ICT Standards

System Security Plan Template

Document number: ISMF-ICT/3.03 - ICT Security/MISP/SD/SSP Template
Version: 1.20
1  Document control
### 1.1 List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MISP</td>
<td>Ministry Information Security Program</td>
</tr>
<tr>
<td>ISO</td>
<td>Information Security Office</td>
</tr>
<tr>
<td>AA</td>
<td>Approving Authority</td>
</tr>
<tr>
<td>CA</td>
<td>Certification Authority</td>
</tr>
<tr>
<td>SSP</td>
<td>System Security Plan</td>
</tr>
<tr>
<td>BCP</td>
<td>Business Continuity Plan</td>
</tr>
<tr>
<td>DRP</td>
<td>Data Recovery Plan</td>
</tr>
<tr>
<td>C&amp;A</td>
<td>Certification and Accreditation</td>
</tr>
<tr>
<td>MOU</td>
<td>Memo of Understanding</td>
</tr>
<tr>
<td>NDA</td>
<td>Non Disclosure Agreement</td>
</tr>
</tbody>
</table>
1.2 **Purpose of this Document**

The System Security Plan Template is an attachment to the MISP Policy and MISP Handbook. It is part of the ICT Security package that has been produced within the scope of the ICT Standards project. This project is one of the three sub-projects executed under the global project name “Software Development and Technical Assistance for NISFED, e-Government and ICT Standards Applications”, started 20/08/2006 and rolled out within the scope of the ISMF programme¹.

---

¹ For a complete list of documents related to the ICT Standards project, refer to the Project Master Plan; ISMF-ICT/3.01, V.2.00.
2 Executive Summary

Notes The Executive Summary provides a quick management-level reference. It should be a one-page summation of the major aspects of the System Security Plan (SSP).

- The SSP should be consistent with the MISP Handbook
- Make sure every page of the SSP is labeled “SENSITIVE” in the header, footer, or watermark
3 System Identification

3.1 System Name / Title

Notes  □  Unique identifier & name given to the system

3.2 Responsible Directorate

Notes  □  Directorate responsible for the system

3.3 Information Contact(s)

Notes  □  Identify the owner(s) of the system and at least one other manager expertly knowledgeable about it.
  □  Name
  □  Title
  □  Address
  □  Phone Number
  □  Fax Number
  □  E-mail Address

3.4 Assignment of Security Responsibility

Notes  □  Identify the person(s) responsible for security of the system and an alternate emergency contact.
  □  Name
  □  Title
  □  Address
  □  Phone Number
  □  Fax Number
  □  E-mail Address

3.5 System Operational Status

Notes  □  If more than one status is selected, list which part(s) of the system are covered under each status designation.
  □  Operational
  □  Under Development
  □  Undergoing a major modification

3.6 General Description / Purpose
3.7 System Environment

3.8 System Interconnection / Information Sharing

3.9 Applicable Laws or Regulations Affecting the System

3.10 Information Sensitivity and Criticality Assessment
4 Management Controls

This section describes the management control measures that are intended to meet the protection requirements of the MISP. Management controls focus on the management of the IT security for a system and the management of risk for a system.

4.1 Risk Assessment and Management

Notes  
- Describe the risk assessment methodology used to identify the threats and vulnerabilities of the system. Make sure the methodology specifically identifies threats, vulnerabilities, and additional security controls required/implemented to mitigate risks.
- List the group that conducted the assessment, and the date(s) the review was conducted.
- If there is no system risk assessment, include a milestone date (month and year) for completion of the assessment. If the risk assessment is more than 3 years old, or if a major modification has occurred since the previous risk assessment, make sure the SSP includes a milestone date for completion of a follow-up risk assessment.

4.2 Review of Security Controls

Notes  
- List any independent security reviews conducted on the system in the last three years.
- Include information about the type of security evaluation performed, who performed the review, the purpose of the review, the findings, and the actions taken as a result.

4.3 Rules of Behaviour

Notes  
- A set of rules of behaviour in writing must be established for each system. These System Rules of Behaviour should be made available to every user prior to the user receiving access to the system, with a signature page to acknowledge receipt.
- The rules of behaviour should clearly delineate responsibilities and expected behaviour of all individuals with access to the system. They should state the consequences of inconsistent behaviour or non-compliance. They should also include appropriate limits on interconnections to other systems.
- Attach the rules of behaviour for the application as an appendix and reference the appendix number in this section or insert the rules into this section.
- For an example RoB document, see Rules of Behaviour, ref ICT Security/MISP/SD/C&A

4.4 Planning for Security in the Life Cycle

Notes  
- Although a computer security plan can be developed for system at any point in the life cycle, the recommended approach is to design the plan at the beginning of the life cycle.
- It is recognized that in some cases, at any one time the system may be in several phases of the life cycle. For example, a large human resources system may be in the operation/maintenance phase, while an older, batch-oriented input sub-system is being replaced by a new, distributed, interactive user interface. In this case, the life cycle phases for
the system include the disposal phase (data and equipment) related to the retirement of the
batch-oriented transaction system, the Build (acquisition) phase associated with the
replacement interactive input system, and the Operations/Maintenance phase for the balance
of the system.

- In this section of the Plan, determine which phase(s) of the life cycle the system, or parts of
  the system, are in. Identify how security has been handled during each of the listed
  applicable life cycle phases.
  - Planning
  - Definition
  - Analysis
  - Design
  - Build
  - Implementation
  - Operations/Maintenance
  - Disposal

- If the system is in the build phase, make sure the SSP contains the following information:
  - Security requirements that are identified during the design phase.
  - Security controls that test the procedures developed before procurement.
  - Solicitation documentation that includes security requirements and evaluations test
    procedures.

- If the system is in the Implementation phase, make sure the SSP contains the following
  information:
  - Description of when design review and system tests were conducted and who
    conducted them.
  - Testing schedule and procedures for controls implemented after initial testing and
    acceptance.
  - References to test procedure documentation.
  - Description of whether such documentation is kept up to date

- If the system is in the Operational phase, make sure the SSP contains the following
  information:
  - Description of the security operations and administration, including information
    pertaining to backup procedures, training for users and administrators, management of
    cryptographic keys, maintenance of user and administrative privileges, and updating
    security.
  - Description of the process for ensuring operation assurance.
  - Description of auditing processes used to maintain system operational assurance.

- If the system is in the disposal phase, make sure the SSP contains the following
  information:
  - Requirements and procedures for secure transfer and/or long-term storage of data.
  - Requirements and procedures for media sanitization.

### 4.5 Certification and Accreditation

**Notes** Certification consists of a technical evaluation of a sensitive application to see how well it
meets security requirements. Accreditation is the official management authorization for the
operation of an application and is based on the certification process as well as other
management considerations. Certification (or recertification) is required at least once every
three years; an application must also be recertified if the system undergoes a major modification.

The ISO uses the certification report to evaluate certification evidence, decides on the acceptability of the security safeguards, approves corrective actions, ensures the corrective actions are implemented, and issues the accreditation statement however the more sensitive the application, the higher the management level of the accrediting official should be.

- Describe who is responsible for certifying and accrediting the system, the process for performing the C&A, when those actions occurred, and what the results were.
- Provide the date of authorization, name, and title of management official authorizing processing in the system.
- If not authorized, provide the name and title of manager requesting approval to operate and date of request.
- Attach Certification and Accreditation memos, if they exists
5 Operational Controls

This section describes the operational control measures that are intended to meet the protection requirements of MISP. Operational controls are security controls that are primarily implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise, and often rely upon management activities as well as technical controls.

5.1 Personnel Security

- Have all positions been reviewed for sensitivity level?
- Have individuals received background screenings appropriate for the position to which they are assigned?
- Is user access restricted to the minimum necessary to perform the job?
- Is there a process for requesting, establishing, issuing, and closing user accounts?
- Are critical functions divided among different individuals (separation of duties)?
- What mechanisms are in place for holding users responsible for their actions?
- What are the friendly and unfriendly termination procedures?
- Describe the process used for requesting, establishing, issuing, and closing user accounts.

5.2 Physical and Environmental Protection

- Discuss the physical protection in the area where system processing takes place (e.g., locks on terminals, physical barriers around the building and processing area, etc.).
- Factors to address include physical access, fire safety, and failure of supporting utilities, structural collapse, plumbing leaks, interception of data, mobile and portable systems.
- Describe controls to prevent data interception from direct observation, interception of data transmission, and electromagnetic interception.

5.3 Production, Input and Output Controls

- The controls used to monitor the installation of system software updates should be listed. Below is a sampling of topics that may be reported in this section:
  - Are there procedures to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information?
  - Are there procedures for ensuring that only authorized users pick up, receive, or deliver input and output information and media?
  - Are there audit trails for receipt of sensitive inputs/outputs?
  - Are there procedures for restricting access to output products?
  - Is there internal/external labelling for sensitivity
  - Is there external labelling with special handling instructions (e.g., log/inventory identifiers, controlled access, special storage instructions, release or destruction dates)?
  - Are there audit trails for inventory management?
Is there a media storage vault or library containing physical, environmental protection controls/procedures?

- Are there procedures for sanitizing electronic media for reuse?
- Are there procedures for controlled storage, handling, or destruction of spoiled media or media that cannot be effectively sanitized for reuse?
- Are there procedures for shredding or other destructive measures for hardcopy media when no longer required?

State whether or not the system employs Configuration Management (controls and documents changes to the system and its operational environment, and assesses the IT Security impact of any changes), and in what manner it does. If it does not, state why and/or when it will be implemented.

5.4 Contingency Planning and Disaster Recovery

Notes

- Briefly describe the procedures (contingency plan) that would be followed to ensure that the system continues to be processed if the supporting IT system were unavailable.
- If a formal contingency plan has been completed, reference the plan. A copy of the contingency plan may be attached as an appendix.
- Include descriptions for the following:
  - Agreements of backup processing
  - Documented backup procedures including frequency (daily, weekly, monthly) and scope (full, incremental, and differential backup)
  - Location of stored backups and generations of backups
- Are tested contingency/disaster recovery plans in place? How often are they tested?
- Are all employees trained in their roles and responsibilities relative to the emergency, disaster, and contingency plans?
- Coverage of backup procedures, e.g., what is being backed up?

5.5 System Configuration Management Controls

Notes

- Are there restrictions/controls on those who perform hardware and software maintenance and repair activities?
- Are there special procedures for performance of emergency repair and maintenance?
- Are there procedures used for items serviced through on-site and off-site maintenance (e.g., escort of maintenance personnel, sanitization of devices removed from the site)?
- Are there procedures used for controlling remote maintenance services where diagnostic procedures or maintenance is performed through telecommunications arrangements?
- Are software warranties managed to minimize the cost of upgrades and cost-reimbursement or replacement for deficiencies?
- Was the system software developed in-house or under contract?
- Does the Ministry own the software? Was it received from another entity?
- Is the system software a copyrighted commercial off-the-shelf product or shareware?
- Has the software been properly licensed, and have enough copies been purchased for the system?
- Are there organizational policies against illegal use of copyrighted software and shareware?
Are periodic audits conducted of users' computers to ensure that only legal licensed copies of software are installed?

What products and procedures are used to protect against illegal use of software?

Describe any formal change control process in place.

Is there version control that allows association of system components to the appropriate system version?

Are all changes to the system software or system components documented?

Are there impact analyses to determine the effect of proposed changes on existing security control to include the required training for both technical and user communities associated with the change in hardware/software?

Are there change identification, approval, and documentation procedures?

Are there procedures for ensuring contingency plans and other associated documentation are updated to reflect system changes?

Does the change control process require that all changes to the system software be tested and approved before being put into production?

Are there procedures for testing and/or approving system components (operating system, other system, utility, applications) prior to promotion to production?

Is test data live data or made-up data?

Do test plans trace back to the original security requirements?

Are test results documented?

### 5.6 Data Integrity / Validation Controls

#### Notes

- Is virus detection and elimination software installed? If so, are there procedures for updating virus signature files, automatic and/or manual virus scans, and virus eradication and reporting?
- Are reconciliation routines used by the system, i.e., checksums, hash totals, record counts? Include a description of the actions taken to resolve any discrepancies.
- Are integrity verification programs used by the system to look for evidence of data tampering, errors, and omissions?
- Is an intrusion detection tool installed to monitor the system?
- Are procedures in place to handle and close out security incidents?
- Are other network security software packages used?
- Is system performance monitoring used to analyze performance logs in real time to look for availability problems, including active attacks, and system and network slowdowns and crashes?
- Is penetration testing performed on the system? If so, what procedures are in place to ensure that tests are conducted appropriately?
- Is message authentication used in the system to ensure that the sender of a message is known and that the message has not been altered during transmission?

### 5.7 Documentation

#### Notes

Documentation includes descriptions of the hardware and software, policies, procedures, and approvals related to automated information security in the system.
Documentation should also include descriptions of user and operator procedures, and backup and contingency activities.

- List the documentation maintained for the system. Examples may include:
  - Vendor documentation of hardware/software
  - Functional requirements
  - Design specifications
  - Source code documents
  - Testing procedures and results
  - Records of verification reviews/site inspections
  - Standard operating procedures
  - User and Technical manuals
  - Emergency procedures
  - Contingency plans
  - Risk assessments
- Describe the procedure used to update this documentation
- List the physical location of documentation

5.8 Security Awareness and Training

Notes
- Describe the type and frequency of system-specific training provided to employees and contractor personnel (workshops, formal classroom, focus groups, role-based training, and on-the-job training).
- Describe the procedures for assuring that employees and contractor personnel have had adequate training.
- Describe the awareness program for the system.

5.9 Incident Response Capability

Notes
- Are there procedures for reporting incidents handled either by system personnel or externally?
- Are there procedures for recognizing and handling incidents, i.e., what files and logs should be kept, who to contact, and when?
- Who receives and responds to alerts/advisories, e.g., vendor patches, exploited vulnerabilities?
- What preventive measures are in place, i.e., intrusion detection tools, automated audit logs, penetration testing?
6 Technical Controls

This section describes the technical control measures that are intended to meet the protection requirements of the system. Technical controls are security controls that the computer system executes. The controls can provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. The implementation of technical controls, however, always requires significant operational considerations, and should be consistent with the management of security within the Ministry.

6.1 Identification and Authentication

Notes

- Describe the system's user authentication control mechanisms (password, token, and biometrics).
- Indicate the frequency of password changes, describe how changes are enforced, and identify who changes the passwords (the user, the system administrator, or the system).
- Provide the following if an additional password system is used in the system:
  - Password length (minimum, maximum)
  - Allowable character set
  - Password aging time frames and enforcement approach
  - Number of generations of expired passwords disallowed for use
  - Procedures for password changes (after expiration and forgotten/lost)
  - Procedures for handling password compromise
  - Procedures for training users and the materials covered
- Describe the level of enforcement of the access control mechanism (network, operating system, and system)
- Describe how the access control mechanism supports individual accountability and audit trails (e.g., passwords associated with a user ID that is assigned to a single person)
- Describe the self-protection techniques for the user authentication mechanism (e.g., passwords encrypted while in transmission, automatically generated, or checked against a dictionary of disallowed passwords)
- State the number of invalid access attempts that may occur for a given user ID or access location (terminal or port) and describe the actions taken when that limit is exceeded
- Describe the procedures for verifying that all system-provided administrative default passwords have been changed
- Describe the procedures for limiting access scripts with embedded passwords (e.g., scripts with embedded passwords are prohibited, scripts with embedded passwords are only allowed for batch systems)
- Describe any policies that provide for bypassing user authentication requirements, single-sign-on technologies (e.g., host-to-host, authentication servers, user-to-host identifiers, and group user identifiers) and any compensating controls
- Describe any use of digital or electronic signatures and the standards used. Discuss the management procedures for key generation, distribution, storage, and disposal.
- Make sure the following controls are stated. Describe:
  - Procedures for training users and the subjects that are covered
  - How biometric controls are used and implemented
  - How token controls are used and implemented
Cryptographic key management procedures for key generation, distribution, storage, entry, use, destruction, and archiving

6.2 Logical Access Controls

Notes

Discuss the controls in place to authorize or restrict the activities of users and personnel within the system. Describe hardware or software features that are designed to permit only authorized access to or within the system, to restrict users to authorized transactions and functions, and/or to detect unauthorized activities (i.e. access control lists [ACLs]).

- How are access rights granted? Are privileges granted based on job function?
- Describe the system's capability to establish an ACL or register.
- Describe how users are restricted from accessing the operating system or other system resources not required in the performance of their duties.
- Describe controls to detect unauthorized transaction attempts by authorized and/or unauthorized users. Describe any restrictions to prevent users from accessing the system outside of normal work hours or on weekends.
- Indicate after what period of user inactivity the system automatically blanks associated display screens and/or disconnects inactive users. After what period of user inactivity does the system require the user to enter a unique password before reconnecting?
- Indicate if encryption is used to prevent access to sensitive files as part of the system access control procedures.
- Describe the rationale for electing to use or not use warning banners, and provide an example if banners are used.
- Make sure the following controls are stated. Describe:
  - How separation of duties is enforced to prevent an individual from having all necessary authority or information access to allow fraudulent activity without collusion.
  - How the Access Control Lists (ACLs) are maintained.
  - How often ACLs are reviewed to identify and remove users who have left the organization or whose duties no longer require access to the application.
  - Policy or logical access controls that regulate how users may delegate access permissions or make copies of files or information accessible to other users.
  - What other hardware or technical control is used to provide protection against unauthorized system penetration and other known Internet threats and vulnerabilities if the system is connected to the Internet or other wide area network(s).
  - Any port protection devices used to require specific access authorization to the communication ports, including the configuration of the port protection devices, and if additional passwords or tokens are required.
  - How host-based authentication is used.

6.3 Public Access Controls

Notes

If the general public accesses the system, discuss the additional security controls used to protect the system's integrity
What additional controls are used to protect the confidence of the public in the system? Such controls include segregating information made directly accessible to the public from official Government records. Others may include:

- Some form of identification and authentication
- Access controls to limit what the user can read, write, modify, or delete
- Controls to prevent public users from modifying information in the system
- Digital signatures
- CD-ROM for on-line storage of information for distribution
- Copies of information for public access available on a separate system
- Controls to prohibit the public from accessing live databases
- Verification that programs and information distributed to the public are virus-free
- Audit trails and user confidentiality
- System and data availability
- Legal considerations

6.4 Audit Trails

Notes

- Does the audit trail support accountability by providing a trace of user actions?
- Are audit trails designed and implemented to record appropriate information that can assist in intrusion detection and remediation? Does the audit trail include sufficient information to establish what events occurred and who (or what) caused them (e.g., type of event, when the event occurred, user ID associated with the event, program or command used to initiate the event)?
- Is access to online audit logs strictly enforced?
- Is the confidentiality of audit trail information protected if it records personal user information?
- Describe how frequently audit trails are reviewed and whether guidelines exist.
- Does the appropriate system level administrator review audit trails following a known system software problem, an unexplained system or user problem, or a known violation of existing requirements by a user?

Make sure the following controls are stated. Describe:

- How audit trails are designed and implemented to record appropriate information to assist in intrusion detection.
- How audit trails are used as online tools to help identify problems other than intrusions as they occur.
- How implemented audit trails are sufficient to establish what events occurred and who (or what) caused them.
- How separation of duties between security personnel who administer the access control function and those who administer the audit trail is used and enforced.
- How the appropriate system-level or application-level administrator reviews the audit trails following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem.
- How audit analysis tools, such as those based on audit reduction, attack signature, and variance techniques, are used in a real-time or near-real-time fashion.