

Cybersecurity RFP Recommendations

The content below must be included in all IT related RFP in the non-functional requirements in addition to other IT requirements.

For IT-related procurement activities, the successful bidder will meet the following minimum mandatory cybersecurity recommendations where applicable. Please check the box next to each recommendation to indicate your compliance. Please, provide reasonable evidence in support to your statement of compliance (i.e. certificates, product documentation, audit reports).

1. The IT solution must be ISO certified (27000 family).
2. For sensitive data, data at rest must be encrypted by the IT solution. Industry best practice cryptographic algorithms must be enforced by the IT solution.
3. For sensitive data, secure data destruction processes must be in place. Vendor must provide evidence of secure data destruction.
4. Data in transit and in use must be encrypted. Industry best practice cryptographic algorithms must be enforced.
5. Data must be encrypted on all removable media used by the IT solution. (I.e., USB memory stick, external hard drives).
6. When authentication is required, all systems or applications should integrate with the WHO Single Sign On authentication scheme (SAML; OpenID Connect).
7. Multi-factor Authentication (MFA) must be enforced.
8. A system or an application must support Role-Based Access Control (RBAC).
9. A system or an application in production must use individual accounts. All account sharing is strictly prohibited.
10. For non-SaaS solutions, a system or an application in production must have logging capabilities as defined in ISO 27001 annex A.12.4
11. A solution should have all levels of technical support for security controls.
12. A vendor must allow WHO to perform periodic vulnerability scans and penetration testing when required.
13. A hosting provider should produce evidence that security controls are in place (i.e. network and web application firewalls; proxy; etc.) including evidence of recent security audits and security penetration tests.
14. A solution must include non-repudiation methods and fraud prevention when financial transactions are executed. This includes MFA, audit trail, digital signatures, challenge-response OTP tokens, and other security controls.
15. A vendor must have a technical change and configuration management process in place that is compliant with ITIL.
16. A vendor must have secure software development processes in place (for example: OWASP Secure Coding Practices).
17. A vendor must provide technical support to the Project Team during the Risk Assessment conducted by the WHO Cybersecurity Team.
18. A vendor must ensure they have backup and restore processes in place. It is recommended a Disaster Recovery Plan and periodic testing is performed.

19. The IT solution must have a governance mechanism to ensure confidential and sensitive data (to be determined through a separate confidentiality undertaking) is sufficiently protected in accordance with the highest standards, and in compliance with all applicable laws, ordinances, rules and regulations (including the [UN Principles on Personal Data Protection and Privacy](#)).