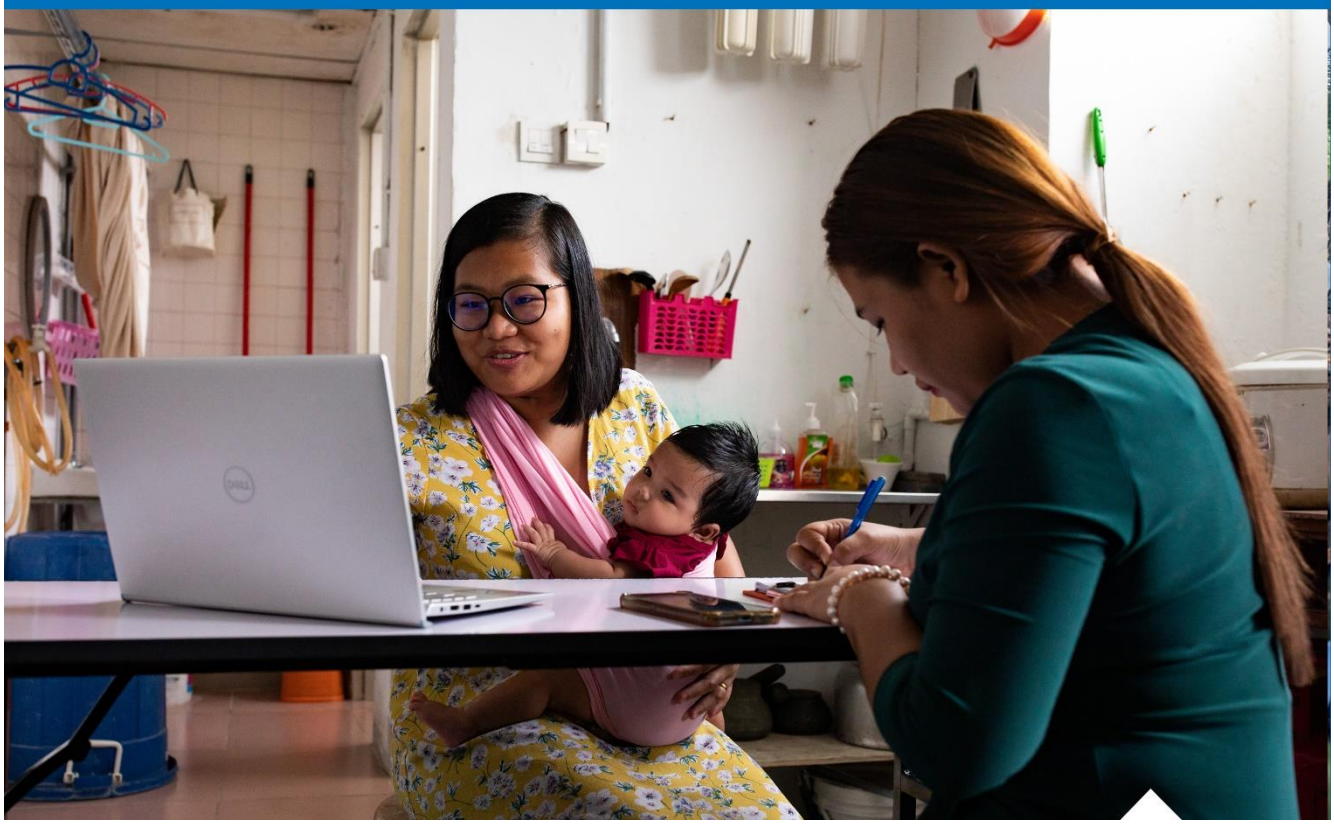
EXTERNAL GUIDANCE NOTE FOR UNHCR FUNDED PARTNERS ON THE MINIMUM INFORMATION SECURITY BASELINE



Version: 1.0

Published: 19 March 2024

Table of Contents

Annexes

1. PURPOSE

1.1 The goal of this document and associated initiatives is to improve the state of information security in UNHCR-funded partners to whom UNHCR entrusts the processing of personal data of forcibly displaced and stateless persons and that UNHCR encourages to use UNHCR's information systems to deliver our joint goals.

1.2 This will be achieved through a better understanding of the capabilities and gaps we face today in partner information security and by working collaboratively to raise information security standards.

2. RATIONALE

2.1 **Achieving this goal will help UNHCR to:**

2.1.1 Safeguard UNHCR processes and systems (such as Population Registration and Identity Management Eco-System (PRIMES) when contributed to and used by partners.

2.1.2 Protect personal data when delivering services to forcibly displaced and stateless persons in an "indirect" (via others) as well as a "direct" (UNHCR to person) model.

2.1.3 Make partners aware of the potential risks to UNHCR's and the partner's reputation if data is not appropriately protected.

2.1.4 Sustain the reputation of UNHCR.

2.2 **Achieving this goal will help partners to:**

2.2.1 Strengthen their overall cybersecurity posture, reducing the risk of cyber threats, data breaches, and other security incidents.

2.2.2 Protect sensitive data from unauthorised access, disclosure, or theft.

2.2.3 Adapt to evolving threats and technologies ensuring ongoing protection of information assets and maintaining cybersecurity resilience.

3. AUDIENCE

3.1 Project managers or IT teams in UNHCR funded partners.

4. SCOPE

4.1 **To define a minimum IT and information security baseline for funded partners which**

would be:

4.1.1 Considered during UNHCR's partnership selection process,

4.1.2 Committed to as part of UNHCR's Partnership Terms, when entering into a funded partnership contract, and

4.1.3 Subject to periodic internal control assessment and project audit processes by UNHCR, with progress against UNHCR recommendations monitored during implementation.

4.2 The baseline is applicable to all funded partners to whom UNHCR entrusts the implementation of projects specified in a signed partnership document along with the assumption of full responsibility and accountability for the effective use of resources and the delivery of outputs as set forth in such a document**. It is not applicable to UNHCR itself, grant agreement partners1, private sector partners, IFRC, commercial organizations (suppliers, service providers), nor other UN agencies.**

4.3 Key elements have already been required since 2015 under the partnership agreement General Conditions of Contract and a data protection annex signed with funded partners where they are processing personal data.

5. UNHCR'S APPROACH

5.1 **This is the first version of such a document and UNHCR will continue to review and update it to ensure that it remains relevant and effective.**
UNHCR's approach has been to:

5.1.1 Deliver a baseline which is understandable and **achievable to most partners.** It is a minimum, not a target.

5.1.2 Combine data protection and information security requirements to create a single set of layered requirements, rather than two sets of rules.

5.1.3 Focus on **practical controls** that a UNHCR Project Control function, Programme function or country Cyber Security Focal Point could check.

5.1.4 Build it into standard processes as part of **self-assessment checklists and tools** (for example the ICA/Q and Data Protection and Information Security Self-Assessment) for partners to assess their status and see if they need help (and to prioritise work).

5.1.5 Use it as the basis for **cybersecurity training** for partners which will further support them in implementing necessary IT and information security practices.

[1] A grant agreement is a type of agreement with organizations or groups in which persons with direct lived experience of forced displacement play a primary leadership role and whose stated objectives and activities are focused on responding to the needs of refugees and/or related communities.

6. WHAT THIS DOCUMENT DOES NOT IMPLY

6.1 It does not imply that UNHCR will finance or give partners equipment or solutions to solve any gaps identified from its application. This would be one option, as would be preferring partners with better IT, or incentivising partners to "raise their game" themselves.

6.2 It does not commit UNHCR to recommend, design or deliver any standard or approved worldwide IT solutions to partners.

6.3 This document does not guarantee absolute protection against cyber threats, as the threat landscape is constantly evolving and requires ongoing vigilance.

6.4 It does not cover national legal requirements. It is the responsibility of each partner to ensure that they are in compliance with all relevant laws and regulations in their respective countries.

7. THE FUNDED PARTNERS BASELINE

7.1 **The baseline is a minimum, not an aspiration or target, and it is not exhaustive. It is split into two sections:**

7.1.1 Good practice safety and 'hygiene' requirements for **every partner** in a partnership relationship with UNHCR.

7.1.2 Additional requirements where partners are **processing personal data on behalf of or jointly with UNHCR** or with whom personal data is shared, including partners using UNHCR-owned information systems such as PRIMES.

7.2 Partners will be required to meet this baseline progressively over time. Application of the baseline will take place through multiple channels, including concept note evaluations, self-assessment questionnaires, internal control assessments, implementation monitoring and project audits.

7.3 UNHCR also encourages partners to seek guidance and support from its IT and information security teams if they have any questions or concerns about meeting the baseline requirements. By working together, UNHCR and its partners can better protect the sensitive information of refugees and other vulnerable populations.

8. BASELINE – ALL UNHCR FUNDED PARTNERS

8.1 **This section applies to all partners with whom UNHCR works, where UNHCR either shares data, offers financial support, offers the use of the UNHCR brand or otherwise cooperates.**

8.1.1. **Focal Point:** The partner has a named IT focal point capable and qualified to address IT, information security and data protection risks.[2]

8.2.2. **Operating System:** The operating systems on the partner's computers are genuine, supported, licensed and auto-update is on. Recent updates have been installed to ensure that the system is protected against known vulnerabilities.[3]

8.1.3 **Antivirus:** The partner has an up-to-date antivirus solution on its corporate PCs. Regular scans are scheduled to detect and remove any malware or viruses that may have infected systems.

8.1.4 **Applications:** The partner uses licensed versions (or open-source software) for its main applications and keeps them up to date to ensure that they are protected against known vulnerabilities (specifically for document authoring, presentations, spreadsheets, financial systems, payroll, web browser and email). [4]

8.1.5 **Perimeter:** The partner has a perimeter device (a home router at least) with standard Wi-Fi encryption (WPA 2 or above). Default passwords are changed to prevent unauthorized access, and the router separates guests (visitors) from staff Wi-Fi to ensure that sensitive information is not accessed by unauthorized individuals.

8.1.6 **Access Control:** Access to key systems (including accounting systems) is restricted to named user IDs with complex and regularly changed passwords. This will help prevent unauthorized access to sensitive information.

8.1.7 **Training:** Partner staff have been trained since joining in basic information security in a matter of the partner's choice. This will help ensure that they are aware of the risks and how to mitigate them, reducing the likelihood of a security breach or data loss.

9 BASELINE – FUNDED PARTNERS PROCESSING PERSONAL DATA

9.1 **An additional six requirements apply to partners who are processing personal data that is jointly or solely controlled by UNHCR, either through file exchange or through use of UNHCR systems such as proGres and BIMS.**

9.1.1 **Encryption of storage:** The partner uses encryption for all its personal data storage including hard disk encryption (such as BitLocker) for its laptops (in case they are stolen). [5]

9.1.2 **Encryption in transit:** When sharing information on forcibly displaced and stateless persons over the Internet, the partner always uses encrypted methods such as

[2] *Focal Point* - A person who understands computers to some degree and is capable and empowered to address the type of issues addressed here. Does not have to be an employee.
[3] *Recent* - everything from last month and before. Exceptions for partners are be documented in sanctioned countries, during the assessment.
[4] Exceptions for partners in sanctioned countries are documented during the assessment.
[5] See also previous model Data Sharing Agreement (DSA) clause 11.2 (d).

password-protected files or other commercial, custom, or UNHCR-provided tools.[6] It does not email Excel or csv files containing personal data unencrypted. [7] This will help ensure that personal data is not intercepted by unauthorized individuals.

9.1.3 **Email:** The partner does not use personal email accounts (e.g. Gmail, Yahoo or Hotmail) for the transfer of personal data, but email accounts issued by or managed by the partner, so that access can be withdrawn if an employee leaves the partner. This will help ensure that personal data is not accessed by unauthorized individuals after leaving.[8]

9.1.4 **MFA:** The partner uses multi-factor authentication (MFA) whenever technically possible for its main applications, including any case management tools and document drives, and for access to UNHCR-managed refugee systems. This will help ensure that only authorized individuals can access personal data.

9.1.5 **Account sharing:** The partner does not allow the sharing of user accounts. All operational activity can be traced to a specific person. No personal data processing or other key transaction (since as financial transactions) takes place using generic/shared accounts. This will help ensure that personal data is not accessed by unauthorized individuals and that all activity can be traced back to a single unambiguous author.

9.1.6 **Offboarding:** When offboarding partner staff, access to databases, work email accounts and other platforms containing personal data are immediately removed upon closure of the partnership. All project assets, including devices, are returned by the staff member and UNHCR data and access codes are removed from any partner project assets and partner staff-owned devices and accounts. This will help ensure that personal data is not accessed after an employee leaves the partner organization.

10 MONITORING AND COMPLIANCE

10.1 This baseline is intended to clarify and define what UNHCR operations expect from every funded partner, with various points of application including partnership selection; capacity assessment; implementation monitoring and partner project audit.

10.2 For funded partners, UNHCR may, during a competitive partnership selection process, weight such criteria amongst others for partner selection.

10.3 Individual gaps and opportunities to strengthen partners' capacity will be identified from the assessments and followed up during implementation monitoring of funded partners at the operational level. When a data protection and information security capacity assessment is conducted on a funded partner (which includes these requirements), applicable risk and treatments plans will be added to the project workplan risk register and raised as implementation monitoring recommendations and followed up. Compliance, and risk management at the individual partner level, is therefore devolved to the UNHCR operation.

[6] Such as WeTransfer, Dropbox, OneDrive, UNHCR's SFS, Oracle Aconex.
[7] Corresponds to previous model DSA clause 11.2 (e).
[8] Special approaches may be needed for heavily sanctioned countries.

11 CONTACT

11.1 For further advice or information concerning the application of this document, please contact the country cybersecurity focal point or the UNHCR Chief Information Security Officer (CISO) at ciso@unhcr.org.

ANNEX1: BASELINE CONROLS AND MITIGATION MEASURES

No.	Control	Control description	Detailed requirement	Risk level	Possible mitigating measures to reduce risk
1	**Focal Point**	The partner has a named information security focal point or IT focal point.	Focal point name	yes-low, none-medium	• Name or appoint a person who is responsible (and the main focal point) for addressing IT, information security, and data protection risks. Can be a contractor.
2	**Operating Systems**	The operating systems on the partner's computers are genuine, supported, licensed and auto-update is on. Recent updates have been installed.	Genuine Supported Licensed Auto update	yes-low, no-high	• Buy licenses. • Regularly perform updates and upgrades. • Use automation tools to patch and upgrade.
3	**Antivirus**	The partner has an up-to-date antivirus/anti-malware solution on its personal computers. Regular scans should be scheduled to detect and remove any malware or viruses that may have infected the systems.	Up to date Regular scans	yes-low, partially-medium, no-high	• Choose, buy and implement an anti-virus solution. • Run real-time AV protection with automatic virus definition updates. • Run regular automated AV scans, if possible. • Keep inventory or use automated tools to ensure each PC is current and reporting.
4	**Applications**	The partner uses licensed versions (or open-source software) for its main applications (specifically, for document authoring, presentations, spreadsheets, financial systems, payroll and email services). These applications has to be kept up to date to ensure that they are protected against	Licensed Up to date	yes-low, partially-medium, no-high	• Buy licenses and/or support if anything has gone out of support (if legally possible in your country). • Make sure that applications are consistently maintained and kept up to date.

		known vulnerabilities.			
5	**Perimeter**	The partner has a perimeter device (home router at least) with standard Wi-Fi encryption (WPA 2 or above), the default passwords are changed and the router segregates guests (visitors) from staff.	Modern Home Router Default password changed Segregates guests and staff	yes-low, partially-medium, no-high	• Actively manage and maintain the security of your perimeter (e.g. your Wi-Fi internet router). • Control which users, and devices, can access their networks. • Run a guest service and separate guests (visitors) from staff Wi-Fi.
6	**Access control**	Access to key systems (including accounting systems) is protected by named user IDs and complex and regularly changed passwords (or multi-factor authentication – see below).	Named user IDs Complex password Password changes regularly	yes-low, partially-medium, no-high	• Ensure everyone is using individually named user accounts for their day-to-day work. • Close down any shared user accounts. • Implement a password policy to ensure passwords are kept secret and well-managed.
7	**Training**	Staff are trained in information security and their progress is recorded. Best Practices for ensuring the acceptable use of assets are defined.	Information security training provided to all staff Acceptable use of assets	Training on data protection & information security provided-low, only one training provided-medium, no training provided-high	• Provide training to your staff and contractors. including in zipping files with passwords or using built-in password functions in Word, Excel, email. • Train employees on encryption in transit and how to use it properly. • Train employees on how to identify phishing attacks and avoid clicking on suspicious links or downloading attachments from unknown sources.
8	**MFA**	The partner uses multi-factor authentication (MFA) whenever technically	Email MFA Case management	yes-low,	• Enable MFA wherever offered by the vendor Prefer vendors who support industry

		possible for its main applications, including any common case management tools and document drives, and for access to UNHCR-managed refugee systems.	and shared drives MFA UNHCR system (e.g. ProGres) MFA	partially-medium, no-high	standard MFA solutions. • Explain to staff how to use it. • Work with UNHCR PRIMES Support Unit to enable MFA on your UNHCR partners accounts.
9	**No account sharing**	The partner does not allow the sharing of user accounts. All operational activity can be traced to a specific person. No personal data sharing takes place using generic/shared accounts.	No transactions on key systems with generic or shared accounts. Important UNHCR-related work mails not sent from generic mailboxes	yes-low, no-high	• Ensure all users are given individual user accounts. No "admin", "partner name123", "user1". • Privileged and admin rights are kept to named individuals and never use for daily work
10	**Encryption of storage**	The partner is using encryption for all its storage of personal data including hard disk encryption (such as BitLocker) for its laptops (in case they are stolen).	BitLocker installed and operating Server /data repositories encrypted USB encryption available and used	yes-low, no-high	• Turn on encryption if available. Store recovery keys safely. • Store data in UNHCR encrypted services (e.g. UNHCR SharePoint, PRIMES, Kobo) where appropriate. • Ensure staff are aware of the need to carefully protect any USB drives, phone or laptops containing sensitive information by providing awareness training,
11	**Encryption in transit**	When sharing personal data of forcibly displaced and stateless people over the Internet, the partner uses encrypted methods such as password-protected files or other commercial, custom or UNHCR-provided tools. The partner does not email Excel or csv	Password protected files used – no open excel files attached to emails Encryption of email used (if available in products) Do not send password in same email	yes-low, no-high	• Transfers data using UNHCR encrypted services (e.g. UNHCR SharePoint, PRIMES, PROMS. • Buy or license storage and transfer services from providers (in general avoid free services as free services generally mean you are the product being sold).

		files containing personal data unencrypted (and when using encryption, does not send the password in the same mail).	Share personal data using commercial or UNHCR provided tools		
12	**Email**	The partner does not use personal email accounts (e.g. Gmail, Yahoo or Hotmail) for the transfer of personal data, but email addresses issued or managed by the partner, so that access can be withdrawn if an employee leaves the partner.	No personally owned email IDs After leaving, an employee email access is withdrawn	yes-low, no-high	• Buy a domain (USD 20/y). • Buy a managed email service from a commercial provider (there are many good low-cost services). • Write and use procedures to promptly remove staff who separate from organizational email.
13	**Offboarding**	When offboarding partner staff, access to databases, work email accounts and other platforms containing personal data are immediately removed upon reassignment or separation. All partner devices (laptops, mobile phones, keys, access cards) are returned and UNHCR data is removed from any staff owned devices and accounts.	All personal data immediately removed from user devices Partner-owned devices are returned to partner UNHCR data is removed from personal devices Offboarding record maintained	yes-low, no-high	Ensure offboarding processes are written and effective. Ensure someone is responsible for managing and doing the offboarding of Partner staff. Maintain a record of the offboarding process for each employee to ensure that all tasks have been completed and to use as a reference in case of any future audits.