ADMINISTRATIVE INSTRUCTION ON END USER DEVICES

2024

Approved by:	Doug Greene, Director and CIO DIST
Date of approval:	24 March 2024
Contact:	Chief Information Security Officer Division of Information Systems and Telecommunications (DIST)
Date of entry into force:	Revision 1 1 March 2024
Review date:	By 1 March 2029

This document is for general distribution. All rights reserved. Reproductions and translations are authorised, except for commercial purposes, provided the source is acknowledged.

© UNHCR, December 2024

TABLE OF CONTENTS

1. Purpose 4
2. Terms and Definitions 4
3. Scope 4
4. Rationale 5
5. Allocation of UNHCR End User Devices 5

Computers 5

Desk phones 6

Mobile phones, smartphones and tablets 6

Mobile satellite devices (satellite phones, satellite terminals) 7

Other internet-enabled personal devices 7

6. Use of “Bring Your Own” Devices (BYOD) 7
7. Private Use of UNHCR Devices and Services 8

Storage of data on a UNHCR end user device 8

Special considerations for end users separating from UNHCR 9

8. Security considerations for UNHCR End User Devices 9
9. Prohibited Use of UNHCR End User Devices and Services 9
10. Monitoring of Personal and UNHCR End User Devices and Services 10
11. Supported Technologies 10
12. Roles, Responsibilities & Accountabilities 11

End users worldwide (Country Offices / Regional Bureaux / Headquarters) 11

Supervisors/Unit Heads 12

Administrative Units in Regional Bureaux and Country Offices 12

Regional Bureaux IT Lead 12

Division of Information Systems and Telecommunications (DIST) 12

13. Monitoring and Compliance 12

APPENDIX 1: Baseline Controls for all End User Devices 13

1. Purpose

This Administrative Instruction (AI) sets out the principles and standards for acceptable use of UNHCR computer equipment, software (applications), and network facilities by **end users**[1], in order to:

(i) Foster and maintain an environment where users have confidence in the integrity and security of those facilities;

(ii) Ensure all applicable hardware inventory and software licensing requirements are met;

(iii) Establish consistency in computer use procedures and regulations across UNHCR;

(iv) Reduce the likelihood of misuse of UNHCR **IT systems, applications and services**; and

(v) Sustain and support a limited and reasonable degree of use of UNHCR assets for private purposes and professional use of personal assets in limited and well-defined areas.

Revision 1 of this Administrative Instruction has been issued to:

- address various inconsistences in the original;
- further clarify some aspects of the original;
- address the widespread introduction of "cloud" services; and
- align this AI with Revision 2 of the *Administrative Instruction on Access Controls Management* and the recent publication of new policies on data protection and information security.[2]

2. Terms and Definitions

Administrative Instruction (AI) – AI is a common UNHCR acronym which means a type of policy that has been authorised by the division director. This is not to be confused with term *artificial intelligence*.

Asset Focal Point – ensures day to day overall asset management (including issuing assets to custodians), tracks and maintains asset information (custodian, location, transfer, derecognition, retirement etc.) in the Asset Register, ensures proper documentation / comments are attached and recorded in Cloud ERP.

Authorized user/end user – UNHCR staff, affiliate, partner, interns, corporate consultants, and other persons irrespective of employment status with UNHCR – who use any UNHCR IT system, application, or service.

Bring your own device (BYOD) – device(s) that may be the personal property of the end user or provided by a third party (e.g., partner, government, commercial company), where the end user is an employee of that entity.

DIST – UNHCR Division of Information Systems and Telecommunications

End user device/device– any personal computer used by an authorized user, regardless of whether it is owned and controlled by UNHCR. This includes but is not limited to laptop and desktop computers (irrespective of operating system), mobile phones, smartphones, tablets (with or without SIM cards), mobile satellite devices, desk phones, etc.

IT systems, applications, and services – as defined in the AI on Access Controls Management.

Mobile device - a phone, smartphone, or tablet.

Mobile satellite devices - satellite phones, satellite terminals;

Personal or non-standard applications – any application installed by an end user rather than preconfigured and installed centrally.

UNHCR end user device – any end user device that is owned and controlled by UNHCR, remains the property of the organization, and is assigned to an authorized user as custodian.

3. Scope

This Administrative Instruction applies to all UNHCR personnel across the organization, including at headquarters, regional and country level.

The primary target audience is:

[1] Bold terms (in their first use) are defined in the Terms and Definitions section of this document

[2] UNHCR/HCP/2022/02 – General Policy on Personal Data Protection and Privacy, and UNHCR/HCP/2023/02 – Policy on Information Security

- All end users who have, or are responsible for, any end user device used to access any UNHCR IT system, application or service; and
- Managers and IT/Admin Units who are responsible for authorizing the issuance and recovery of UNHCR end user devices.

Devices covered by this Instruction include, but are not limited to:

- Computers, laptops (irrespective of operating system);
- Desk phones;
- Mobile phones, smartphones, tablets (with or without SIM cards);
- Mobile satellite devices (satellite phones, satellite terminals); and
- Other "internet" connected devices that can access UNHCR data (e.g., wearables).

This Administrative Instruction covers all devices provided to end users by UNHCR and any other device that is not UNHCR property but is used to conduct UNHCR business or to access UNHCR data or information (a *Bring Your Own Device* (BYOD)).

UNHCR IT systems, applications, and services covered by this Administrative Instruction are those that can be accessed by the end user using an end user device, irrespective of the location of that system, application or service. Specifically, all "cloud" services are in scope.

Compliance with this Administrative Instruction is mandatory. Non-compliance may constitute misconduct as defined in the AI on Conducting Investigations in UNHCR.[3]

Failure to comply with this Administrative Instruction may result in suspension of access to UNHCR end user device(s) and service(s). In certain cases, non-compliance with this instruction may be considered misconduct and subject to investigation and disciplinary measures.[4]

Out of scope devices

This Administrative Instruction does not cover network devices, shared storage devices, or servers, as these are managed centrally and not assigned to any one end user for their use (shared assets for collective use).

This Instruction also does not cover the allocation and use of "Secure Communications" devices such as HF, VHF, UHF hand-held radios, their supporting infrastructure, or other devices provided locally in high-risk areas or emergency operations support, with the exception of those mentioned in section 5 below.

4. Rationale

Information Technology (IT) is an essential component of the day-to-day operations of UNHCR, providing services to users to facilitate their work. In the last decade, the use of IT resources has grown rapidly with:

(i) New modes of communication changing the nature and speed of collaboration;

(ii) Significantly increased mobility of the UNHCR workforce, in particular to support teleworking; and

(iii) Increased expectations on UNHCR's workforce to be reachable anywhere and to respond quickly.

At the same time, risks such as theft, disclosure of information, disruption of services, fraud, litigation, reputation damage, or excessive costs continue to increase and must be addressed.

The recent issuance of the General Policy on Personal Data Protection and Privacy and Policy on Information Security offer direction that it is the data on an end user device that is most vulnerable and valuable, more than the device itself. This Administrative Instruction addresses these concerns.

5. Allocation of UNHCR End User Devices

This section outlines the principles guiding the allocation of end user devices by UNHCR to end users.[5]

Computers

Each office will assign a laptop[6] computer to an end user following the established administrative

[3] UNHCR/AI/2019/15 – Administrative Instruction on Conducting Investigations

[4] Refer to UNHCR/AI/2018/18 – Administrative Instruction on Misconduct and the Disciplinary Process

[5] See also provisions in the UNHCR/AI/2024/02 – Administrative Instruction on Asset Management in UNHCR.

[6] As of January 2023, desktop computers are no longer approved "standard" items for procurement.

procedures in that office, in line with applicable administrative instructions.[7] These procedures should be guided by the following standards:

- End users should not be allocated more than one laptop.
- A laptop computer with a docking station should be assigned by default to all end users and this should be the primary device used for all UNHCR work. End users who require remote access to IT systems, applications and services should transport the laptop to and from the office and the remote working location, including when teleworking.
- The laptop will be configured with the current version of the Windows operating system; will have biometric authentication enabled (if available); have hard disk encryption enabled; will be registered in the UNHCR Asset Register in Cloud ERP; and will be fully managed by DIST.

Desk phones

For end users who do not need to receive or make external calls, the enterprise messaging platform should be used for all internal communications (avoiding the need for a phone).

Where an end user does need to communicate with external third parties, each UNHCR office may still allocate a phone (physical "desk phone" or "soft phone") and an associated telephone number to end users following administrative procedures in that office. Softphones (software on an end user device) are preferred and should be allocated wherever supported.

End users should be required to provide authentication when making external calls (for professional or private purposes) that will incur charges to the organization. Typical authentication methods include a PIN code or a log-in process before using the device. Charging rules and requirements for personal use are covered under *Administrative Instruction on Cost Recovery of Communications Related Services*.

Mobile phones, smartphones and tablets

UNHCR-purchased mobile devices (phone, smartphone, or tablet) and/or SIM cards may be issued to an end user if they meet one or more of the criteria below:

- For operational reasons they need to be reachable immediately;
- Are "on call" outside of normal business hours;
- Are not normally present at a fixed location and without a mobile device timely communication is difficult;
- Work in situations where UNDSS or the Field Safety Officer recommend the use of mobile phones as an alternative to radio handsets or mobile satellite devices;
- Telework[8] from home or a remote location and need reliable communications *for operational reasons* beyond that available through their laptop (using the enterprise messaging platform);
- Are designated duty officers on special programs, emergency response teams, or officers providing information systems and telecommunications support;
- Visit areas where land-based phones or lines are not available (or restricted) such that the efficiency of UNHCR operations is hampered; or
- Are deployed on emergency missions, with the understanding that the device is to be returned at the end of the mission.

The end user's supervisor and the responsible budget holder must approve the request for mobile devices and agree to cover the purchase cost (if any) and all usage charges for professional purposes.

Transfers of mobile devices between end users is only allowed with the agreement of the original requesting supervisor/budget holder. In such cases, the mobile device must be set back to "factory defaults" and all data removed before being transferred.

After the transfer, the mobile device and responsibility (including budgetary transfer if another unit is concerned) for the item must be transferred to the new user. Transfers must be recorded in the Cloud ERP asset register by the Asset Focal Point.[9]

End users should be allocated a mobile device that is commensurate with the use they will make of it to execute their official duties. In some cases, this will mean being provided with a re-conditioned/re-purposed device or with a model that is one or two generations behind the latest model.

End users who are issued a mobile device should also be provided with a usage guide that indicates how best to reduce on-going usage charges (e.g. using a secure Wi-Fi network in preference to the GSM data

[7] See also provisions in the UNHCR/AI/2024/02 – Administrative Instruction on Asset Management in UNHCR, for asset assignments to UNHCR personnel.

[8] Refer to Policy on Flexible Work and the associated Guidelines.

[9] Refer to UNHCR/AI/2024/02 – Administrative Instruction on Asset Management in UNHCR.

network [10] ; data roaming bundles when traveling outside the country[11]).

Mobile satellite devices (satellite phones, satellite terminals)

Mobile satellite devices may be issued to an end user if they need to be permanently reachable and they travel and work in areas with:

- No mobile network coverage and unreliable land line connections; or
- High security risks as defined by UNDSS or the UNHCR Field Safety Officer.

DIST manages global contracts with providers of mobile satellite devices and services and other entities. Procurement of mobile satellite devices and/or services must follow UNHCR procurement rules and can only be with UNHCR frame agreements (FA) holders. It is the responsibility of field operations to ensure that (i) use of such devices is authorized and has required the necessary import and usage licences are obtained. (ii) the use of such devices is coordinated at the interagency level, as required (iii) FSS officers are consulted, as business owners of security communications, and (iv) Coordination occurs with other operations for common operations (e.g. cross-border).

Regional and Field IT will be the focal points for selection of UNHCR standard technology as required.

End users should also be informed of the high costs of using mobile satellite services (voice and data) and that the administrative budget of the operation is required to cover these costs.

Other internet-enabled personal devices

This includes such things as "smart watches", "AR" (augmented reality) and "VR" (virtual reality) glasses, etc. many of which can be configured to access UNHCR data (e.g. smartwatch notifications with the option to reply) or our IT systems, applications and services. For the purposes of this Administrative Instruction these devices should be considered "personal" and treated like any other BYO device (see Section 6 below).

6. Use of "Bring Your Own" Devices (BYOD)

Use of **Bring your Own Devices** [12] (i.e. non-UNHCR owned and controlled devices) is permitted to access UNHCR IT systems, applications and services if the following is understood and accepted by the end user:

- The use of BYOD must adhere to all relevant UNHCR policies and administrative instructions.
- BYODs must comply with the same minimum baseline controls as mandated for UNHCR-issued devices (see Annex 1); UNHCR reserves the right to restrict and control access to corporate IT applications, systems and services from BYOD;
- The BYOD can only be used for UNHCR work on an occasional basis and must not be the end user's primary working device;
- When used within UNHCR premises (including offices and guest houses), BYODs must only connect to the "UNHCR Guest" or "Visitor" Wi-Fi network. Direct connection to the UNHCR internal networks via a LAN cable or to "UNHCR Internal" Wi-Fi network is not permitted.
- UNHCR remains the owner of all UNHCR data regardless of the ownership of the device and this data must be always kept secure. Obligations of confidentiality continue to apply vis-à-vis personal data and other data classified as confidential.
- UNHCR reserves the right to refuse, prevent, or withdraw access from the end user and/or personal devices or software where it is considered that there are unacceptable security or other risks to our workforce, reputation, systems or infrastructure;
- UNHCR requires the installation and update of UNHCR-approved device management software on all UNHCR end user devices and may require the same on BYODs. Failure to accept this will result in access to UNHCR IT systems, applications and services being limited or refused;
- The device must be fully licensed and run updated software. The end user is expected to maintain all components [firmware, BIOS (Basic Input/Output System), operating system, applications] at the latest level and to apply all security patches promptly on release by the provider of the operating system, computer firmware, or third-party software; where possible "auto-update" must be enabled;
- If the device permits, data encryption and remote data wiping must be enabled;

[10] Secured Wi-Fi network means a trusted network (e.g. UNHCR, home) or public network secured with VPN

[11] Refer to UNHCR/AI/2019/12 – Administrative Instruction on Cost Recovery of Communications Related Services.

[12] For the purposes of this AI, any device not explicitly owned by UNHCR and provided to the end user is considered a "Bring your own Device" (BYOD). Specifically, this also includes devices provided to corporate consultants, partners, or government staff by their employer.

- Inactivity lock-out must be enabled – preferably with biometric activation especially on a full restart of the device after power-down;
- Loss, theft, or compromise (data breach, malware attack, etc.) of any BYOD containing UNHCR data must be reported to the Global Service Desk as if the device was the property of UNHCR;
- Should the end user separate from the Organization, all UNHCR data and software must be removed from the device; and
- In the context of duly authorized investigations, the IGO may request access to UNHCR data stored on the BYOD if the end-user consents.

7. Private Use of UNHCR Devices and Services

End users are discouraged from using UNHCR end user devices and services for private purposes (non-official purposes).[13] However, limited private use is permitted, provided that:

- It would not reasonably be expected to compromise the interests or the reputation of UNHCR;
- It involves no additional cost to UNHCR;[14]
- It takes place during personal time or, if during working hours, does not significantly impinge on such working hours;
- It does not adversely affect the ability of other users to perform their official functions;
- It does not place an additional support burden on IT staff;
- It does not interfere with the activities or operations of UNHCR or adversely affect performance; and
- The contractual status of the end user allows for the reimbursement of costs related to personal usage[15]

End users are required to maintain a separate email address for private use. The use of a UNHCR email address for private purposes should only be done where there is a justifiable reason for disclosing a connection to the organization, e.g. registration on professional training events or communication with bodies that have a legitimate need to know employment status, such as banks.

End users are encouraged to keep personal use of the internet to outside of core office hours.[16]

In UNHCR guesthouses,[17] the supporting office must, where possible, provide internet access with adequate bandwidth for both professional and personal use in common areas and private quarters. This access will be subject to normal UNHCR internet content filtering rules. Each location may establish additional local rules and guidelines to ensure that there is no adverse effect on legitimate work activities. End users shall not share the credentials to internet access outside of professional needs to non-UNHCR users.

Storage of data on a UNHCR end user device

UNHCR provides multiple facilities to end users where they can store their working files and other data for their individual business use – e.g. the UNHCR email system or cloud storage. This data is automatically replicated between the cloud service and the end user device so that the end user has continuous access even when disconnected. It also gives the ability to work on a file from multiple devices if needed and protects the end user against hardware failures.

Use of this service by all end users is strongly recommended. Any end user who wishes for personal reasons not to use UNHCR cloud services must personally ensure all data is fully backed up.

End users need to be aware that:

- If they store private data on UNHCR devices, this will also be synchronized to UNHCR's cloud services. This includes email (with or without attachments) and files (of any type) on UNHCR's cloud storage services;

[13] UN Staff Regulations and Rules, Article 1, Regulation 1.2(q), applies.

[14] Refer to UNHCR/AI/2019/12 – Administrative Instruction on Cost Recovery of Communications Related Services

[15] UNHCR/AI/2019/12 – Administrative Instruction on Cost Recovery of Communications Related Services

[16] In locations outside Headquarters, core office hours are defined by the Regional Bureau Director, Representative, or Head of Office reflecting the daily work schedules of personnel in their offices.

[16] Refer to UNHCR/AI/2019/8 – Administrative Instruction on UNHCR-Provided Accommodation in the Field.

- Their private data may still be retained in backups and other storage, even if deleted from the end user device.
- This data may – under certain circumstances – be searched by UNHCR for legitimate and lawful reasons.

Special considerations for end users separating from UNHCR

When an end user leaves UNHCR (separation, contract end, retirement,[18] etc.), their account will be disabled following the process outlined in the Administrative Instruction on Access Controls Management. However, the data associated with that account will not immediately be deleted and will be retained in backups and archives based on the respective retention policies of the repository. Even after the end user's account is deleted, the full content of their email will be retained for several years.[19] This permits authorized UNHCR personnel (e.g., the IGO) to request the recovery of data in the support of an investigation.

Thirty days before an end user account is deleted, the user's manager will be notified and given the opportunity to review the contents of the end user's UNHCR personal cloud account.

Managers or IT support staff shall not be given any access to a separated end user's mailbox, even with business justification. Email should only be extracted and read by others if supervised by IGO.

8. Security considerations for UNHCR End User Devices

Theft or accidental loss of an UNHCR computer or mobile device potentially leaves the entire contents of the device, and the data stored on it, vulnerable to extraction and misuse if not appropriately protected through encryption.

All UNHCR Windows and Mac devices must have their hard disks encrypted with corporate tools.[20]

Every mobile device must be protected with a complex password/PIN/pattern and/or biometrics at power-on during the device issuance process to protect the data contained on the device in the event of loss or theft. These devices must also have an inactivity timeout enabled requiring the same unlocking as for power on.

All end user devices containing a SIM card must have PIN and PUK codes enabled.

Every UNHCR end user device (computer, mobile device etc.) must have its operating system and applications regularly upgraded to protect against security flaws and attacks.

9. Prohibited Use of UNHCR End User Devices and Services

UNHCR end user devices and services must not be used for any activity that is inconsistent with the mission of the organization, misrepresents UNHCR, is in contravention of UN Staff Rules and Regulations or the UNHCR Code of Conduct, violates any UNHCR policies and official guidance, or would be considered unlawful by local/national laws.

UNHCR end user devices and services must not be used for:

Political and/or reputationally damaging activities

- Any activity that could cause reputational damage to the organization.
- Promoting a political party/movement, or a candidate for political office, or campaigning for or against government decisions.

Network security and integrity

- Intentionally causing disruption to computer systems or networks belonging to UNHCR or others.
- Compromising the security of UNHCR's resources.
- Circumventing internet access control, security, or auditing.
- Exposing UNHCR network resources directly to the Internet, bypassing network security controls.
- Installation and use of software or hardware tools which could be used for the unauthorized monitoring of electronic communications (without prior approval).

Data security and integrity

- Compromising the confidentiality, availability or integrity of UNHCR data.
- Any activity that would compromise the privacy of other users.
- Forging a message or email header information.
- Accessing, or attempting to access, to another person's mailbox or files regardless of whether the access was successful or whether any messages of files accessed contain sensitive (non-public) information.

[18] See also section 12 End User Responsibilities

[19] *Litigation Hold* is a service that has been enabled at the organizational level. Email content in the Litigation Hold is automatically deleted six years after deletion in the End user's mailbox or the deletion of the account.

[20] DIST may be contacted for a list of approved corporate tools

- Auto-forwarding of UNHCR email messages to an external account (non-UNHCR.ORG address) without explicit written permission.
- Deliberately flooding a user's mailbox with automatically generated mail.
- Transferring large data files (e.g., watching Netflix, YouTube, large file attachments, video, or radio streaming, VoIP) through a satellite terminal.
- Any activity that would intentionally contradict with safeguarding and responsible use of UNHCR's resources.

Software license violations

- Downloading services or software from unreliable sources (e.g., unrecognized application stores other than the official Google Play, Apple App Store, Windows Store), especially software advertised as "cracked" or free versions of paid products.
- Installing any "cracked" software or commercial software that is not fully licensed by the end user or UNHCR.

Content violations

- Infringe intellectual property rights (e.g., unlicensed installation, distribution, or copying of copyrighted material)
- Peer-to-peer file sharing (e.g., BitTorrent);
- Anything that would be contrary to the UNHCR Code of Conduct – including viewing, creating, downloading, hosting, or transmitting pornographic, offensive, or obscene material (information, images, video clips, audio recordings, etc.) which could cause offence to others on the grounds of race, religion, gender, sexual orientation, disability, age, or political beliefs;
- Retrieving, creating, hosting, or transmitting any material which is designed to cause annoyance, inconvenience, needless anxiety to others, or is defamatory in nature.

Non-UNHCR related usage

- Transmission of unsolicited commercial or advertising messages, chain letters, or other "junk-mail" or "spam" of any kind.
- Commercial activities, such as running any sort of private business, advertising, or performing work for personal gain or profit.
- Other private purposes unless exceptionally allowed by respective UNHCR policies.

Any violation(s) must be reported to the IGO, and may be subject to potential investigation and disciplinary action.

10. Monitoring of Personal and UNHCR End User Devices and Services

UNHCR reserves the right to monitor and log data traffic transferred between end user devices and UNHCR systems, both over internal networks and via the Internet. This could include the processing of personal data of end users for monitoring or security purposes.

UNHCR may process end user personal data for the following purpose(s):

- maintaining the technical integrity and effective operation of UNHCR end user devices and other IT services. This requires the monitoring of all inbound and outbound email and other communications to and from corporate systems.
- ensuring the security of UNHCR systems, investigating IT security incidents, and supporting UNHCR internal accountability processes, such as investigations of misconduct. UNHCR-DIST will monitor an end user device by logging all activity of the end user device.

In exceptional circumstances, or to comply with its legal obligations, UNHCR may access UNHCR-owned data and information stored on a BYOD with the end-user's consent. Under these circumstances all reasonable efforts will be made to ensure that UNHCR does not access user's private information.

11. Supported Technologies

DIST defines all UNHCR-wide technology standards for IT and telecommunication devices and services. The only supported UNHCR end user devices are those that are published in CIMT (the Common ICT Management

Tool) [21] and which are available in Cloud ERP for procurement.

Only supported devices may be purchased using UNHCR funds.

Only devices meeting approved standards are guaranteed to be supported by DIST. Other products will not be supported and may by blocked or restricted if needed for operational reasons.[22]

12. Roles, Responsibilities & Accountabilities

End users worldwide (Country Offices / Regional Bureaux / Headquarters)

All end users must:

- Enable all available security features on every end user device: SIM lock, power on password/PIN, screen timeout, data encryption, remote wipe, etc. All devices, whether UNHCR or BYOD, must comply with these security configurations.
- Regularly update the software (e.g. iOS/Android update services). All devices, whether UNHCR or BYOD, must comply with these security configurations.
- Ensure the safekeeping, care, physical security, and appropriate use of the devices and accessories assigned to them;
- Acknowledge that UNHCR end user devices are the property of the organization. They must not be lent to anyone who is not themselves an authorized user including, but not limited to, family, friends, or members of the public;
- Not remove or modify security features (including device encryption) configured by IT;
- Utilize the most cost effective and secure connections for all data usage. General guidance on cost-effective use of smartphones is available on the Intranet.[23] Regional Bureaux and Country Offices are encouraged to adapt this guidance for their specific countries;
- Obsolete devices or devices running obsolete software may be denied access to the UNHCR network and UNHCR IT systems, applications and services;
- Submit a UNHCR end user device for examination by the IGO, if requested as part of an official complaint assessment, investigation or other authorized activity;
- Cooperate fully with a duly authorized investigation that would require accessing relevant data stored on a BYO Device.

Prior to separation/transfer:

- Ensure all data of institutional value is moved to a corporate repository, transferred to their supervisor or to another colleague; this includes messages from the email system and files from the end user's cloud storage service;
- Delete all private files from their UNHCR end user device and the central services (Email, cloud storage). It is the end user's sole responsibility to retain copies of any private files;
- Perform a full "factory reset" before returning the device, or ensure that the local (IT) Focal Point resets the device on return (this includes providing any passwords or security lock access to the device);
- If, on separation for retirement, the end user elects to purchase a UNHCR device for their private use, then all UNHCR licensed software must be removed and all UNHCR data deleted; and a "factory reset" should be performed;
- Remove any UNHCR information (e.g. email attachments, documents / spreadsheets, data sets, etc.) stored on any end users' personal device as soon as it is no longer required;
- Remove all UNHCR information from a personal end user device and reset it to the manufacturers' original settings before selling, exchanging, or disposing of the device;
- When changing their position, unit / location, disposing of, or transferring a device to another end user, ensure that the local IT Asset Focal Point is informed, and that the Cloud ERP Asset Register is promptly updated in line with the Administrative Instruction on Asset Management.

In case of loss/theft:

- In case of loss, theft or compromised data (data breach, malware attack) of an end user device (property of UNHCR or BYOD) the end user must contact the Global Service Desk to register a security incident and request blocking the device and its access immediately.
- A written report on the event should be submitted, through his/her supervisor (as per the applicable procedures for asset management) and to the Data Protection Focal Point (if the device contained personal data).

[21] CIMT is available for authorized users only

[22] The DIST Architecture Review Board (ARB) approves IT technical standards.

[23] UNHCR/AI/2019/12 – Administrative Instruction on Cost Recovery of Communications Related Services

Supervisors/Unit Heads

Supervisors/Unit Heads have the authority to:

- Provide initial approval for the UNHCR end user device allocation;
- Approve purchase of the UNHCR end user device, along with any expenses incurred;

They have the accountability for:

- Ensuring that end users separating from UNHCR have completed a full hand-over of all organizational data;
- Ensuring that the personal cloud storage contents of an end user who has separated, only contains copy (backup) data and files that have institutional value. Under no circumstances should a supervisor make copies (backups) of files that are the personal property of the end user; and
- Periodically review (at a minimum, annually) the continuing need for UNHCR end user device allocation.

Administrative Units in Regional Bureaux and Country Offices[24]

The Administrative Unit, supported by the local IT Asset Focal Point is accountable for:

- Ensuring the requirements of this AI are followed in their respective office;
- Maintaining the accounts for phones and SIM cards issued by the office with individually named owners (custodians);
- Maintaining up-to-date records in the organizational asset registry of all UNHCR End user Devices with individually named owners (custodians) issued by the office;
- Determining the best mobile network calling plan (subscription) for mobile devices and ensuring this is followed;
- Providing guidance and support for UNHCR devices and the standard application software running on these devices. Local IT staff will not provide support for any BYOD or for personal or non-standard applications that the end user may have installed on a device; and
- If not done by the end user before returning the device, resetting it to "factory default" settings and wiping all data from returned or obsolete devices prior to re-issue or disposal.
- Ensuring that the end user provides all passwords and security lock codes to perform this action.

Regional Bureaux IT Lead

The Regional Bureau IT Lead is accountable for:

- Supporting the implementation of this AI in the countries in their region;
- Providing guidance to Country Offices in their region.

Division of Information Systems and Telecommunications (DIST)

For end users in headquarters, DIST has the authority to:

- issue all UNHCR end user devices and maintain up-to-date records in the Cloud ERP Asset Register with individual named owners (custodians) of all UNHCR end user devices assigned to colleagues in Headquarters;
- issue all SIM cards and maintain the telecommunications accounts for mobile devices and SIM cards; and
- reset to factory settings and wipe all data from the returned or obsolete devices prior to re-issue or disposal.

DIST is accountable for:

- Establishing and maintaining current and fit for purpose solutions and standards for end user devices and provide guidance on usage. This includes the minimum mandatory baseline controls for all end user devices (see Appendix 1).
- Device monitoring to ensure compliance with the defined baseline controls.
- Taking appropriate corrective action when non-compliance is detected.
- Providing guidance and support only for UNHCR devices and the standard application software running on these devices.

13. Monitoring and Compliance

For Headquarters, monitoring will be performed by DIST IT Operations Service – End User Device team.

For all other locations, monitoring will be performed by the Administrative Unit of the respective Bureau / Office in coordination with the Regional Bureaux IT Lead.

[24] Includes multi-country offices, field and sub/ branch offices.

APPENDIX 1: Baseline Controls for all End User Devices

The following provisions apply to all end user devices (UNHCR or BYOD) used for accessing UNHCR data or for conducting UNHCR business. For devices managed by UNHCR, the following provisions will normally be put in place centrally and must not be disabled. The same provisions apply to BYOD irrespective of whether they are the personal property of the authorized user or were provided to them by their employer (partners, corporate consultants, etc.).

- The operating system is genuine, supported, licensed, and auto-update is enabled;
- Using a "jail-broken" operating system to access UNHCR data, applications, systems, and services is strictly forbidden;
- Patching process for the operating system ensures recent updates have been installed (within 1 month of their release);
- Security updates for utilities, drivers, and firmware (BIOS, etc.) are installed within three months of issue by manufacturer;
- Hard disk encryption of all data on the device with Windows BitLocker or equivalent;
- An up-to-date antivirus solution installed (e.g. Defender for Endpoint) and regular scans scheduled and run;
- Main applications (including document authoring, presentations, spreadsheets, and email) are licensed versions (or open-source software) with auto-update enabled;
- A device firewall is installed and running with basic web content filtering, to block content that could reasonably be deemed to be illegal, inappropriate, or objectionable;
- Device screen lock is enabled (at power-on and following a period of inactivity); and
- Local passwords follow UNHCR standards (minimum length and complexity).

This list is not exhaustive and may be updated from time to time.

Failure to comply with these controls could result in access to UNHCR data or IT services being blocked or discontinued until the device is brought into compliance.