as part of the SR. The CDR is to contain a record of holdings and disposal of material received, generated or dispatched by <*Facility/Entity name*> to provide an audit trail.

### A CDR template is located within the *Security Register Template* at tab E1, available on the DISP website or on the DOSD.

### *You may wish to include details about any additional local arrangements for the CDR at <Facility Name>.*

Classified Document Muster

*Delete if not applicable*

### A document muster of information classified SECRET or TOP SECRET, and other accountable material is to be conducted at least every two years by <*Facility/Entity name*>.

### At the discretion of <*Facility/Entity name*> CSO, a classified document muster will occur:

1. annually, if substantial file holdings exist in the facility;
2. when the CSO, SO or CDR Responsible Members change; and
3. if a security incident or suspected compromise of a file or facility occurs.

### The CDR is SR to be annotated to show the musters and checks have been conducted. Any discrepancies are to be recorded and investigated by the SO, and DS&VS notified in accordance with *DSPF Principle 77* *Security Incidents and Investigations*.

### *You may wish to include details about any additional local arrangements for document musters at <Facility Name>.*

Security Caveats

*Delete if not applicable*

### Security classified information may bear a security caveat in addition to the above security classifications. The caveat is a warning that the information has special requirements in addition to those indicated by the protective marking. Caveats are not classifications in their own right and must not appear without the appropriate protective marking of PROTECTED or above.

### *Detail if any of this information is held.*

Official Information

### Defence official information is classified in accordance with the Australian Government Security Classification System (AGSCS), and protected in a manner that prevents unauthorised access by, or disclosure to, those who do not have a need-to-know and the appropriate security clearance.

### <*Entity name*> personnel using classified material are to ensure that there is no deliberate or casual inspection, or oversight by unauthorised persons. All classified material is to be secured in an approved security container when not in actual use or under direct supervision of an appropriately cleared person with a need-to-know.

### Classified information must be released in accordance with *DSPF Principle 10* and Control 10.1 *Classification and Protection of Official Information*.

### A protective marking assigned to official information indicates the consequence of unauthorised disclosure. It identifies the level of protection that must be provided during use, storage, transmission, transfer and disposal of classified information.

### <*Facility/Entity name*> holds AGSCS Information up to <*insert details LEVEL*> at <*facility name*>. Personnel must use security classifications for the purpose of protectively marking official information.

Delete the classifications not held by the Entityas appropriate.

1. **TOP SECRET** - requires the highest degree of protection as the compromise of the information could cause exceptionally grave damage to national security.
2. **SECRET** - used when the compromise of the information could cause serious damage to national security, the Australian Government, nationally important economic and commercial interests, or threaten life.
3. **PROTECTED** - used when the compromise of the information could cause damage to the Australian Government, commercial entities or members of the public.
4. **OFFICIAL: SENSITIVE** – used when the compromise of the information could cause limited damage to the Australian Government, commercial entities or members of the public. Official: Sensitive information must be stored in a lockable container and disposed of via a SCEC shredder.

### Applying protective marking to official information can be found in the *DSPF Control 10.1* *Assessing and Protecting Official Information*.

### Defence engaged staff are recommended to complete the Assessing and Protecting Official Information Course at the commencement of the engagement with Defence and every two years thereafter. Training completion records are to be retained in the Security Register.

### *You may wish to include any local arrangements for copying, storing and handling of Official and/or Classified information within <Facility Name>*

Transfer of Classified Information/Security Protected Assets

 *Delete if not applicable*

### The security measures required to protect classified information and security protected assets during physical transfer will depend on the protective markings used, the Business Impact Level of the aggregated information or asset, source and destination, and the transfer method used. <Facility/Entityname> personnel who intend to transfer classified information or security protected assets to another person must confirm, prior to transfer, that:

1. the intended recipient has a need-to-know and the required security clearance; and
2. the recipient facility is accredited to the standard required to protect the information or asset.

### The process and further information is detailed within *DSPF Principle 71 and Control 71.1 Physical Transfer of Information and Assets*

### *You may wish to include details about any additional local arrangements for the transfer of classified information/assets at <Facility Name>.*

Copying and Reproduction of Protectively Marked Information

*Delete if not applicable*

### To reduce the risk of compromise, reproducing protectively marked information is to be done only when it is necessary. Reproduction of classified material must be carried out in accordance with the *DSPF Principle 10 and Control 10.1 Assessing and Protecting Official Information*.

### <Facility/Entityname> to detail controls and processes for reproduction of protectively marked information here, or delete if not conducted.

Disposal and Destruction of Protectively Marked Information and Assets

*Delete if not applicable*

### <Facility/Entityname> are to ensure disposal of Commonwealth records is done in accordance with the *Archives* *Act* 1983. Under the *Archives* *Act* it is illegal to destroy Commonwealth records without the permission of the National Archives of Australia, or in accordance with a practice or procedure approved by the National Archives of Australia, unless the destruction is required by law.

### Protectively marked material must not be disposed of by ordinary refuse or recycling collection unless it has already been through a Security Construction Equipment Committee (SCEC) approved destruction process. Only material that is PUBLIC DOMAIN or has already undergone a SCEC approved destruction process can be discarded in ordinary refuse. SCEC approved contractors may carry out disposal and destruction of classified waste. Further guidance can be obtained from the SO.

### For further guidance on approved equipment to shred and destroy classified information and assets, please contact the DISP team at DISP.info@defence.gov.au.

### <Facility/Entityname> destruction will be carried out by a nominated person and witnessed by a responsible person, both of who have been security cleared to the classification of the information or material being destroyed. If SECRET or above, the CDR must be completed and signed by the nominated person and witnessed at the time of disposal.

### The approved method for destruction of classified material at <*facility name*> is <*enter destruction method*> with <*enter type of approved destruction equipment*> located at <*enter location*>.

### <Facility/Entityname> classified waste will be disposed of by the following method;

<*Detail classified waste disposal method, including approved contractor, collection times, and escort arrangements*>

# CONCLUSION

SECURITY IS EVERYONE’S RESPONSIBILITY

### All personnel must be aware of their personal responsibilities in the protection of information and assets.

### Failure by staff to abide by security policies and plans and the regulations outlined in the DSPF may result in DISP membership being terminated and the cancellation of any contracts <*Entity name*> may have with Defence.