Req No	**Security Requirement**
7.1	*The supplier staff developing the software are contractually required to be trained in UNHCR's secAll supplier staff, contractors and UNHCR workforce directly developing the software are trained in UNHCR's security requirements in mandatory UNHCR training courses or approved materially equivalent trainingurity requirements as laid down in mandatory UNHCR training courses*
7.2	*All supplier staff and contractors developing the software have signed confidentiality agreements.*
8.1	An Information Asset Classification has been conducted on the software and information it supports (defining required Confidentiality and Integrity levels)
9.10	Users are allocated a personal and unique User ID to ensure traceability and accountability. Sharing of User IDs is not permitted.
9.11	The allocation of Authentication Information (such as passwords, tokens) to Authorized Users is controlled through a formal, secure process.
9.12	Formal "Joiner, mover, leaver" controls are followed for all access via all accounts. It includes authorisation in writing by the Supervisor / Responsible Manager of the User or their delegate.
9.15	The need for all privileged accounts (including system, service and shared accounts) is reviewed and recertified by the System Owner or delegate at least 6-monthly.
9.17	Privileged access rights are immediately removed when no longer required
9.18	Privileged Access Rights are assigned to a different account (the Privileged Account) from the one used for regular business activities.
9.20	The application complies with UNHCR mandatory password content requirements.
9.21	The application complies with UNHCR mandatory password expiry requirements.
9.24	Passwords and secrets for special accounts (e.g., Shared, Service, Local, Built-In, and Functional Privileged) accounts are kept in a secure password vault with strictly controlled and limited access.
9.30	Access to the application is controlled by a secure log-on procedure
9.32	Privileged accounts are not allowed multiple, concurrent logins/sessions
9.33	The software automatically locks users out after 15 minutes of inactivity (if technically possible)
9.38	Multi-factor authentication (MFA) is required for all privileged access to the system (if technically possible)
9.40	The Application locks out user accounts (at least temporarily) if a maximum number of failed authentication attempts is exceeded
9.43	The "Login" facility for shared accounts is disabled.
9.53	All changes to account privileges and access rights for user accounts are recorded in a log file.
10.01	Platform storage is encrypted at rest (e.g. with BitLocker in Windows 10).
10.02	No sensitive information (e.g. credentials, private keys, passwords) is stored in clear text (documents, files, etc) or readable code (scripts, etc).
10.03	Infrastructure Backups are encrypted.
10.0	Encryption in transit is enforced for the application with at least Transport Layer Security (TLS) 1.2
12.17	The application support organisation contractually has appropriate use rules for the platform and they are effective (e.g. no unwanted software, games, browsers etc).
12.50	The production (PROD) environment is not used for Development and testing nor development tools are installed on it.
13.01	The platform hosting the application has an Intrusion Detection System or Intrusion Prevention System (IDS/IPS) running and its alerts are analysed in real time
13.02	The application software is protected by a managed network firewall or security gateway
13.04	Internet ports are restricted: Only http (port 80) (redirects) and https (port 443) are open on the Internet.
13.05	Application is behind a Web Application Firewall (WAF)
13.07	The network ranges able to communicate with the software product are minimised to only those necessary for the software's performance.
13.10	If the application has an API for data exports, then it has controls to both limit volumes and log all exports
14.03	The source code repository is secured from external reading or writing.
14.06	Application developers have been trained in secure coding practices.
14.07	Real personal data is not used for development and testing.
14.08	The applications must not display error or system messages that reveal information about the underlying configuration.
14.09	The software product has a contracted or documented application support team.
14.10	If the application is multi-tier and internet exposed, the database runs on a different machine to the web server.
14.11	The application (including platform and middleware) is penetration tested by UNHCR or an independent party before go-live
15.09	Supplier and their staff delivering services within UNHCR managed environments are contractually required to comply to UNHCR security policies.
15.10	Organisations delivering operational services with security requirements report out on their compliance with these requirements (ideally under SLAs) at least every 6 months.
16.02	The hosting and support contract requires the supplier to report to UNHCR any actual or probable security or data protection incident affecting UNHCR data or services within 48 hours
16.03	Security incidents for issues inside the application (e.g. an unauthorised elevation of privileges) are reported to UNHCR
18.01	The hosting entity respects UN Privileges & Immunities from national law enforcement subpoenas and all other national law including lawful intercepts and notifies UNHCR of any such requests
18.02	Hosting is only in countries party to the 1946 Convention on the Privileges and Immunities of the United Nations.
18.03	The support entity contractually respects UN Privileges & Immunities (insofar as they are working for UNHCR, GDPR and other national laws do not apply).
18.04	All software used is current, licensed and supported or Open Source (no cracked, "freeware" or obsolete products). Any Open Source Software used (in the scope of the service) must be formally approved by ARB.
18.06	All Personally Identifiable Information is protected in accordance with the UN Principles (https://unsceb.org/privacy-principles)
18.07	(PoC data only) Data Sharing Agreements are signed and current for all application integrations with partner and supplier organisations
18.09	The application has a logon screen warniThe application has a logon screen warning banner which gives notice that the information system must only be accessed by authorized users, requires users to comply to UNHCR policies and accepts that they are being monitored.ng banner which gives notice that the information system must only be accessed by authorized users, requires users to comply to UNHCR policies and accepts that they are being monitored.