UNITED NATIONS INDUSTRIAL DEVELOPMENT ORGANIZATION

SECRETARIAT

DGB/2023/01
8 February 2023

Distribution: All staff members at Headquarters, established offices and Permanent Missions

DIRECTOR-GENERAL'S BULLETIN

UNIDO Information Security Policy

1. The purpose of the present bulletin is to promulgate the UNIDO Information Security Policy.

2. Ensuring information security is critical to protect Information Technology (IT) systems and sensitive information from cyber-attacks. The increasing online presence of the Organization and transitioning of IT infrastructure to cloud-based solutions, advanced interconnectivity as well as a mobile workforce have led to increased risks, incidents and cyber-attacks. Information security attacks continued to increase in recent years, not only in terms of vectors and numbers but also in terms of impact. Identified incidents in UNIDO, such as compromised accounts or malware outbreaks, pose significant risks in terms of potential financial losses, reputational damages or data alteration.

3. Information security is a continuous and necessary process and a vital part of digital transformation. Ensuring the security and resilience of UNIDO's information assets is critical in supporting the Organization's ability to be fit for the future and deliver its mandate through progress by innovation. In this sense, information security is an organizational-wide process that combines in a harmonized approach the elements of people, process, and technology, which are necessary for modernizing UNIDO, in a safe, secure and resilient way to optimize organizational efficiency and effectiveness.

4. This policy sets the tone for the UNIDO information security framework that is in line with the internationally recognized ISO 27000 series standard. It identifies the commitments and objectives required for a comprehensive, resilient and sustainable information security programme, and describes the strategic information security principles as well as the related roles and responsibilities.

5. The UNIDO Information Security Policy builds on and complements the Organization's existing regulatory framework. The UNIDO Information Security Policy shall be read in conjunction with the UNIDO Information and Communications Technology Policy (DGB/2017/09), Business Continuity Plan (DGB 2020/08), Information Disclosure Policy (DGB/2021/17) and upcoming policies on data protection.

6. Responsibility for maintaining and implementing an organizational culture of information security lies with all personnel.

7. The Managing Director of the Directorate of Corporate Services and Operations (COR), as custodian of this policy, shall be responsible for ensuring compliance with the UNIDO Information Security Policy. The day-to-day implementation and monitoring of the policy shall be the responsibility of the Information Technology and Digitalization Services (COR/DIG). The Managing Director of COR, in cooperation with Human Resource Services (COR/HRS) and COR/DIG, shall establish the functions that may be required for the effective management and implementation of information security across UNIDO in conformity with the provisions of this policy, including, but not limited to, the independent function of the Information Security Officer.

8. The UNIDO Information Security Policy will be reviewed and evaluated in one year from the initial promulgation date. In this regard, COR/DIG through the Managing Director of the Directorate of Corporate Services and Operations (COR) will report its findings to the Director General, including any recommendations on adjustments to the policy, as needed.

9. The present bulletin comes into effect on the date of issuance.

UNITED NATIONS
INDUSTRIAL DEVELOPMENT ORGANIZATION

UNIDO INFORMATION SECURITY POLICY

CONTENTS

Objective and Scope 4
Guiding Principles 5
Organization of Information Security 6
Specific Roles and Responsibilities 7
Non-Compliance 10
Review and continuous improvement 10
Glossary of Terms 12

UNIDO Information Security Policy

Objective and Scope

1. UNIDO is committed to preserving the confidentiality, integrity and availability of the physical and electronic information assets of the Organization in order to deliver its services, maintain the confidence of its Member States, personnel and other stakeholders as well as its reputation, and ensure compliance with its obligations and the efficient and secure use of its resources.

2. This policy applies to all users of information assets (physical and electronic) and systems that are owned, controlled, licensed, operated, managed, or made available (or otherwise used) by UNIDO and which are capable of generating, transmitting, receiving, processing, or representing data in electronic or physical form.

3. A user of information within the scope of the preceding paragraph includes all UNIDO staff, employees and other personnel (including interns), suppliers, and contractors, regardless of their working or contractual relationship with UNIDO and irrespective of their location, including third parties who are given access to UNIDO information assets and the corresponding information systems that are used to store and process such assets.

4. Within this context, UNIDO implements, maintains, monitors and continuously improves a comprehensive information security framework that is aligned to the extent possible with the internationally recognized ISO 27000 series standard, taking into account any external requirements, the mandate of the Organization as well as emerging information security risks.

5. The framework consists of the current policy and an information security management system (ISMS) that is under development. The ISMS will include topic-specific administrative issuances and technical procedures that will elaborate the implementation of information security controls and take into account the needs of certain target groups within the Organization. The ISMS will establish a systematic approach for managing the Organization's information security and shall serve as a practical model for defining, implementing, monitoring, maintaining and improving the appropriate protection of information assets to achieve business objectives. This includes monitoring of the promulgated information security procedures and controls to ensure an effective and efficient implementation of information security across the Organization, including processes on the information security risk management, vulnerability management and security testing amongst others.

6. The ISMS is expected to include the following topics:

    a. Information security risk assessment;

    b. Information security risk treatment;

    c. Implementation of risk treatment plans, operational planning and control;

    d. Monitoring, performance evaluation and management review;

    e. Support, including resources, knowledge, awareness and communication;

    f. Continuous improvement.

7. In line with best practices, this policy also establishes and defines the independent information security function. The information security function deals with supporting processes, controls, and systems, which ensure that the requisite actions are taken to protect UNIDO's information resources in the most appropriate and efficient manner.

Guiding Principles

8. Information security is a risk management discipline that addresses the appropriate protection of confidentiality, integrity and availability of information and the systems used for its storage, processing and transmission. These information assets must be identified, valued, assessed, and protected, as appropriate, to align with the needs and risk tolerance of the organization.

9. The following are the guiding principles of the information security framework:

a. **Appropriate levels of security**

The multitude of diverse systems and types of information in UNIDO give rise to a variety of information security requirements. Appropriate security and internal controls are applied through a tiered system of policies and procedures, based primarily on the criticality and sensitivity of information as defined in the section on Information Management (INF.2. Classification), contained in the UNIDO Information and Communications Technology Policy (DGB/2017/09) and in the Information Disclosure Policy (DGB/2021/17).

b. **Mainstreaming of Information Security**

Information security is integrated horizontally across organizational directorates, divisions, offices and units, and vertically throughout various programmes and projects.

c. **Information-Centric and Identity-based Access**

With an increasingly mobile workforce and the proliferation of interconnected networks utilized by UNIDO, the information security architecture must be adjusted to protect the information itself, by following good security and integrating known security principles related to identity and access management such as need-to-know or least-privilege-required. Information systems should be designed and implemented based on the premise that trust is never granted implicitly but is instead continuously evaluated.

d. **Commitments and Support**

The continued support and commitment of UNIDO's leadership is essential for the establishment and maintenance of an effective information security framework. This includes alignment of information security risk management with the principles adopted through the UNIDO Enterprise Risk Management Policy (DGB/2021/01) and the UNIDO Internal Control Framework (DGB/2021/02). The endorsement and consistent support from senior management, confirmed by concrete actions, is critical for successful implementation of the framework.

e. **Accountability**

In line with the UNIDO Accountability Framework (DGB/2021/03), the adoption of an effective information security framework relies on the accountability of management at all organizational levels of risk management and internal control activities.

f. **Resources**

Information security risk and internal control management shall be supported at the organizational unit level, in line with the UNIDO Enterprise Risk Management Policy (DGB/2021/01) and the UNIDO Internal Control Framework (DGB/2021/02), within available resources.

Organization of Information Security

10. The effective application of information security within UNIDO is aligned with the "three lines" model adopted by the UNIDO Internal Control Framework (DGB/2021/02), and supplemented by external assurance providers. The "three lines" model supports an efficient and effective information security risk management and internal control by helping to ensure a structured governance and oversight mechanism that clarifies and segregates essential roles and responsibilities.

11. The first line of defense is with all personnel, managers and process owners who perform regular activities that relate to or include elements of information security, such as:

    a. Implement and monitor security controls in business processes;

    b. Operationalize work instructions, procedures, administrative instructions related to, or containing, information security aspects;

    c. Identify, assess and manage information security risks;

    d. Perform activities related to security operations, such as, for example, security monitoring, incident response, and vulnerability management;

    e. Help improve the effectiveness and efficiency of information security controls and respond promptly to any gaps, weaknesses or deficiencies in controls, by either resolving or reporting them up the chain of accountability.

12. The second line of defense in information security deals with processes which ensure that the requisite actions are taken to protect UNIDO's information resources in the most appropriate and efficient manner and in pursuit of organizational goals. The Information Security Policy also sets the requirement for the establishment of an Information Security Management System (ISMS) as a practical model for defining, implementing, monitoring, maintaining and improving the appropriate protection of information assets to achieve business objectives. This includes monitoring of the promulgated information security procedures and controls to ensure an effective and efficient implementation of information security across the Organization. The second line of defense function in information security at UNIDO is performed by the Managing Director, COR, the Chief, COR/DIG, and the Information Security Officer in accordance with the responsibilities outlined in Section IV below. Key responsibilities of the second line of defense in information security, in line with the UNIDO Internal Control Framework, are as follows:

    a. monitor the implementation of information security strategies and mid- and long-term goals;

    b. monitor, measure and report on results and performance;

c. monitor information security controls;

d. monitor compliance with information security policies and administrative issuances, and adherence to agreements relating to information security;

e. monitor, review and report on risks; and

f. provide quality assurance.

13. The third line of defense is carried out by the independent assurance providers, focusing on the efficiency and effectiveness of risk assessment and risk management processes and controls in place. These include functions of independent evaluation, internal audit and investigation. The third line also includes assurance reviews on the effectiveness of the first and second lines.

Specific Roles and Responsibilities

Director General:

14. The Director General is the Chief Administrative Officer of UNIDO and has the ultimate responsibility for promulgating and implementing an effective information security policy as well as for setting the tone at the top of the Secretariat on all information security matters.

All responsible officials in charge of organizational units[1]:

15. Accountable for the protection of information within their respective directorate, division or office, and are responsible for the following:

a. Protecting information assets within their business area;

b. Demonstrating leadership with respect to information security management.

Managing Director, Directorate of Corporate Services and Operations (MD/COR):

16. Has a delegated responsibility by the Director General for information security at UNIDO and is, therefore, accountable to the Director General for ensuring compliance with the UNIDO Information Security Policy and for its implementation, as well as for updating the policy based on lessons-learned, organizational needs and priorities, as well as availability of financial resources;

17. Establishes the functions required for the management and implementation of the information security management system (ISMS) across UNIDO and monitors its effectiveness.

Chief, Information Technology and Digitalization Services (COR/DIG):

18. Accountable to MD/COR for ensuring compliance of IT systems and applications managed by COR/DIG with the applicable information security procedures and for the development, management and review of the Organization's information security management system and operations;

19. Assigns the role of Information Security Officer in line with the terms of reference of COR/DIG included in the UNIDO Secretariat Structure 2022 (DGB/2022/19);

20. Aligns the UNIDO Information Security Policy outcomes to the requirements of UNIDO;

[1] For example Managing Directors, Directors, Chiefs of Divisions, etc.

21. Develops and maintains the Information Security Policy;

22. Maintains the pragmatic alignment of the UNIDO ISMS with the ISO 27001 standard;

23. Reviews the ISMS every biennium for its continuing suitability, adequacy, and effectiveness, and promoting continual improvement;

24. Reports to the Managing Director, COR on the status and implementation of information security in UNIDO.

Information Security Officer:

25. Operates the ISMS in accordance with the defined information security policies, processes, and procedures;

26. Coordinates information security activities across the Organization and collaborates with all internal stakeholders and organizational units at headquarters, established offices and throughout the field network;

27. Coordinates information security risk assessments, risk treatment planning, and implementation of mitigating controls;

28. Reviews the performance of the ISMS against the defined information security objectives and key performance indicators;

29. Monitors compliance with the ISMS;

30. Coordinates with Learning and Development Services (COR/LED) to develop, manage and implement a mandatory information security awareness programme;

31. Reports immediately major information security concerns that actually or imminently hinder the delivery of critical services or impact UNIDO's mandate to the Managing Director, Directorate of Corporate Services and Operations (COR) and the Office of the Director General, and reports any weakness or breakdown in the internal control framework to the Director of the Office of Evaluation and Internal Oversight (EIO) and relevant functional leads, in accordance with the Internal Control Framework and the EIO Charter;

32. Provides timely advice to the Managing Director, COR and the Chief, COR/DIG on matters of information security or security requirements for information systems development or enhancements;

33. Identifies significant threats and risks to the security of information and physical or electronic assets that store, process, or transmit the information, and reports these to the Managing Director, COR and the Chief, COR/DIG;

34. Evaluates information received during and after an information security incident, recommends appropriate actions to the Managing Director, COR and the Chief, COR/DIG in response to identified incidents, and initiates reviews where necessary;

35. Coordinates the implementation of information security controls and implements performance measurement processes for the required controls;

36. Serves as liaison regarding information security between UNIDO and external entities, including the United Nations and other agencies, in order to share knowledge and promote best practices.

Information stewards:

37. Information stewards are officials in charge of organizational units, typically Directors or Chiefs of Divisions, in which the information originates or is mostly used. They can delegate the right to make decisions on classifications and handling to supervisors of the subordinated organizational units;

38. Responsible for ensuring information security, i.e. for the integrity, availability, proper location and confidentiality of the information they own or control, at all times;

39. Hold the decision making authority for information throughout its life cycle, including creating, classifying, restricting, regulating and administering its use or disclosure, in accordance with the Information Disclosure Policy (DGB/2021/17). This includes responsibility for the physical assets that store, process, or transmit the information they own;

40. Responsible for the classification and proper handling of, as well as authorizing and revoking access to, such information assets;

41. Promote information security initiatives within their business areas; direct and support personnel in applying the Information Security Policy, and any related standards, procedures and processes to their respective areas of responsibility.

Information custodians:

42. Information custodians are persons or entities who have been assigned by information stewards the responsibility for maintaining and safekeeping of information assets, on a temporary or permanent basis[2]. Information custodians may not be the actual users of the information under their responsibility;

43. Responsible for maintaining the information security, i.e. confidentiality, availability and integrity of information assets;

44. Act according to the needs and requirements of the information steward;

45. Ensure adequate, timely, and consistent implementation of defined information security controls;

46. Ensure that user access to information resources and assets is based on a need-to-know and least privilege principles ensuring internal controls and the accountability framework principles are followed;

47. Additional responsibilities exist for information custodians who are responsible for an IT environment:

    a. Maintaining the confidentiality, availability, and integrity of IT assets residing in their IT environment, individually and as a system;

    b. Ensuring adequate, timely, and consistent implementation of defined IT security

[2] For example COR/DIG, external or cloud providers, etc.

controls; and

c. Demonstrating leadership and commitment with respect to IT security management.

All users of UNIDO information assets:

48. All users, as defined in paragraph 3, within the scope of this policy shall:

a. be responsible for ensuring that UNIDO's information assets are used exclusively for their intended purpose; in proper pursuit of the interests of the Organization; and in accordance with applicable UNIDO policies (e.g., regarding data protection and information disclosure);

b. be responsible for ensuring that information is not improperly disclosed, modified, or endangered, and that access to UNIDO's information resources is not made available to any unauthorized persons;

c. maintain security awareness by completing any UNIDO mandatory cyber security training that is assigned and technically accessible (for holders of a UNIDO email address) and avail themselves with organizational advisories or relevant information related to cyber security;

d. familiarize themselves, understand, and comply with applicable information security policies, procedures and guidelines, and seek guidance, when needed, from the UNIDO Information Security Officer or the Chief, COR/DIG, regarding questions on information security policies or other security concerns.

e. report immediately actual or suspected information security incidents via email to cybersecurity@unido.org, via Service Portal – https://cybersecurity.unido.org, or in person.

Non-Compliance

49. Any request for an exemption from any part of this policy (non-compliance) or other ISMS policy documents shall be addressed in writing to the Information Security Officer, along with any pertinent documentation and explanation. The Information Security Officer may require approval from the requestor's supervisor(s).

50. Based upon the initial assessment by the Information Security Officer, non-compliance requests shall be cleared by the Chief of COR/DIG and sent for approval to the Managing Director of COR. The requesting user and supervisor(s) shall be informed of the assessed risk of the proposed non-compliance and any additional controls needed and shall confirm in writing that they assume responsibility for such risks and will implement the necessary mitigating controls, in accordance with the UNIDO Enterprise Risk Management Policy.

51. Non-compliance permissions shall be granted for a maximum of twelve (12) months at a time, after which the non-compliance request shall have to be renewed by the requestor.

Review and continuous improvement

52. Information security management is a dynamic process, which shall be reviewed and adjusted regularly. Reviews of this policy must reflect the evolving needs of UNIDO. Moreover, the direction of information security management in the United Nations system, developments in best practice and updates to applicable standards will be monitored regularly and adopted where appropriate.

53. The policies on information security and the ISMS shall be reviewed periodically (at least every biennium or whenever significant changes occur), incorporating lessons learned to strengthen organizational capacity and to ensure its continued relevance to its mandate and objectives.

54. The monitoring and revision process must be inclusive and well-documented to provide meaningful information to senior management for decision-making and for improving the ISMS.

Glossary of Terms

Term	Description
Need-to-know	Describes the restriction of data that is considered sensitive. Under need-to-know restrictions, one would not be given access to such information, unless one has a specific need to know; that is, access to the information must be necessary for one to conduct one's official duties.
Least Privilege	The principle means giving a user account or process only those privileges that are essential to perform its intended function.
ISO 27000	The ISO/IEC 270001 family of standards, also known as the ISO 27000 series, is a series of best practices to help organizations improve their information security. This is considered as the de-facto standard in information security management. Published by ISO (the International Organization for Standardization) and the IEC (International Electrotechnical Commission), the series explains how to implement best-practice information security practices.
Information security management system (ISMS)	An ISMS is a systematic approach to risk management, containing measures that address the three pillars of information security: people, processes and technology.
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
Integrity	Integrity means maintaining and assuring the accuracy and completeness of data over its entire lifecycle.
Availability	The property that the information must be available when it is needed. This means the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly.
Users	All UNIDO staff, employees and other personnel (including interns), suppliers, and contractors, regardless of their working or contractual relationship with UNIDO and irrespective of their location, including third parties who are given access to UNIDO information assets and the corresponding information systems that are used to store and process such assets.
Information stewards	Officials in charge of organizational units, typically Directors or Chiefs of Divisions, in which the information originates or is mostly used. They can delegate the right to make decisions on classifications and handling to supervisors of the subordinated organizational units.
Information custodians	Persons or entities who have been assigned by information stewards the responsibility for maintaining and safekeeping of information assets, on a temporary or permanent basis[3]. Information custodians may not be the actual users of the information under their responsibility

[3] For example COR/DIG, ITS, external or cloud providers, etc.