Headquarters, Copenhagen
28 September 2018

Operational Instruction/Directive Ref. OI.ICT.2018.02

ICT Security and Access

1. Authority

1.1. This Operational Instruction (OI) is promulgated by the Chief Information Officer (CIO) on the basis of a delegation of authority from the Chief Financial Officer (CFO) under OD.FG.2018.02: ICT and Digital Systems Management.

2. Purpose

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

2.2. This OI is promulgated in accordance with the OD.FG.2018.02: ICT and Digital Systems Management and is based on best-practice guidelines in respect to effective security and access to UNOPS ICT systems. It documents how users should treat user accounts, how these accounts should be issued and managed, and the responsibilities of UNOPS.org account holders.

3. Effective Date

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

4. Consequential Changes

4.1. This OI shall supersede and replace:

- AI.CSPG.2014.03: Atlas Security, and
- OD 13: Electronic Communications policy.

[signature redacted]
Tushar Dighe
Chief Information Officer

Operational Instruction/Directive Ref. OI.ICT.2018.02

ICT Security and Access

Table of Contents

1. Definitions

1.1. The term “account 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. User Accounts

2.1. All UNOPS personnel shall be issued a UNOPS.org domain account to facilitate access to UNOPS systems, electronic information, and tools.

2.2. UNOPS partner personnel are not entitled to a UNOPS.org domain account, and should only be issued accounts based upon approval with explicit approval by the CIO.

2.3. UNOPS.org domain accounts 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. UNOPS.org domain accounts shall be personal and non-transferable. Login details shall be personal, confidential and shall not be shared with anyone.

2.6. Personnel shall be responsible and accountable for all communications, actions and approvals performed using their UNOPS account. Personnel to whom a password has been assigned shall not disclose the password to anyone, and shall be responsible and accountable for all actions performed and transactions approved through the use of that password.

2.7. UNOPS account validity shall be based on the account holder’s contract start and end dates, although an account 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.org domain accounts ~~Accounts~~ will terminate on the date of contract expiration. In exceptional circumstances, the account may remain active up to 30 days beyond contract end date, subject to formal approval process. ~~but approval rights in oneUNOPS~~

~~based on applicable Delegations of Authority (DoAs) and accounts with elevated rights shall be automatically revoked upon contract end date.~~ **[Rev. 24.10.2019]**

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 ICT.

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 shall be done using the official UNOPS email platforms.

3.3. Internal memos, documents, and the like which have only made available to UNOPS account holders, shall be considered as internal information and shall not be shared, forwarded or otherwise disseminated to non UNOPS account 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. Download, 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 ICT shall be installed on UNOPS computers, or used for official UNOPS use, without prior approval of UNOPS ICT.

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 ICT.

7. Usage of Systems

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

7.2. Send, post or transmit messages or statements which violates any UNOPS policies or guidelines, or that may affect UNOPS reputation.

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

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

7.2.3. Knowingly ~~a~~effect, or attempt to ~~a~~effect, the performance, availability, integrity or confidentiality of UNOPS or non-UNOPS systems and services. **[Rev. 24.10.2019]**

7.2.4. UNOPS account 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.

8. Data breaches

8.1. Any data or account breaches suspected or confirmed shall be reported to the relevant ICT 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 ICT.