Website Technical Requirements Checklist

#	Functionality
1.	**Website Technical Requirements**
1.1	**Integration Requirements**
1.1.1	Perform integration of proposed solution with data sources namely government e-tendering portal (https://etendering.tenderboard.gov.om) in order to retrieve tenders information directly from that website.
1.1.2	Link to the Ministry of Labour (MOL) job application
1.2	**Security**
1.2.1	• The pages of the website that deal with critical data should only be accessible via a secured link.
1.2.2	• The website communications must be secured using protocols such as HTTPS, SSL etc. The security measurement should be up to the ITA requirements.
1.2.3	There should be regular security assessments and major yearly checks for the website. The website should also have a security and risk assessment done before launching
1.2.4	The following security coding guidelines must be followed: • Do not hard code username/passwords in logs and application code • Do not maintain plain text passwords in configuration files and database • Do not use insecure protocols to exchange data with external parties • Prevent any information leakage through error messages • Shield the system errors and debug information from the end-user which might reveal the technology and product used • Session should expire when no activity or when maximum period has elapsed • Do not put sensitive data in URL parameters • Log all access to sensitive data • Do not rely on client side input validation, always validate input • Check input for cross site scripting (XSS) • Prevent Cross Site Scripting • Users should not use application credentials to access any system or any database • Denial of Service (DOS) attacks and other security issues should be taken care of. All forms/user entry screens should have CAPTCHA or other similar mechanisms to counter any attacks.

1.2.5	Test and quality benchmarks shall be established for all components of the Solution. These benchmarks shall assess compliance with the agreed design, as well as any special requirements. They shall cover solution operations and performance, reliability, data integrity, security, standardization, OS/browser independence, and
1.2.6	MTCIT's Information Security Division or a 3rd party organization will carry out a penetration testing and vendors are expected to fix any gaps identified as a result.
1.2.7	The database layers of the implemented solutions should employ user input filtration, user input strong typing, and other security features to prevent SQL injection threats and vulnerabilities. Avoid any dynamic SQL in the implementation which is prone to SQL injection attacks.