Australian Government
Defence

DISP

Chief Security Officer and Security Officer Roles and Responsibilities

Industry Entities are required to have a Chief Security Officer (CSO) and a Security Officer (SO) to apply for and maintain DISP membership.

The CSO and SO must be Australian citizens and be able to obtain and maintain an Australian Government Vetting Agency (AGSVA) Personal Security Clearance at the highest level of classification that the entity will have access to as part of DISP membership.

Note: DISP will sponsor clearances where required.

For more information on DISP membership refer to the Applying for DISP Membership Fact Sheet

The CSO and SO role can be held by the same person depending on the size and needs of the entity.

The role of a Chief Security Officer

A Chief Security Officer (CSO) is a senior executive within an entity who has oversight of, and responsibility for, security arrangements and championing a positive security culture.

The CSO must be a member of at least one of the organisation's **Australian**:

- Board of directors or similar governing body
- Executive
- Partnership group
- Senior management

They must have the ability to implement policy and direct resources within the entity.

An entity may only have one CSO.

The role of Security Officers

Security Officers (SOs) are individuals within an entity who have delegated authority from the CSO to undertake the day-to-day management of protective security.

Entities may have multiple SOs.

For more information refer to the Defence Security Principles Framework (DSPF) [PDF 10,220 KB].

If you require support, please contact DISP.Info@Defence.gov.au.

Responsibilities of a Chief Security Officer

- Reviewing the DISP membership application for their entity and completing the declaration in the DISP Members Portal, see the Applying for DISP Membership Fact Sheet for more information.

Note: the CSO will not have access to edit the application.

- Meeting all obligations contained in the DSPF [PDF 10,220KB] for their level of DISP membership.
- Reporting any change in the entity's circumstances that may impact its ability to maintain DISP membership (including changes in ownership and control) to Defence.
- Implementing an appropriate system of risk, oversight and management and providing board oversight of the security register.
- Fulfilling DISP reporting obligations and submitting the annual security report for their entity.
- Ensuring that there is security training available for all entity staff.

Responsibilities of Security Officers

- Completing the DISP membership application for their entity, see the Applying for DISP Membership Fact Sheet for more information.

Note: only one SO can have access to complete the DISP Membership application.

- Developing and applying security policies and plans for their entity.
- Maintaining a Designated Security Assessed Positions list and security register including security incident reports, contact reports and overseas travel briefings, and making these available to Defence upon request.
- Sponsoring, managing and withdrawing Personal Security Clearances for the entity, if they hold a minimum Negative Vetting 1 (NV1) Personnel Security Clearance and have the appropriate level of DISP membership. This includes supporting clearance holders to submit change of circumstances [PDF 220KB], incident and contact reports and conducting overseas travel briefings [192KB].
- Facilitating Defence mandated security education and training courses for entity personnel engaged in Defence work.
- Ensuring all Industry Entity staff complete security training, including for insider threat identification, reporting and management.
- Meeting all physical security requirements as per the DSPF Principle 72 [PDF 10,220KB].

Joint responsibilities

- Complying with the requirements of DISP membership.
- Taking part in the Security Awareness Training course and refresher training every three years.

Note: A minimum baseline Personal Security Clearance is required to attend the training. Completion of the course is not required prior to a DISP Membership being granted but you must attest to intent to complete.

- Responding to and reporting any security incidents [PDF 192KB] as soon as possible to Defence.
- Undergoing an interview with Defence to confirm understanding of their security obligations.
- Protecting official, sensitive and classified materials entrusted to the entity in accordance with DSPF requirements [PDF 10,220KB] at all times.
- Notifying Defence in writing of any changes to the CSO or SOs within 14 business days of the change.

If you require support, please contact DISP.Info@Defence.gov.au.