Headquarters, Copenhagen
6 July 2021

Operational Instruction Ref. OI.ITG.2021.02

IT Security and Access

1. Authority

1.1. This Operational Instruction (OI) is promulgated by the Chief Financial Officer and Director of Administration under OD.ITG.2021.01: IT and Digital Systems Management.

2. Purpose

2.1. The purpose of this OI is to provide instructions regarding the security and access to UNOPS IT resources for the purpose of secure systems delivery.

2.2. This OI is promulgated in accordance with the OD.ITG.2021.01: IT and Digital Systems Management and is based on best-practice guidelines in respect to effective security and access to UNOPS IT systems. It documents how users should treat digital identities , how these digital identities should be issued and managed, and the responsibilities of UNOPS Digital Identity holders.

3. Effective Date

3.1. This OI shall become effective **immediately**.

4. Consequential Changes

4.1. This OI shall supersede and replace OI.ICT.2018.02: ICT Security and Access of 28 September 2018. The purpose of this revision is to cover the use of assigned IT equipment outside office premises 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

Operational Instruction Ref. OI.ITG.2021.02

IT Security and Access

Table of Contents

1. Definitions

1.1. The term “digital identity holders” shall refer to individuals or entities issued with login credentials to a UNOPS owned or managed internal system, service, software, or application.

1.2. The terms “systems”, “services”, “applications”, “software”, and “subscriptions” shall be used interchangeably, and the principles outlined in this OI covers any and all of these terms.

2. UNOPS Digital Identities

2.1. All UNOPS personnel shall be issued a UNOPS Digital Identity to facilitate access to UNOPS systems, electronic information, and tools.

2.2. UNOPS partner personnel are not entitled to a UNOPS Digital Identity and should only be issued digital identities based upon explicit approval from the CIO.

2.3. A UNOPS Digital Identity shall not be issued to personnel without a valid UNOPS contract, without explicit approval by the CIO and General Counsel. Exceptions can be approved on a case-by-case basis or based on affiliation type.

2.4. Email addresses can only be issued to UNOPS supervised personnel with a valid UNOPS contract. Exceptions shall require explicit approval by the CIO and General Counsel. Exceptions can be approved on a case-by-case basis or based on affiliation type.

2.5. A UNOPS Digital Identity shall be personal and non-transferable. Login details shall be personal, confidential and shall not be shared with anyone.

2.6. Digital Identity holders shall be responsible and accountable for all communications, actions and approvals performed using their UNOPS Digital Identity . Personnel to whom a UNOPS Digital Identity has been assigned shall not disclose the log-in credentials to anyone and shall be responsible and accountable for all actions performed and transactions approved through the use of that log-in credential.

2.7. UNOPS Digital Identity validity shall be based on the personnel contract start and end dates, although a digital identity may be created and login details issued prior to the start date, provided that a signed contract and all necessary information is available in oneUNOPS.

2.8. UNOPS Digital Identities will terminate on the date of contract expiration. In exceptional circumstances, the digital identity may remain active up to 30 days beyond contract end date, subject to formal approval process.

2.9. In the case of immediate contract termination or when put on administrative leave, revocation of access to UNOPS systems can be requested by local management in coordination with the Legal Group (LG) and/or the Internal Audit and Investigation Group (IAIG), through ITG.

2.10. UNOPS digital identity holders should NOT:

a) Leave their computer unlocked when unattended.

b) Leave their log-in credentials unprotected (for example writing it down).

c) Perform any unauthorized changes to UNOPS IT systems or information.

d) Attempt to access data that they are not authorised to.

e) Exceed the limits of their authorization or specific business needs on UNOPS IT systems.

3. Official Usage of UNOPS Systems

3.1. All internal electronic information assets, e.g. documents, emails, presentations, spreadsheets etc., shall be stored on official UNOPS systems.

3.2. All work-related email communications shall be done using the official UNOPS email platforms.

3.3. Internal memos, documents, and the like which have only been made available to UNOPS Digital Identity holders, shall be considered as internal information and shall not be shared, forwarded or otherwise disseminated to non UNOPS Digital Identity holders, without prior approval.

3.4. Using a mailbox assigned to another person to fraudulently transmit or receive a message associated with that person shall be prohibited.

3.5. Any device that is linked to UNOPS systems may be subject to remote removal of UNOPS data in cases of theft, loss, or misuse.

4. Personal Usage of UNOPS Systems

4.1. Limited personal use of UNOPS systems and internet access shall be permissible insofar it does not interfere with the performance of official duties, violate any UNOPS policies, cause network performance issues, or incur any costs to UNOPS.

4.2. Restrictions on personal use and/or access to specific services may be put in place to ensure sufficient access or capacity for official use.

5. Intellectual Property

5.1. Downloading, copying, using or sharing any data, media, software, or service for work purposes or on UNOPS systems for which the user does not hold a valid license or usage right shall be prohibited. The terms of the license(s) or usage right shall not be violated.

5.2. All emails, documents, intellectual works created using UNOPS systems shall remain the property of UNOPS.

6. Applications and services

6.1. No software, applications or services beyond those provided through UNOPS ITG shall be installed on UNOPS computers, or used for official UNOPS use, without prior approval of UNOPS ITG.

6.2. Software, applications or services, not directly licensed by UNOPS, shall not be installed on UNOPS computers or devices without prior approval of UNOPS ITG.

7. Usage of Systems

7.1. UNOPS Digital Identities, systems or services shall not be used to:

a) Send, post or transmit messages or statements which violate any UNOPS policies or guidelines, or that may affect UNOPS reputation.

b) Send, post, share or transmit to any external party, information which can be considered proprietary, without formal approval or when not in line with established practice within one’s field of work.

c) Conduct commercial transactions of non-official nature, aside from personal online transactions as described in 4.1.

d) Knowingly affect, or attempt to affect, the performance, availability, integrity or confidentiality of UNOPS or non-UNOPS systems and services.

e) UNOPS Digital Identity holders shall take reasonable steps to ensure that the availability, integrity and confidentiality of UNOPS information is maintained, and not knowingly or through gross negligence, take any action or refrain from taking necessary action to compromise such information.

f) Set up automatic forwarding rules in order to forward UNOPS email to non-UNOPS email accounts without expressed approval.

g) Make official commitments through the Internet or email on behalf of UNOPS, unless authorized to do so.

8. Data breaches

8.1. Any data breaches or digital identity theft suspected or confirmed shall be reported to the relevant IT focal point immediately along with any other relevant reporting channels.

8.2. All hardware or data losses, thefts or damage must be reported immediately to the relevant IT focal point.

9. Removable Storage Devices

9.1. Mobile storage devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only UNOPS authorised removable storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

9.2. UNOPS data classified as Unclassified, Confidential and Strictly Confidential should not be stored on USB sticks, external hard drives, or other removable media.

10. Working Remotely

10.1. Equipment and storage media taken off-site must not be left unattended in public places and not in sight in vehicles.

10.2. Devices must be carried as hand luggage when travelling.

10.3. UNOPS information should be protected against loss or compromise when working remotely.

10.4. Personal devices used to access UNOPS systems and information must be appropriately protected (e.g., anti-virus, full disk encryption, host-based firewalls, etc.)

10.5. UNOPS issued laptops should not be shared with friends or family members. Only UNOPS personnel should be allowed access to devices.

11. Actions Upon Termination

11.1. Upon termination of their contract, personnel agree that they will return all UNOPS-issued IT equipment upon termination of contract (e.g. laptop, mobile phone, etc.).