

Class I System

UNICEF SECURITY REQUIREMENTS

1. CATEGORIZATION

Class I systems carry the highest classification and are viewed as highly sensitive / critical UNICEF ICT assets.

System Classification	Description	Asset Rating		
		Confidentiality	Integrity	Availability
Class I	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. If the classification of the information changes during the development of the system / service or at any point during its life cycle, it shall the responsibility of the owner or their delegate to reinitiate the information / system classification process. This requirement shall be viewed as an obligatory responsibility of the system owner to ensure proper protection the system and underlying information assets, by ICTD or service provider.

2. APPLICABILITY / SCOPE

The security requirements outlined in this document shall be viewed as mandatory, to any internal or external party who is providing a solution / service to UNICEF which processes, stores, and or transmits information which may fall under types noted below and or system(s) which is linked to a critical business process.

The Class I system are classified by the ones which contains sensible information:

Personal information (Personally Identifiable Information)

In accordance with and defined by *Article 9. GDPR*, *sensitive personal information* is defined as:

- 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.

Class I also contains **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.

Class I classification cover all **UNICEF Critical business**.

Non-PII which carries a UNICEF classification of “confidential”

3. SECURITY REQUIREMENTS

3.1. General Security Requirements

- UNICEF shall reserve the right to audit the security, quality and accurateness of outsourced software development and operational maintenance of the system/application, through proper security assurance testing, and/or external security assessment.
- Solution / Service shall be located in an internal / private network with proper firewalling to protect it from “external / public” traffic.
- System (host) shall have proper end-point protection.

3.2. Identification, Authentication and Authorization

- The service / solution providers 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.
- The service providers shall centrally manage the user account using federated identities and whenever it is possible they shall integrate their solution with the UNICEF Identity Management system. UNICEF will provide all the required information to the Application / Solutions service provider. The credentials will use robust algorithms and they will be renewed frequently. The allocation of authenticators will be controlled through a formal management process.
- Multi-factor authentication will be used for privileged accounts and user access outside of UNICEF trusted network.
- All the user and system accounts shall be disabled after defined period of inactivity and shall be eliminated in the case of standard accounts and passwords. Approvals will be required for creation, deletion or modification of any information system account.
- All user/system access from external networks, etc. will traverse specific entry and exit points where external communication is terminated and re- established into “trusted network”.

3.3. Cryptography

- System shall have cryptographic controls in place to secure sensitive data while in transit and while at rest.

- Secure sensitive, as per GDPR, data while in use shall be masked, pseudonymized or otherwise protected for being accessed / viewed.
- The service provider shall use secure data exchange protocols and keep them up to date, as per defined UNICEF standards. For example, the minimum acceptable for network protocol HTTPS is TLS v.1.1 or wherever possible TLS v.1.2 shall be used. TLS shall be implemented with HSTS (HTTP Strict Transport Security).
- All passwords shall be encrypted with robust cryptographic algorithms and secure keys. The keys will be generated using strong cryptographic algorithms.
- Key files must be protected from unauthorized modification using an application that enforces automatic reconciliation from an authoritative source.
- Whenever possible, encryption keys shall be securely stored outside of the systems on which they are used. For example, by using HSM (Hardware Security Module), a USB token or any other secure key storage.

3.4. Secure Development

- The service solution provider shall apply the security by design principle and use a recognized development methodology which takes into account the security aspects during the whole life cycle (analysis, design, development, implementation, testing, deployment and maintenance phases) which applies a specific treatment to the data used for tests and allows for the inspection of the source code.
- The service solution provider shall develop data protection by design and by default, following the best practices under the regulation of the GDPR, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing.
- Servers and applications shall be configured to perform with the minimum system authorizations necessary following the “minimum functionality” rule and the security by default. The service / solution provider shall implement appropriate technical and organizational measures for ensuring it.
- The development of applications will be carried out using a different system, which is separate from production.
 - No development tools may be installed on a production eco-system.
 - Development System / Application environment shall be as the same patch level as the production environment.
 - Testing of the information systems will not be done using real data.
- 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.

- Account lockout features will be used for invalid authentication attempts.
- No user ID and or password shall be embedded in the application code.
- The system/application design shall generate and process auditing tracks.
- 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.

3.5. Updating assets' inventory

- The assets' inventory related to UNICEF applications shall be updated, capturing all system elements (class, location, O/S, etc. in servers, networks, portables,...), describing their nature, and identifying their owners.

3.6. Security Operations

- Servers and applications/configurations shall be hardened, focus on keeping the security patches updated, using only secure ports and services/applications which are strictly necessary and limiting the hosts and accounts. Specially, to configure securely the administrator and privilege users accounts, and the protection of any sensitive information.
- Generic error messages shall be displayed without disclosing detailed and or information and or enumeration account or system information.
- 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.
- It shall be implemented and monitored malicious code protection.

3.7. Vulnerability Management

- The service / solution provider is required to run security tests prior to the launch of the site and periodically with a minimum frequency of once a year.
- The service / solution provider is required to provide written documentation reporting on the results of the security scans and the remediation solutions taken. Such reports will be sent to UNICEF's Chief of IT Security or the relevant focal point (s).
- Critical security patches shall be applied within 3 days, following established testing / change management processes.

3.8. Change Management

- 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.
- 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.

- The updating of the operational software, applications and program libraries will only be performed by trained and qualified administrators upon appropriate management authorization.

3.9. Availability

- Systems availability shall be set according to Service Level Agreements.

3.10. Log Management

- Authentication, validation activities and all privilege changes shall be logged and securely stored, with limited access.
- Access to content, key information and updates/modifications to operational program libraries shall be logged and restricted.
- Logs/events will be generated in a format that can be easily parsed and used as an input for logging process management, including who, when, location and user agent type, among others.
- Integrity log checking shall be performed to ensure consistency.

3.11. Security Incident Management

- The security incident notification / escalation shall be clearly established between the service provider, and UNICEF's Security Operations Centre.
- In cases where solution is managed by a third party, the service provider shall share and where applicable interconnect with UNICEF's Security Incident Management framework.
- System breaches which affect confidential data, shall be communicated to UNICEF P.O.C immediately.
 - o Breach of personal data, in the context of this document, shall be viewed as a failure in or compromise of security controls that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal / confidential data.

3.12. Continuity and monitoring Management

- Systems/application, as well as underlying services and or networks, shall have the proper controls to meet UNICEF system classification.