**Security Requirements**

**3.1) General Security Requirements**

1. UNICEF shall reserve the right to assess the quality and accurateness of outsourced software development and operational maintenance of the system / application; whether it is through security assurance testing or through external security assessment.

Comment: Agile Kanban has been used as the process for SDLC of the application, where a QA team was present. Each and every feature has been passed through the QA process where quality and accurateness was checked. Moreover the app was accessible to the client from day 1 to boost-up overall QA and feedbacks.

1. 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.

Comment**:** Our api service runs in locally on a linux server, which cannot accessible from outside of the server. Web servers (we use nginx) use a reverse proxy and access our api. By doing this our api service can only be accessible via our hosted web application.

1. 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).

Comment**:** We host sour application on Linux server; Linux server is more secure against malicious code. We also configure firewall on hosted server.

**3.2) Validation of Security Controls**

1. 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

Comment: Attached all the testing documents.

**3.3) Compliance & Certifications**

1. 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.

Comment: We may host our application on various like,

AWS: [ISO Certified (amazon.com)](https://aws.amazon.com/compliance/iso-certified/) AWS has certification for compliance with ISO/IEC 27001:2013, 27017:2015, 27018:2019, and ISO/IEC 9001:2015 and CSA STAR CCM v3.0.1

Azure: [Azure is now certified for the ISO/IEC 27701 privacy standard | Azure Blog and Updates | Microsoft Azure](https://azure.microsoft.com/en-us/blog/azure-is-now-certified-for-the-iso-iec-27701-privacy-standard/)

Digital ocean: [Trust Platform - Certifications (digitalocean.com)](https://www.digitalocean.com/trust/certification-reports/)DigitalOcean is AICPA SOC 2 Type II certified

**3.4) Identification, Authentication and Authorization**

1. 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.

Comment**:** User will get permission set according to his role. These permission set can be controlled.

1. 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.

Comment: As per requirement of the application, federated identities/identity management system is not required for UEMIS. Whereas ASP.NET identity system has been applied which is extensible and can be useful to implement if its required.As our authentication is password based, we maintain a strong password policy. Admin user can create new user.

1. Multi-factor authentication will be used for:

* privileged accounts and
* User access outside of UNICEF trusted network.

Comment: This is not applicable on our application.

1. 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.

Comment: New requirement.

1. 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.

Comment: Access from external network is not allowed on our application.

1. Account lockout features will be used for invalid authentication attempts.

Comment: Already implemented on our application.

1. Application code shall never contain any credentials.

Comment: Application codebase don’t preserve any credentials.

**3.5) Availability and Deletion**

1. 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

Comment: Depends on platform, where we will host Application

1. Any deletion of confidential / personal data must be done so that it cannot be reconstructed.

Comment: We already provide delete facility on beneficiary and facility data

**3.6) Cryptography**

1. 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.

Comment: We use SSL certificate, it provide security while transit data over network.

1. Personal data shall be masked, pseudonymized or otherwise protected from unauthorized access.

Comment: We protect data from unauthorized access.

1. 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.

Comment: We use https protocol, which is industry standard secure data exchange protocol.

1. 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.

Comment: We use Asp.net identity, which used industrial standard cryptographic algorithm.

1. Key files must be protected from unauthorized modification using an application that enforces automatic reconciliation from an authoritative source.

Comment: We will follow as instructed.

1. Encryption keys shall be securely stored outside of the systems on which they are used.

Comment: Encryption key is stored outside the system.

**3.7) Secure Development**

1. The system shall be engineered following the ‘security by design’ principles.1

Comment: We follow security by design principle.

1. The system shall be develop following the ‘data protection by design and by default’ principle. 2 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.

Comment: We follow data protection by design and by default principle.

1. Development and tests of the system will be done with fictitious or pseudonymized information.

Comment: From the beginning of the development, when we complete any feature, QA team test with fictitious information.

1. 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 the established by the system / solution owner.

Comment: From the beginning of the development, we maintain this process

1. 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.

Comment: From the beginning of the development, we go through designs, specifications, testing each and every feature.

1. The system shall display generic error messages that do not disclose detailed information such as process logs, account or system information.

Comment: Our system shows customized error message. System information is not exposed to end user.

1. 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.

Comment: Not applicable on our case

**3.8) Updating assets’ inventory**

1. 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.

Comment: We will follow as instructed

**3.9) Security Operations**

1. 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, noncritical. The patching window SLA, shall be formally documented by both vendor and UNICEF’s Designated Authority (D.A.).

Comment: We will follow as instructed

1. 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.

Comment: We will follow as instructed

1. The system must be configured to display generic error messages that do not disclose detailed information such as process logs, account or system information.

Comment: Our system display generic error message

1. The production environment shall be separated from the test and development environments; preferably on logically and physically different systems.

Comment: Chose any hosting provider to separate production server.

1. Development and test environment shall have the same patch level as the production environment.

Comment: We will follow as instructed

1. The production environment shall not have any development tools.

Comment: Production environment does not contain any development tools

1. 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.

Comment: We use git as our source control and keep all our code on own server.

1. The system shall have malicious code protection measures. Logs generated by malicious code protection measures shall be monitored.

Comment: As we host our application on Linux, server would not be affected by malicious code

**3.10) Vulnerability Management**

1. 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.

Comment: Security test is attached with this document.

1. The service provider is required to report on the results of the security scans and the remediation’s taken. These reports will be sent to UNICEF’s Chief of IT Security or the relevant focal point(s).

Comment: Security test is attached with this document.

1. Critical security patches shall be applied within 3 days, following established testing / change management processes

Comment: We will follow as instructed

**3.11) Change Management**

1. 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.

Comment: We will follow as instructed

1. 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.

Comment: We will follow as instructed

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

Comment: We will follow as instructed

**3.12) Log Management and Monitoring**

1. The system shall generate and process auditing tracks covering all actions taken on personal data, including data access only.

Comment: To audit personal data, we add additional fields CreatedBy, UpdateBy, CreatedDate, UpdatedDate on every row.

1. Authentication validation activities and all changes in authorization shall be logged and securely stored, with limited access.

Comment: All changes in authorization is logged.

1. Access to content, key information and or any modifications to operational program libraries shall be logged and restricted.

Comment: Any modification to operational program libraries will be logged.

1. Logs and events will be generated in a format that can be easily parsed and used as an input for logging process management.

Comment: All stored logs in JSON format.

1. Integrity log checking shall be performed to ensure consistency.

Comment: All kind of data changed on the system are tracked.

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

Comment: Need to configure hosted environment

**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).

1. Security breaches shall immediately be communicated to UNICEF’s Point of Contact.
2. A security incident notification and escalation procedure shall be formally documented and contractually enforced between the service provider, and UNICEF’s Security Operations Centre

Comment: We will follow as suggested.

s