

---

# CLASS I SYSTEM UNICEF SECURITY REQUIREMENTS

---

## 1. Categorization

This document describes UNICEF's security requirements for systems classified as Class I. UNICEF recognizes 4 classes of information: Class I - Confidential, Class II - Internal, Class III - Restricted and Class VI - Public. All classes are based on the business value of the information. As such it is the business that drives the data classification.

Class I systems carry the highest classification throughout the organization. This classification is designated for highly sensitive and critical UNICEF ICT assets.

| System Classification | Description  | Asset Rating    |           |              |
|-----------------------|--|-----------------|-----------|--------------|
|                       |  | Confidentiality | Integrity | Availability |
| Class I               | A system which stores and / or processes confidential information critical to UNICEF operations, individual's safety and / or is directly linked to critical business processes. Unauthorized access may severely impact UNICEF operations / business processes, individual's personal safety and or their identity. | HIGH            | HIGH      | HIGH         |

It shall be noted that the system classification and resulting security requirements are based on input provided by the system owner / sponsor or their delegated authority. That said, if the value - and hence the classification - of the information changes at any point during its life cycle it is the responsibility of the owner or their delegate to reinitiate the information / system classification process. This requirement is an obligatory responsibility of the system owner to ensure proper protection of the system and the underlying information assets.

## 2. Applicability / Scope

The security requirements outlined in this document are mandatory and apply to any internal or external party who is providing a solution, a system or a service to UNICEF which processes, stores or transmits information that meets the classification criteria reflected in this document.

### 2.1. Class I System Properties

A defining property of a Class I system is as follows: a system / service(s) which processes and or stores **personal data** or **confidential UNICEF data** or is **linked to a critical business process(es), as defined in this section.**

#### Personal data

UNICEF defines personal data similar to article 9 of the EU general data protection regulation 2016/679 (GDPR):

*“Data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.*

*Profiling data when there is any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.”*

Any system that processes and or stores personal data is a Class I system.

#### Confidential UNICEF data

Information such as, but not limited to, sensitive Program Division Reports, HR Records, investigative documents, etc. Any system that processes and or stores confidential UNICEF data is a Class I system.

#### Linked to a critical business process

The input received during this phase, shall be viewed as “initial”, and will require follow-up consultation with the office of Business Continuity prior to the system / solution becoming an operational asset (placed into production). Any system that is linked to a critical business process shall be classified as a Class I system.

## 3. Security Requirements

All the requirements covered in this area reflect controls that shall be included in any Request for Proposal (RFP), Work Orders / Package, Term of Reference (ToR) or any document that may be used by a service provider or professional services entity which are providing UNICEF a "Product" or "Service".

Both business owner (data controller) and the service provider (data processor) share the obligations for ensuring proper implementation of the requirements.

It shall be noted that the requirements outlined in this section be viewed as an additional layer to complement vendors existing security eco system and not a replacement. In cases where a service provider's controls are more restrictive the service provider's controls shall prevail and be formally captured by both parties.

### 3.1. General Security Requirements

- a) UNICEF shall reserve the right to assess the quality and accurateness of outsourced software development and operational maintenance of the system / application; whether it be through security assurance testing or through external security assessment.
- b) Solution / Service shall be protected from unwanted network traffic by network filtering or separating measures that lay outside of the system; such as externally controlled routers and firewalls.
- c) The system shall have proper end-point protection, with the following minimum requirements:
  - malicious code protection measures
  - host firewall configured utilizing, at a minimum, least privileged access controls (services, user, communication access).

### 3.2. Validation of Security Controls

- a) UNICEF shall reserve the right to periodically validate the implementation of the security requirements outlined in this document via:
  - Security Assurance Testing
  - Vulnerability Testing
  - Penetration Testing
  - Audits
  - On-site checks

### 3.3. Compliance & Certifications

- a) Any vendor that provides hosting of any class I system, shall carry, at a minimum ISO2700K, certification and provide the following documents for view: ISO Certification, SoA, SOC 2, and SOC3 audit findings.

### 3.4. Identification, Authentication and Authorization

- a) The service provider shall follow the principle of least privilege, guaranteeing that users, group, role, and device identifiers will be unique, assigned to each entity (user or process). Each application user role shall have a correspondent database connection according to its privileges.
- b) The service provider shall centrally manage the user account using federated identities and whenever possible integrate their solution with the UNICEF Identity Management System.  
In case authentication is password based; the password shall forcefully adhere to the common best practice quality requirements and will be forcefully renewed frequently. The allocation of authenticators will be controlled and management through a formal process.
- c) Multi-factor authentication will be used for:
  - privileged accounts and
  - user access outside of UNICEF trusted network.
- d) All the user and system accounts shall be disabled after a defined period of inactivity, in accordance with organizational standards. All default accounts and or passwords shall be removed or changed. Approvals will be required for creation, deletion or modification of any account.
- e) All access from external networks will traverse specific entry and exit points where external communication is terminated and re-established into a UNICEF controlled ICT ecosystem.
- f) Account lockout features will be used for invalid authentication attempts.
- g) Application code shall never contain any credentials.

### 3.5. Availability and Deletion

- a) Systems availability shall be set according to Service Level Agreements, to meet the Confidentiality, Integrity and Availability requirements commensurate with its classification, as noted above
- b) Any deletion of confidential / personal data must be done so that it cannot be reconstructed.

### 3.6. Cryptography

- a) The system shall have cryptographic controls in place to secure sensitive data while in transit, while at rest and while in use. At a minimum, UNICEF cryptographic standards shall be used. In cases where vendor cryptographic standards exceed published organizational standards, vendor technical controls shall prevail.
- b) Personal data shall be masked, pseudonymized or otherwise protected from unauthorized access.
- c) The service provider shall use best practice or industry standard secure data exchange protocols and keep them up to date, as per defined UNICEF standards. Outdated and / or compromised protocols shall never be used.
- d) All passwords shall be encrypted with best current practices or strong industry standards cryptographic algorithms and secure keys. The keys will be generated using strong cryptographic algorithms.
- e) Key files must be protected from unauthorized modification using an application that enforces automatic reconciliation from an authoritative source.
- f) Encryption keys shall be securely stored outside of the systems on which they are used.

### 3.7. Secure Development

- a) The system shall be engineered following the '*security by design*' principles.<sup>1</sup>
- b) The system shall be developed following the '*data protection by design and by default*' principle.<sup>2</sup>  
Hence appropriate technical and organizational measures shall be in place to implement the data protection principles and safeguard individual rights. Data protection shall be integrated in processing activities and operational practices, from the design stage throughout the solutions lifecycle.
- c) Development and tests of the system will be done with fictitious or pseudonymized information.
- d) Any source code developed specifically for the system shall undergo a security assurance testing, and business impact analysis to bring operational business to acceptable level. Risk tolerance level, shall be established by the system / solution owner.
- e) Access to program source code and associated items - such as designs, specifications, testing and validation plans - shall be strictly controlled; to prevent the introduction of unauthorized functionality.
- f) The system shall display generic error messages that do not disclose detailed information such as process logs, account or system information.
- g) Executable code will not be implemented on an operational system until evidence of conforming to the testing criteria (user approval, QA, or the equivalent) is acquired and the associated program source libraries have been updated.

### 3.8. Updating assets' inventory

- a) The assets' inventory related to UNICEF applications shall be updated, as part of the operational process, capturing all system elements, describing their business function, location / identifiers and business owner.

### 3.9. Security Operations

- a) The system shall be hardened, which means that:
  - only the services and network ports necessary for efficient operation are up and running
  - all application code is patched and kept up to date and
  - limiting the accounts and removing, changing or disabling default accounts and passwords**Note:** In order to ensure proper risk driven methodology is followed, patches shall fall into one of the following categories, which are classified by the application / system vendor.; critical, non-critical. The patching window SLA, shall be formally documented by both vendor and UNICEF's Designated Authority (D.A.).
- b) Servers and applications shall be configured to run with the minimum system authorizations necessary. The service provider shall ensure the implementation of the appropriate technical and organizational measures.

---

<sup>1</sup> As described by OWASP in [https://www.owasp.org/index.php/Security\\_by\\_Design\\_Principles](https://www.owasp.org/index.php/Security_by_Design_Principles)

<sup>2</sup> As described in article 25 of the EU general data protection regulation 2016/679 (GDPR)

- c) The system must be configured to display generic error messages that do not disclose detailed information such as process logs, account or system information.
- d) The production environment shall be separated from the test and development environments; preferably on logically and physically different systems.
- e) Development and test environment shall have the same patch level as the production environment.
- f) The production environment shall not have any development tools.
- g) Configuration/Application source code/customized work, shall be protected from unauthorized access / modification and reside in non-production environment with proper back-up / resiliency policy.
- h) The system shall have malicious code protection measures. Logs generated by malicious code protection measures shall be monitored.

### 3.10. Vulnerability Management

- a) The service provider is required to run security tests. Test will run prior to the launch of the system and periodically afterwards; with a minimum frequency of once a year.
- b) The service provider is required to report on the results of the security scans and the remediations taken. These reports will be sent to UNICEF's Chief of IT Security or the relevant focal point(s).
- c) Critical security patches shall be applied within 3 days, following established testing / change management processes.

### 3.11. Change Management

- a) Any changes to UNICEF system(s) or software shall be agreed upon between ICT and the business division / office owner of the affected system and third party.
- b) Changes to system and/or application post baseline will be documented (version / build number), along with description via a formal change management process. The service provider shall report the following information about patches, at a minimum: type, version, reason, post test results after implementation. Patches that fail testing will also be recorded and documented.
- c) The updating of the operational software, applications and program libraries will only be performed by trained and qualified administrators upon appropriate management authorization.

### 3.12. Log Management and Monitoring

- a) The system shall generate and process auditing tracks covering all actions taken on personal data, including data access only.
- b) Authentication validation activities and all changes in authorization shall be logged and securely stored, with limited access.
- c) Access to content, key information and or any modifications to operational program libraries shall be logged and restricted.
- d) Logs and events will be generated in a format that can be easily parsed and used as an input for logging process management.
- e) Integrity log checking shall be performed to ensure consistency.

- f) The system, application, as well as underlying services and or networks, shall be monitored and activities logged.

### 3.13. Security Incident Management

A security breach, shall be viewed as:

- a failure in security controls which leads to the accidental, unlawful or unauthorized access, destruction, loss or alteration of data / information that processed / stored on system
  - a failure in security controls which leads to the accidental, unlawful or unauthorized access to ICT resources, such as - but not limited to - computing resources (processing and or storage / services) and communication resources (infrastructure).
- a) Security breaches, shall immediately be communicated to UNICEF's Point of Contact.
- b) A security incident notification and escalation procedure shall be formally documented and contractually enforced between the service provider, and UNICEF's Security Operations Centre.