Executive Office Directive Ref. EOD.ED.2019.01
Privacy and Information Security

Authority:

This Executive Office Directive (EOD) is promulgated by the Executive Director.

Purpose

The purpose of this EOD is to set out the high level principles regarding privacy and information security at UNOPS.

Effective Date:

This EOD shall become effective immediately.

[signature redacted]

Grete Faremo
Executive Director

1. Introduction

1.1. The United Nations Office for Project Services (UNOPS) holds significant assets in the form of information and physical property.

1.2. Information includes human resources and personnel records, administrative processes, procurement-related data, field operations and location information, legal (including contracts and investigations), third-party data, and politically sensitive information, among others.

1.3. During the course of carrying out their activities, UNOPS collects, processes, stores, transfers and manages a wide range of Information, some of which may be confidential and/or sensitive.

1.4. Such Information shall therefore be managed carefully by UNOPS and in a coherent manner across the organisation, particularly ensuring respect for human rights and fundamental freedoms of individuals, in particular the right to privacy.

1.5. Regulatory frameworks, industry standards and best practices may be used by the organization as guidance for managing certain information, such as information relating to personnel, suppliers, partners and other stakeholders.

1.6. In this context, the purpose of the EOD is to define the key principles, roles and responsibilities for the development and management of UNOPS' Information Security Management System (ISMS) and personal data privacy (PDP) program to address the critical needs of the organization to protect all of these assets, including written and oral information transmitted and stored in magnetic media, computing devices, documents, applications, systems, databases and networks.

2. Key Privacy Principles

2.1. The following key privacy principles apply to personal data, contained in any form, and processed in any manner. Where appropriate, they may also be used as a benchmark for the processing of non-personal data, in a sensitive context that may put certain individuals or groups of individuals at risk of harm. UNOPS personnel need to respect and apply the following principles when processing personal data:

- **Fair and legitimate processing:** UNOPS will process personal data in a fair and legitimate manner with the consent of the data subject; in the best interests of the data subject; consistent with the mandate and objectives of UNOPS; consistent with any other legal basis identified by UNOPS.[3]
- **Purpose specification:** Personal data must only be processed for specified purposes which are consistent with the mandate and objectives of UNOPS, taking into account the balancing of relevant rights, freedoms and interests. Personal data must not be processed in ways that are incompatible with such purposes.
- **Proportionality and necessity:** The processing of personal data must be relevant, limited and adequate to what is necessary in relation to the specified purposes of personal data processing.

- **Retention:** Personal data will only be retained for the time that is necessary for the specific purpose, and in accordance with the Operational Instruction on Document Retention (Ref: OI.LG.2018.03).
- **Accuracy:** Personal data must be accurate and, where necessary, up to date to fulfil the specified purposes.
- **Confidentiality:** Personal data must be processed with due regard to confidentiality.
- **Security:** Appropriate organizational, administrative, physical and technical safeguards and procedures must be implemented to protect the security of personal data, including against or from unauthorized or accidental access, damage, loss or other risks presented by data processing.
- **Transparency:** Processing of personal data must be carried out with transparency to the data subjects as appropriate and whenever possible. This must include, for example, provision for information about the processing of their personal data as well as information on how to request access, verification, rectification, and/or deletion of that personal data, insofar as the specified purpose for which personal data is processed is not frustrated.
- **Transfers:** In carrying out its activities, UNOPS may transfer personal data to a third party, provided that, under the circumstances, UNOPS satisfies itself that the third party affords appropriate protection for the personal data.
- **Consent:** Where processing is based on consent, UNOPS shall be able to demonstrate that the data subject has consented to the processing of their personal data. The data subject shall have the right to withdraw their consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
- **Accountability:** UNOPS must have adequate policies and mechanisms in place to adhere to these Principles.

3. Key Information Security Principles

3.1. The following key information security principles shall underpin the UNOPS ISMS to be developed and overseen by the Chief Information Security Officer (CISO):

- **Not all information shall be treated the same way:** The way any given information is to be managed, and the degree of protection needed for such information, shall be based on the nature of the information and its intended use.
- **Confidentiality:** Confidentiality refers to ownership of the information that is only to be made available or disclosed to authorized individuals, organizations or processes. Access to information, to an extent, is reserved for those who require it on a clearly identified need-to-know basis.
- **Integrity:** Information integrity relates to the accuracy and completeness of information resources. This means it involves protecting the accuracy and consistency of the information, as well as the methods used to process this information.
- **Availability:** This is the property (for an information system) of being accessible and of fulfilling the functions envisaged at the time of the application to an authorized entity, under the expected conditions of time-scales and performance. This means protecting the capacity of an

information system to perform a function under defined schedule, time-scale and performance conditions.

4. Roles and Responsibilities

Chief Information Security Officer (CISO):
4.1. The CISO shall be responsible for developing and overseeing the UNOPS ISMS and PDP program, and ensuring that appropriate security and privacy best practices are implemented and strictly adhered to throughout UNOPS. The CISO is independent in performing his/her information security management function, and in order to effectively function, shall have unrestricted access to UNOPS enterprise facilities, data, networks, systems, computer hosts, to include cloud and third-party hosting instances, to conduct activities related to executing his/her duties.

Chief Information Officer (CIO):
4.2. The CIO shall be responsible for IT resource management, specifically with regards to policy development, standard operating procedure development, best practice development, training, resourcing, budgeting, and planning during a system or project development life cycle. As a key privacy and security leader, the CIO shall work closely with the CISO to assess how IT platforms used by UNOPS can provide opportunities for intrusion, disruption or breach of personal data, and to devise methods to counter any efforts to capitalize on those weaknesses. Specifically, this includes embedding 'privacy by design' and 'security by design' principles into the lifecycle management of IT systems and applications.

UNOPS Directors
4.3. UNOPS Directors shall be responsible for overseeing compliance with, this EOD and other UNOPS policies on privacy and information security within their respective areas of responsibilities.

All Persons with Access to UNOPS Information, Systems and Premises
4.4. All persons with access to UNOPS information, systems and/or premises shall be responsible for ensuring that UNOPS information assets are treated in compliance with this EOD and other relevant UNOPS policies. Specifically, they must ensure, to the best of their abilities, that information assets and systems are used only in support of UNOPS' business operations, that information is not improperly disclosed, modified or endangered, and that access to UNOPS information resources are not made available to any unauthorized person.