Operational Directive Ref. OD.ITG.2021.01
IT and Digital Systems Management

Authority:

This Operational Directive (OD) is promulgated by the Chief Financial Officer and Director of Administration on the basis of a delegation of authority from the Executive Director.

Purpose:

The purpose of this OD is to define the general principles, roles, and responsibilities related to the governance, management, and use of Information Technologies in UNOPS.

Effective Date:

This OD shall become effective **immediately.**

Promulgation Date:

06 Jul 2021

Consequential changes:

This OD shall abolish and supersede OD.FG.2018.02: ICT and Digital Systems Management of15 March 2018. The purpose of the revision is to update organisational references within the OD as well as to bring specific clauses in the OD in line with the approved IT Strategy.

[signature redacted]

Marianne de la Touche
Chief Financial Officer and Director of Administration

1. Introduction

1.1 This OD provides an overview of the key principles that underpin the management of digital systems, services, software, application, and resources.

2. Responsibilities and roles

2.1 The Chief Information Officer (CIO) is responsible for the design of UNOPS digital strategy, enterprise architecture and technical infrastructure in order to deliver and operate digital services, applications, and systems in alignment with UNOPS strategy and business operations' requirements, under the guidance of the CFO and Director of Administration.

2.2 The Senior Leadership Team (SLT) will ensure alignment with UNOPS corporate priorities and business needs.

3. Goals and objectives

3.1 The IT function of UNOPS (UNOPS ITG) serves as a business partner to the organization, and as a source and enabler of innovation.

3.2 UNOPS systems are put in place to allow personnel to work efficiently across units and offices. Systems aim at enabling organic knowledge sharing and effective collaboration on documents, projects and knowledge resources, as well as allowing for improved engagement directly with partners and clients.

3.3 Investments in digital initiatives will be directed towards systems enabling the delivery of services that provide a greater degree of efficiency or effectiveness towards delivery of client projects or differentiate UNOPS in the marketplace.

3.4 UNOPS strives to build systems that provide functionality and algorithms that are not readily available in the market or buy fit for purpose systems as appropriate balancing cost and benefits.

4. Services, systems and software

4.1 Choice of strategic services, systems and software are to be based on ex-ante cost and benefits assessment, ensuring adaptation to business needs and requirements, as well as ex-post evaluation of achieved benefits.

4.2 UNOPS systems are to be robust, accurate, reliable, and efficient so as to mitigate risks, enforce controls, and ensure compliance with established policies and processes.

4.3 To enable efficient and cost-effective service delivery, UNOPS processes are to be aligned with and supported by digital systems and workflows. The delivery of such systems and digital services will be

measured through appropriate SLAs (Service Level Agreements) as well as efficiency and performance related KPIs (Key Performance Indicators)

4.4 Issuance of new, or changes to existing, policies or processes should be reviewed for potential impact on digital systems and workflows, and allow for necessary modifications or development to be completed, prior to taking effect.

5. Software design and architecture

5.1 Software and services, whether developed in-house, purchased, or subscribed to, should to the extent possible:

- Be accessible across devices;
- Be accessible from all locations;
- Be operable under conditions of low bandwidth and high network latency;
- Use UNOPS central identity management platform
- Ensure appropriate information security controls;
- Be aligned with UNOPS enterprise architecture; and,
- Provide relevant integration interfaces.

6. Use and licensing of services, systems and software

6.1 All software or digital services used by UNOPS personnel, installed on UNOPS owned assets, and/or made available by UNOPS to external entities are to be appropriately licensed.

6.2 All software or digital services for internal use are to be reviewed and approved by UNOPS ITG prior to purchase or subscription.

6.3 All UNOPS information assets are to be stored on systems or services approved by UNOPS ITG.

6.4 All official UNOPS communication are to take place using systems or services approved by UNOPS ITG.

7. Information Security

7.1 UNOPS ITG will ensure that internally developed applications and systems as well as any IT systems that are procured adhere to information security policies, as promulgated in EOD.ED.2019.01.

7.2 UNOPS ITG strives to ensure the confidentiality, integrity and availability of UNOPS information assets, in alignment with UNOPS internal control frameworks, data classification and access policies.

7.3 The privacy of UNOPS personnel should be respected in digital processes, systems and services.

7.4

7.5 UNOPS strives to ensure that appropriate resources and relevant systems are in place to mitigate identified information security risks.

8. Operations and hosting

8.1 UNOPS ITG designs and operates its infrastructure, whether self-managed or through outsourced providers, in a way that aims at high availability of critical systems and applications, ensuring operational resilience and minimizing unplanned downtime. UNOPS will measure its infrastructure availability through appropriate SLAs in line with industry standards.

8.2 UNOPS ITG maintains disaster recovery plans for critical IT systems so that to minimise the impact of unforeseen incidents on the operational capacity of the organization. The principles and procedures for business continuity planning are defined under EOI.ED.2018.03: Business Continuity Planning.

8.3 Systems and services should be hosted in line with UNOPS ITG standards, with due consideration to be given to sensitivity of data, controls, manageability, access speed, integration needs, and costs.

9. Use of digital systems and services

9.1 The term “UNOPS digital identity holders” refers to individuals or entities issued with login credentials to UNOPS owned or managed internal systems, services, software, and applications.

9.2 UNOPS digital identities will be issued to all UNOPS supervised personnel.

9.3 Issuance of UNOPS digital identities to other individuals or entities will be based on approval by the CIO and General Counsel, and requires adherence to UNOPS policies of acceptable use, confidentiality, and non-disclosure.

9.4 UNOPS digital identity holders must adhere to all policies and guidelines related to the use of the systems they are granted access to, including making best efforts to preserve the integrity and confidentiality of UNOPS information.