System Security Requirements

Due to the sensitivity of subject data, access to the developed system and its different components, identification, authentication and authorization shall consider the following security aspects:

a) The company will 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) 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 trusted network, if requested.

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.

e) Approvals will be required for creation, deletion or modification of any account.

f) All access from external networks will traverse specific entry and exit points where external communication is terminated and re-established into a the partner controlled ICT ecosystem.

f) Account lockout features will be used for invalid authentication attempts.

g) Application code shall never contain any credentials.

Cryptography

As the system being developed handles sensitive data, rigid protection controls against unauthorized access need to be satisfied:

a) Company should ensure that Cryptographic controls are in place to secure sensitive data while in transit, while at rest and while in use. In cases where vendor cryptographic standards (like in the case of database management systems) cover such security aspects, then they can be sufficient

b) Personal data of students and teachers, as well as any sensitive data subject to this contract, shall be masked, pseudonymized or otherwise protected from unauthorized access.

c) The company 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 Outdated and / or compromised protocols shall never be used.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 features in the 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.

Secure Development

Due to the nature of the system being developed, it has to be protected from vulnerabilities to ensuring the confidentiality, integrity, and availability of the system and data. The following need to be considered:

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

b) The system shall be developed following the ‘data protection by design and by default’ principle. Hence appropriate technical measures shall be in place to implement the internationally recognized data protection principles and safeguard individual rights. Those principles need to be integrated in processing activities and operational practices, from the design stage throughout the solutions lifecycle.

c) Development and tests of the system will need to 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 the 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.

Security Operations

a) The production environment shall be separated from the test and development environments.

b) The production environment shall be separated from the test and development environments.

c) Development and test environment shall have the same patch level as the production environments.

f) The production environment shall not have any development tools.

d) 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.

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

Vulnerability Management

a) The company 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 company 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 immediately, following established testing / change management processes.

Change Management

a) Any changes to the system shall be agreed upon by partner

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 company 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.

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 shall be monitored and activities logged.

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) As applicable, Security breaches, shall immediately be communicated to partner

b) A security incident notification and escalation procedure shall be formally documented and contractually enforced between the service provider, and partner.

Auditing

Client has the right to audit and check live applicability of all security requirements above.