



## Information Security Management System

*Complies with ISO 27001:2013*

*(c) [Copyright 2021] Islamic World Educational, Scientific and Cultural Organization; All rights reserved.  
This document may contain proprietary information and may only be disclosed to third parties with the  
approval of management. The document is not controlled unless otherwise specified; Uncontrolled  
documents are not subject to an update notification.*





### Document Control

Item	Description			
<b>Document Title:</b>	Information Systems Security Policy			
<b>Doc Ref.</b>	ICESCO-ISMS-POL02-V03	<b>Version:</b>	03	
<b>Classification</b>	<input type="radio"/> Top Confidential	<input type="radio"/> Confidential	<input checked="" type="radio"/> Internal Use	<input type="radio"/> Public
<b>Status:</b>	Current	<b>Type:</b>	Policy	
<b>Release Date:</b>	10/08/2022			
<b>Revision Date:</b>	22/08/2022			

Version No.	Date	Author(s)	Position	Remarks
01	10/08/2022	Oussama Abdelalim	<b>Chief Information Security Officer</b>	First Version of the Document
02	15/08/2022	Oussama Abdelalim	<b>Chief Information Security Officer</b>	Reviewed and updated
03	22/08/2022	Sally Mabrouk	<b>IT Supervisor</b>	Reviewed and updated

### Document Review and Approval History

Version No.	Date	Reviewer(s)	Remarks
03	22/08/2022	<b>IT Supervisor</b>	Reviewed

Version No.	Date	Approver(s)	Name	Remarks	Signature
03	1/09/2022	<b>IT Supervisor</b>	Dr. Sally Mabrouk	Approved	
03	16/09/2022	<b>Director General Head of ICESCO Information Security Committee</b>	H.E. Dr.Salim M.Almalik	Approved	

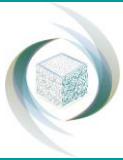


## Table of Contents

1. Object .....	5
2. Scope .....	5
3. Terminologies and abbreviations .....	5
4. Reference document.....	5
5. OBJECTIVES OF THE ISSP .....	5
6. CONSTRAINTS.....	6
7. GENERAL INFORMATION SECURITY RULES.....	6
7.1. Information Security Policy .....	6
7.2. Information Security Organization.....	6
7.2.1. Internal organization.....	6
7.2.2. Mobile devices.....	7
7.3. Human resources security .....	7
7.4. Asset Management .....	8
7.5. Access control.....	8
7.6. Cryptography .....	9
7.7. Physical and Environmental Security.....	9
7.7.1. Secure area .....	9
7.7.2. Materials.....	9
7.8. Operational safety.....	9
7.8.1. Operating Procedures and Responsibilities .....	9
7.8.2. Malware protection.....	10
7.8.3. Backup.....	10
7.8.4. Logging and monitoring .....	10
7.8.5. Mastery of software in operation: .....	11
7.8.6. Technical Vulnerability Management:.....	11
7.8.7. Information Systems Audit Considerations.....	11
7.9. Communications Security .....	11
7.9.1. Network Security Management.....	11



7.9.2.	Transfer of Information .....	12
7.10.	Supplier Relations .....	12
7.10.1.	Security in supplier relations.....	12
7.10.2.	Service Delivery Management .....	12
7.11.	Information Security Incident Management.....	13
7.11.1.	Information Security Incident Management and Improvement .....	13
7.12.	Information Security Aspects in Business Continuity Management .....	14
7.12.1.	Continuity of information security .....	14
7.12.2.	Redundancy .....	14
7.13.	Compliance .....	14
7.13.1.	Compliance with legal and regulatory obligations .....	14
7.13.2.	Information Security Review .....	15



## 1. Object

ICESCO has set itself the objective of continuously demonstrating its ability to evolve its information systems management methods in order to satisfy all interested parties. Achieving this objective requires working in a secure environment to preserve the confidentiality, integrity and availability of ICESCO's information assets.

This policy, which must be scrupulously applied, guides and determines the appropriate and secure uses of the information system and all information assets by all users.

## 2. Scope

This information systems security policy applies to the scope of the information security management system.

## 3. Terminologies and abbreviations

ISSP: Information Systems Security Policy

## 4. Reference document

ISO 27001

WSIS ICESCO Policy

## 5. OBJECTIVES OF THE ISSP

The main objective of the Information Systems Security policy is to put in place rules and principles concerning the use and protection of information, throughout its life cycle.

These rules and principles derive from the international standards ISO/IEC ISO27001 and ISO/IEC 27002 and other relevant regulations and best practice standards.

The basis of this policy is based on the establishment of an Information Security Management System (ISMS) which sets a framework within which the processing of information and the operation of information systems must evolve and defines the basis for continuous improvement in this area.

The Management System aims to formally assign all corporate responsibilities for information protection. It defines a governance structure that allows for ongoing management of security risks, as well as the scope of the scope of information security.

Subsequently, directives, procedures and guides will follow for the implementation of the information security policy.

It aims, among other things, to:



- Protect know-how and sensitive data, related to the activities of the organization.
- Guarantee the availability, integrity and confidentiality of the information system, and the information itself.
- Ensure that the inventory of resources is established and updated and secured in accordance with the classification of information.
- Ensure the implementation of a risk management process according to a documented method for all critical processes.
- Ensure continuous improvement of information security.
- Integrate required security requirements into an agreement for subcontractors and suppliers.

## 6. CONSTRAINTS

It is imperative to comply with all legal, regulatory, normative or contractual obligations as well as information security requirements, as well as the protection of intellectual property rights. In addition, associated with this policy a set of documents have been created and are to be implemented to comply with Information Security Management processes.

## 7. GENERAL INFORMATION SECURITY RULES

### 7.1. Information Security Policy

- Management should establish an Information Security Policy that reflects its will and commitment to the implementation and maintenance of an information security management system.
- The ISSP document should be approved by management and communicated appropriately to all interested parties.
- The information security policy should be reviewed and updated annually or in the event of major changes affecting information security.

### 7.2. Information Security Organization

#### 7.2.1. Internal organization

- The Branch ensures that security values and guidance are shared by all institutional managers and staff.

To this end:

- She ensures the application of the policy in the organization.



- It provides the necessary financial and logistical support for the implementation and application of the policy.
- It sets up an appropriate organization and appoints an Information Systems Security Officer.
- It establishes and assigns all responsibilities for information security.
- Information security objectives should be integrated into the objectives of ICESCO projects;
- In this sense, any project involving the implementation of an information system should be subject to an analysis of information security risks and validation by the CISO;
- As part of its compliance with legal and regulatory requirements, ICESCO maintains appropriate relations with the competent authorities.
- Information security actors maintain appropriate relationships with interest groups, security forums and professional associations.

### 7.2.2. Mobile devices

- Users should take care of the mobile devices entrusted to them.
- They are also responsible for ensuring that their data is kept secure and regularly backed up;
- Computer protection devices installed on mobile devices such as antivirus programs or personal firewalls should never be disabled and should always operate at full capacity;
- It is forbidden to connect to systems outside the ICESCO network without the use of secure means;
- The employee must ensure that the mobile devices assigned to him are always under surveillance if not that they are stored in a locked and secure place;
- Employees are responsible for the equipment during their travels;
- Employees are responsible for communicating any problems with the operation of mobile devices to IT teams;
- In the event of theft or loss of a mobile device, the user must urgently change his access codes and passwords to reduce the likelihood of information leakage.

### 7.3. Human resources security

- During the recruitment process, ICESCO must ensure that employees and contractors understand their responsibilities and are qualified for the roles they are being considered.
- Checks are conducted on all job applicants in accordance with laws, regulations and ethics.
- Contractual agreements between employees and contractors specify their responsibilities and those of the organization with respect to information security.
- Security charters are issued and communicated to employees who agree to apply information security rules in accordance with the policies and procedures in force in the organization.



- In the event of a breach of information security, sanctions will be applied based on the disciplinary process in force which is governed by the Labour Code;
- All employees and third-party users must return all of the organization's assets in their possession at the end of the period of employment, contract or agreement.
- At the end of the contract or in the event of mobility, ICESCO withdraws the access rights of the person concerned and all the information systems to which he or she had access.

#### 7.4. Asset Management

- An inventory of hardware and software assets should be established and maintained periodically.
- A framework for the classification and handling of information assets should be established and implemented;
- The classification rules and data protection measures are defined and communicated in this policy, the procedures and the related charters.
- 

#### 7.5. Access control

- A policy for managing privileged rights on network equipment, systems and applications based on a prior analysis of security requirements, based on business needs, must be applied;
- Permissions and access rights must be granular and aligned with business needs;
- The human resources department must notify the IS administrators for each change in a user's status in order to adapt the rights and/or disable the user account altogether;
- All ICESCO users must comply with the clauses of the IT charter as well as this ISSP in terms of securing authentication information;
- Security measures and prohibitions are applied, namely:
  - The identifiers have a length (min) of 8 characters,
  - The lifetime of passwords is 120 days,
  - The password must be complex (3 or 4 types of lowercase, uppercase, numbers and special non-alphanumeric characters)
  - Prevent trivial passwords (birthday, first name, last name...)
  - Enable account lockout after 5 failed attempts.
  - Default accounts are de facto disabled,
  - No account is shared between multiple users,
  - No user is an administrator of his workstation,
  - Communicate your password to others,
  - Store your passwords in a clear or paper file,
  - Store passwords in an easily accessible place,





- Use passwords related to you (name, date of birth, ...),
- Use the same password for different access.

## 7.6. Cryptography

In case of sending an email with confidential information, it is strongly recommended to encrypt the content or attachment(s) before sending.

## 7.7. Physical and Environmental Security

### 7.7.1. Secure area

Naturally, all ICESCO premises must be protected against external access.

Physical access rights to ICESCO's rooms and technical rooms should be reviewed regularly;

It is necessary to ensure that the entry/exit of visitors to ICESCO premises and machine rooms are recorded.

### 7.7.2. Materials

It is necessary to establish a process of maintenance in operational condition of the general services (loads of the inverters, generator, automatic fire extinguishers, review of the fire extinguishers, air conditioning, ...), and to ensure through periodic tests;

A network connection plan should be drawn up;

All cables must be properly labelled;

Cables must be protected against interference and unauthorized interception. In addition, they should not be confused with telephone cables;

No cable shall pass through a place accessible to the public;

All sensitive paper documents must be systematically destroyed with shredders;

The disposal of physical, optical and magnetic media (CD, DVD, hard disk, DAT, etc.) can only be done once their data has been destroyed.

## 7.8. Operational safety

### 7.8.1. Operating Procedures and Responsibilities

Operating procedures must be documented, maintained and available to the users concerned;

Daily operating activities must be documented in such a way that they can be maintained in the absence of the usual attendant;



A change management procedure should be defined and documented to ensure satisfactory control of all changes to hardware, software or software packages;

#### 7.8.2. Malware protection

An antivirus must be installed, updated as often as necessary on each machine (workstations, laptops and servers);

Viral filtering of attachments accompanying emails must also be carried out;

A complete antiviral, anti-spyware scan of the machines must be performed at least once a week;

In the event that for compatibility reasons or it is not possible to install an antivirus on a machine, an integrity check of sensitive files must be set up.

#### 7.8.3. Backup

It is important to identify the data that needs to be backed up and the owner should set the backup level;

Safeguarding procedures should be documented;

Safeguarding procedures should be defined and formalized;

The backup should be placed in places protected from fire, magnetic radiation, water, moisture and malicious access;

#### 7.8.4. Logging and monitoring

Event logs and system administrator activities should record user activities, exceptions, and security-related events for a predefined period of time to facilitate subsequent investigation and access control monitoring;

This retention period must comply with legal requirements.

Log management must be centralized, and logs must be exploited to determine possible intrusion attempts or malicious activities;

It is necessary to set up a log management and correlation solution.

Logged information must be protected from unauthorized modification and access;

The law of least privilege must be applied. The activities of system and network administrators should also be monitored;

An NTP system should be set up on which all systems synchronize.



#### 7.8.5. Mastery of software in operation:

The installation, deletion or modification of software on operating systems may not be done without the explicit agreement of its person responsible and without prior analysis of the risks involved;

The safety measures to be taken when installing, removing or modifying a system or equipment in production must be described and followed.

#### 7.8.6. Technical Vulnerability Management:

All technical vulnerabilities in the information systems in operation should be informed in a timely manner; ICESCO shall assess their exposure to these vulnerabilities and take appropriate actions to address the associated risk;

Administrator access rights on workstations should be restricted;

The CISO must ensure the technological watch in terms of vulnerabilities. It must inform all entities of new vulnerabilities likely to impact a system used by ICESCO. The managers of each system/application must assess the criticality of the vulnerability as well as its possible impact on their system and then take action to address the identified risk;

#### 7.8.7. Information Systems Audit Considerations

When auditing information systems, the following rules should be followed to minimize the risk of business disruption. In particular, it is necessary to:

That the requirements of the audit be defined with the entities concerned,

To agree on the scope of the controls and to verify it,

That all access, except read-only, be allowed only for isolated copies of system files that will be deleted after the audit is complete,

Explicitly identify and make available the resources intended for the execution of these controls,

Monitor and log all accesses in order to have a reference trace; time-stamped reference traces for critical data or systems should be taken into account,

Document all procedures, requirements and responsibilities,

The person(s) conducting the audit are not involved in the activities being audited.

### 7.9. Communications Security

#### 7.9.1. Network Security Management



It is forbidden to connect an external device in the ICESCO local network;

It is necessary to compartmentalize the networks to obtain sub-networks adapted to the business needs;

It is necessary to set up all the standards and configurations of switches, routers and firewalls inspired by the recommendations of manufacturers and publishers;

System and network administrations must connect in a protected zone (VLAN Admin) to provide protected access to systems and networks.

#### **7.9.2. Transfer of Information**

It is necessary to establish the security rules relating to the secure exchange of information;

Clauses on information exchange procedures should be incorporated into agreements with third parties;

Access, confidentiality, integrity and availability of messaging must be guaranteed;

ICESCO users should treat junk mail, spam, hoaxes or chain emails with the utmost caution. It is strictly forbidden to forward these types of emails;

It is necessary to inform in the agreements and contracts (employment, third parties, ...) the confidentiality clauses.

### **7.10. Supplier Relations**

#### **7.10.1. Security in supplier relations**

The necessary measures should be taken to ensure that third parties provide the service for which they are mandated and that they comply with the security requirements laid down in this ISSP;

Security requirements should be included in subcontracts, depending on the nature of the service, namely:

Compliance with applicable legal and regulatory requirements,

Security responsibilities for ICESCO and the subcontractor,

Information confidentiality requirements,

Service continuity measures in the event of a disaster (if applicable),

Etc.

#### **7.10.2. Service Delivery Management**



ICESCO should carry out monitoring and verification by auditing at regular intervals the provision of services provided by suppliers;

Changes in the services of third parties providing a critical service to ICESCO should also be taken into account.

## 7.11. Information Security Incident Management

### 7.11.1. Information Security Incident Management and Improvement

Employees should report security breaches they have identified or suspect to their manager;

As an example, here is a list of security incidents:

Loss of service, materials or equipment;

Human error calling into question information security;

Failure to comply with security policies or recommendations;

A violation of physical security provisions;

An uncontrolled change to the system;

An access violation.

...

Third parties are also required to report their security incident;

Escalation forms and procedures are the responsibility of the CISO;

The employee discovering the incident must note the time and constitute as much evidence as possible;

Employees will receive incident management training;

Employees who have committed a security breach due to non-compliance with safety instructions will be sanctioned according to the procedures in force;

The causes of incidents must be systematically investigated and investigated. Corrective and preventive actions must be carried out to prevent any risk of repetition of incidents that have already occurred;

Evidence must be collected whenever legal action is considered;

The collection of evidence is the responsibility of the owner of the asset.



## 7.12. Information Security Aspects in Business Continuity Management

### 7.12.1. Continuity of information security

ICESCO must have a continuity plan to ensure the continuity of its business activities;  
ICESCO must ensure that the continuity plan covers all risks of business interruption (fire, virus infection, destruction of equipment, etc.);  
The continuity plan includes annual testing planning to ensure that each of the business processes identified as vital is properly covered by this plan;  
The realization of these regular tests must be part of an improvement process. Corrective but also preventive actions must be taken during each deviation encountered during these tests;

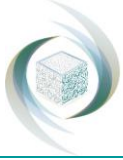
### 7.12.2. Redundancy

ICESCO's sensitive equipment should be redundant to meet business requirements.

## 7.13. Compliance

### 7.13.1. Compliance with legal and regulatory obligations

It is necessary to identify all the texts of the legislation to which ICESCO is subject, it must, in particular, respect the Moroccan laws governing computer security and acts of cybercrime.  
It is necessary to identify the elements subject to intellectual property law and respect this right.  
The necessary information protection measures should be implemented in order to preserve intellectual property rights;  
In addition, it is strictly forbidden to install applications for which ICESCO does not have the licenses. ICESCO will sanction any user who hinders this requirement;  
The necessary safeguards should be implemented to protect legal registrations concerning her;  
The necessary measures for the protection of privacy and the protection of personal data should be implemented;  
The cryptographic measures put in place must comply with applicable agreements, laws and regulations.



### 7.13.2. Information Security Review

ICESCO shall conduct independent audits of its information security management system at regular intervals to assess its ISMS;

Indicators should also be put in place to assess the extent to which this IHSP, standards and regulations have been applied;

When deviations are observed, their cause must be investigated, then corrective and preventive actions must be put in place in order to achieve the objectives set;

The realization of these audits must be done in line with the business activities so as not to disrupt them;

Finally, application configurations, systems and networks must be regularly checked to ensure that they correspond to the theoretically expected configurations.