DATA ITEM DESCRIPTION

1. DID Number: DID-ENG-SOL-SSOP-
2. TITLE: SECURITY STANDARD OPERATING PROCEDURE
3. DESCRIPTION AND INTENDED USE

Security Standard Operating Procedures (SSOPs) provide step-by-step guidance to be followed by each different role (eg, system administrator and system operator) required to undertake security-related tasks and processes for a Security System-of-Interest (SSoI) (eg, Mission System) when the SSoI is being operated and sustained. The SSOPs address Information and Communications Technology (ICT) security, cyber security and, if applicable, physical security, and Emanation Security (EMSEC). SSOPs supplement the information provided in the associated System Security Plan(s) (SSP(s)) and the In‑Service Security Management Plan (ISSMP) to:

ensure that all parties involved in operating, supporting and managing a SSoI understand their roles and responsibilities in relation to security;

assist with mitigating the risks associated with security threats;

assist with ensuring that security threats and incidents are appropriately managed and the impacts on the operations of a SSoI are minimised; and

assist with managing and maintaining Security Authorisations over the life of the SSoI.

The Contractor uses the SSOPs:

to document the procedures required to undertake security related tasks and processes for a SSoI; and

as one of the security artefacts to provide assurance to the Commonwealth that the Contractor’s security activities will enable the required Security Authorisations for a SSoI to be achieved.

The Commonwealth uses the SSOPs:

to gain assurance that the Contractor has a sound security program in place that complies with applicable Government and Defence security requirements and policies;

to understand and evaluate the Contractor’s approach to meeting the security requirements of the Contract as part of the system security program;

to identify and understand the Commonwealth’s involvement in the Contractor’s security program, including the monitoring of the Contractor’s program;

as an input to its own planning, including in relation to attaining the required Security Authorisations for the SSoI covered by the SSOPs; and

as one of the suite of security artefacts provided to the relevant Defence authorities as part of obtaining the required Security Authorisations for a SSoI.

1. INTER-RELATIONSHIPS

SSOPs are subordinate to the following data items, where these data items are required under the Contract:

Systems Engineering Management Plan (SEMP);

Contractor Engineering Management Plan (CEMP)

Integrated Support Plan (ISP);

Materiel System Security Management Plan (MSSMP);

In‑Service Security Management Plan (ISSMP);

System Safety Program Plan (SSPP); and

In-service Materiel Safety Plan (ISMP).

SSOPs inter-relate with the following data items, where these data items are required under the Contract:

System Specification (SS) for each different type of SSoI;

the security-related data items required under the Contract (other than those identified under clause 4.1 (eg, SSP));

the safety-related data items (eg, Safety Case Report (SCR) and Hazard Log); and

Verification and Validation (V&V) data items, such as the V&V Plan (V&VP), Verification Cross Reference Matrix (VCRM), Acceptance Test Plans (ATPs), and Acceptance Test Reports (ATRs).

1. APPLICABLE DOCUMENTS

The following documents form a part of this DID to the extent specified herein:

|  |  |
| --- | --- |
| 1. Governing Security Documents | 1. (see the Glossary for the definition of this term) |

1. Preparation Instructions
   1. Generic Format and Content

Subject to clause 6.1.2, the data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled ‘General Requirements for Data Items’.

Where a set of SSOPs is required for an ICT Security Authorisation, the format and content requirements for the SSOPs shall comply with any template for a SSOP issued by Defence in addition to the content requirements set out in clauses 6.1.3-6.1.5 and clause 6.2 of this DID.

The set of SSOPs for a SSoI shall provide sufficient information to satisfy the objectives and purposes set out in clause 3, including to ensure that the information provided in the SSOPs is suitable for the applicable stages of the security design and implementation activities and the Security Authorisation requirements for the SSoI.

Each SSOP shall be consistent with and, where applicable, comply with the Applicable Documents identified at clause 5.

The data item shall include a traceability matrix that defines how each specific content requirement, as contained in this DID, is addressed by sections within the data item.

* 1. Specific Content

Note: Where there are classified aspects to the employment of an SSoI that have not been provided to the Contractor (eg, utilisation of the Mission System in a tactical environment), the Commonwealth will need to supplement the SSOPs provided by the Contractor to incorporate this information before the SSOPs are issued for use.

* + 1. Scope

Each SSOP shall set out the scope of coverage of the SSOP as it relates to the SSoI.

Each SSOP shall identify the set of SSOPs for a SSoI, showing how this SSOP integrates with the set of SSOPs.

* + 1. Roles

The SSOPs shall identify the set of roles that have security responsibilities for the SSoI (eg, security manager, security officer, system administrator, system operator and system support staff) to meet the requirements of the SSP and related documents.

For each identified role, the SSOPs shall address any specific security-related requirements and/or restrictions, such as identifying:

the security clearance requirements and any security-related restrictions (eg, with respect to dual nationality or particular ‘eyes only’);

the personnel who are or will be ‘authorised’ or ‘emergency authorised’ or who are ‘un-authorised’ personnel; and

any role-specific restrictions (eg, limitations on duration in roles, whether individuals can perform multiple roles, and conflicting roles).

* + 1. Procedures

The SSOPs shall document the step-by-step requirements and guidance that must be followed by the individuals performing the roles identified through clause 6.2.2 to meet the requirements of the SSP and related documents.

In meeting the requirements of clause 6.2.3.1, the set of SSOPs shall address the following procedural requirements, as allocated to each of the identified roles:

physical security aspects, such as:

monitoring and managing access control;

identification and management of personnel authorised for entry, distribution and security of physical keys; and

the management and storage of cryptographic keying material;

access and account management;

training, including on-the-job training, in relation to security induction, awareness, responsibilities, incident response, and other matters pertinent to the management, operation and support of the SSoI;

security Preventive Maintenance activities (eg, updating anti-virus software; managing removable media; data backup; event log monitoring; and checking the integrity of physical security devices, EMSEC protection measures, and system software);

security Corrective Maintenance activities (eg, recovering from a system failure caused by a security incident);

managing security incidents, including:

reporting security incidents; and

ensuring that evidence is protected and not lost, deleted or corrupted;

disaster recovery;

system updates and upgrades, including Software Configuration Management and Software Release management;

supply chain security; and

general security matters applicable to all system users and maintainers, such as:

who has responsibility for which aspects of security;

warnings that user’s actions may be audited and users will be held accountable for their actions;

guidelines on choosing and protecting passwords;

guidelines on enforcing need-to-know on the system;

what to do in the case of a suspected or actual security incident;

the highest level of classified material that can be processed on the system and handling procedures for classified information;

start of day/shift/operations;

securing the system or workstation when temporarily absent;

securing the system or workstation at the end of the day/shift/operations;

controlling and sanitising media;

adding, removing, decommissioning and undertaking destruction of equipment and media;

physical data transfer between network enclaves or environments;

labelling, handling and disposing of hardcopy;

preventing overview of data by visitors;

what to do for hardware and Software Maintenance; and

other operational and security tasks and activities as allocated by the system managers/authorities.