SECURITY POLICIES AND PLANS

Entry Level

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](#_Toc202884486)

[2. BUSINESS DETAILS AND DESCRIPTION 5](#_Toc202884487)

[3. POINTS OF CONTACT 6](#_Toc202884488)

[3.1 Defence, DISP 6](#_Toc202884489)

[3.2 Entity Name 6](#_Toc202884490)

[4. RESPONSIBILITIES 6](#_Toc202884491)

[4.1 Chief Security Officer Responsibilities 6](#_Toc202884492)

[4.2 Security Officer Responsibilities 7](#_Toc202884493)

[5. SECURITY POLICY DOCUMENTATION 8](#_Toc202884494)

[5.1 Protective Security Policy Framework 8](#_Toc202884495)

[5.2 Defence Security Principles Framework 8](#_Toc202884496)

[5.3 Australian Government Information Security Manual 8](#_Toc202884497)

[6. GOVERNANCE SECURITY 9](#_Toc202884498)

[6.1 Security Policies and Plans 9](#_Toc202884499)

[6.2 Security Register 9](#_Toc202884500)

[6.3 Designated / Industry Security Assessed Positions Register 10](#_Toc202884501)

[6.4 Report Changes in Foreign Ownership Control and Influence 10](#_Toc202884502)

[6.5 Ongoing Assurance and Uplift Program 10](#_Toc202884503)

[6.6 Security Risk Assessments 11](#_Toc202884504)

[6.7 Annual Security Awareness Training 11](#_Toc202884505)

[6.8 Insider Threat Program 11](#_Toc202884506)

[6.9 Overseas Travel 12](#_Toc202884507)

[6.10 Official Overseas Travel 12](#_Toc202884508)

[6.11 Change of Circumstance Reporting 13](#_Toc202884509)

[6.12 Contact Reporting 13](#_Toc202884510)

[6.13 Security Incident Reporting 14](#_Toc202884511)

[6.14 Security Officer Training 16](#_Toc202884512)

[6.15 Defence Online Security Dashboard (DOSD) 16](#_Toc202884513)

[7. PERSONNEL SECURITY 17](#_Toc202884514)

[7.1 Employment Screening 17](#_Toc202884515)

[7.2 Personnel Security Clearances 17](#_Toc202884516)

[7.3 Security Clearance After-Care 17](#_Toc202884517)

[8. PHYSICAL SECURITY 19](#_Toc202884518)

[8.1 Physical Certification of Zones 19](#_Toc202884519)

[9. INFORMATION AND CYBER SECURITY 20](#_Toc202884520)

[9.1 ICT Networks Standard Operating Procedures 20](#_Toc202884521)

[9.2 Official Information 20](#_Toc202884522)

[10. CONCLUSION 21](#_Toc202884523)

[10.1 SECURITY IS EVERYONES’ RESPONSIBILITY 21](#_Toc202884524)

**ABBREVIATIONS**

|  |  |
| --- | --- |
| AGSVA | Australian Government Security Vetting Agency |
| 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 |
| PSSA | Protective Security Self-Assessment |
| 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> has been 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 which are 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 the 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 CSO 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 Chief Security Officer (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** must be able to obtain and maintain a minimum Baseline Security Clearance.

### < *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. 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 FOCI Declaration (AE250-1).
8. *Please insert any additional CSO responsibilities set by the Entity, if applicable.*

## Security Officer Responsibilities

### The SOis responsible for the development and implementation of the security policies and plans and acts on behalf of the CSO. The SO must be able to obtain and maintain a Personnel Security Clearance at the Baseline level or above, as appropriate with the 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 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. facilitating annual security awareness training of personnel;
6. reporting security incidents and fraud incidents, and contact reports, in accordance with Defence policy; and
7. yearly assurance activities to support the CSO.
8. <*Include additional SO responsibilities as directed by the CSO>*

### **Additional Security 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)*>

# SECURITY POLICY DOCUMENTATION

## Protective Security Policy Framework

### 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 found 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

## Security Policies and Plans

### 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*>. It 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.

### 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 from 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 Assessments

### 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 SRAs can be found 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 will 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 on countries is also available from DISP through the SO. 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 be debriefed by the SO.

### More information concerning overseas travel can be found in the *DSPF Control 44.1 Overseas Travel*, and in the Security Toolkit on the DOSD. A copy of the AB644 from can be obtained on the DISP website or via 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 located on the DISP website 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 reports and can be contacted by emailing security.incidentcentre@defence.gov.au

### The XP188 form is located on the DOSD 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 Contact Reporting within <Entity Name>.*

## Security Incident Reporting

### <*Entity name*> personnel are responsible to report 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 are to be recorded in the SR. The SO should 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 which threaten to reduce the level of protection being afforded to Defence material in <*Entity name*> custody. If you are of a criminal act or 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 DOSD 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.

* 1. 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 DISP membership is granted.

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

# PERSONNEL SECURITY

* 1. 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 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. 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 <Entity Name>.*

# PHYSICAL SECURITY

*Delete if not applicable*

## Physical Certification of Zones

### Entry Level DISP members are required to notify DISP of the physical security arrangements at each facility as part of the membership application process.

### **Zone 1**: Self Certification or 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. No certification or accreditation is required for Zone 1.

### *You may wish to include information about the physical certification of <Entity 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.

### 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.*

## 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 official information are to ensure that there is no deliberate or casual inspection or oversight by unauthorised persons. All Official information is to be secured in an approved security container when not in actual use.

### 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.

1. **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 required 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 information within <Entity Name>*

# CONCLUSION

## SECURITY IS EVERYONES’ 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.