SDLC Security **minimum** requirements.

The following are baseline security requirements that are set to help developer teams and architects deliver a secure system to MoDEE.

These requirements should be fulfilled in addition to:

1- the requirements of previous contracts; i.e. the RFP and Information Security component, and

2- All the remediation recommendations resulting from the penetration tests.

#	Item
OWASP Top 10, do all the required to protect the e-services against:	
1.	The delivered system should be protected and secured against OWASP Top 10 1. 1. Broken Access Control 2. 2. Cryptographic Failure 3. 3. Injection 4. 4. Insecure Design 5. 5. Security Misconfiguration 6. 6. Vulnerable and Outdated Components 7. 7. Identification and Authentication Failure 8. 8. Software and Data Integrity Failure 9. 9. Security Logging and Monitoring Features 10. 10 Server-Side Request Forgery
2.	The system should pass the penetration test by MoDEE
HTTPS protocol	
3.	Use HTTPS protocol on login and sensitive data transfer pages
Software Updates	
4.	Make sure that all SW components used in development are updated and supported by security patches.
5.	Make sure that all used platforms on servers and back-end officers are up to date and supported by security patches.
6.	Use the latest version of communication protocols; secure versions
Restrict File Uploads	
7.	Validate uploaded file types on the server side

8.	Store files uploaded by clients in separate folders and databases
9.	Restrict types of uploaded files
10.	Ban double extension files
11.	Use antimalware detection like Sandboxing technology on the app and web servers.
Using Captcha	
12.	Use secure CAPTCHA that can protect against bots.
13.	Passing reCAPTCHA is mandatory before submission
14.	Can the CAPTCHA use can collect as minimum user data as possible?
15.	Collect the user's consent before any data collection
When migrating data, security should be a top priority to prevent data breaches, loss, and unauthorized access. Here are the key security requirements to consider:	
16.	Data Encryption(both in transit and at rest)
17.	Access Control(Least Privilege, MFA and Role-based Access Control)
18.	Data Integrity: - Checksums/Hashes: Use checksums or cryptographic hashes to verify that the data has not been tampered with or corrupted during the transfer. - Validation Procedures: Implement validation steps, including data validation and consistency checks, to ensure no data loss or modification occurs during migration.
19.	Backup and Recovery(Pre-Migration Backups, and Post-Migration Backups)
20.	Data Masking and Anonymization: Mask or anonymize sensitive data during the migration process,
21.	Disposal of Old Data: After migration, securely delete or wipe the original data to prevent any unauthorized access once it's no longer needed.
Users Passwords	
22.	Use a strong password policy and provide strong password setting guides, For example, 8 4 Rule.
23.	Store passwords as encrypted hashed values?
24.	Lock the account locked after three failed logins
Viruses and Malware	
25.	Use antimalware on the production, Staging, and Development environment; the developer should report to the PM or system team if the antimalware does not exist or is not updated.
Adjust Default Settings	
26.	Are account configuration default settings changed for both the hosting environment and content management system
Error Messages	
27.	The error message displays information that the visitor needs, without revealing the structure of any component of the website.
28.	Detailed errors kept in the server log?
Secure APIs	
29.	Do APIs use HTTPS?

30.	Use token-based API authentication like OAuth 2.0
31.	Tokens should have an expiration time
32.	Configure limit rate on API. i.e. have a limitation on how many times the client is allowed to call it?
33.	Validate API parameters
34.	IDs should be opaque and globally unique. For example, rather than using the ID “1002 “and “1003 “use “r5t844fsg6fssf2vfrb9bd8”.
35.	Add a timestamp to the Request, so it only accepts requests within a reasonable timeframe.
36.	Filter the API-returned data on the backend side.
37.	Prevent request manipulation
38.	Publishing Swagger files is not allowed
User Authentication and Authorization	
39.	Use MFA authentication
40.	Use SANAD authentication services whenever possible Use LDAP protocol to validate admins on the admin portal
OTP requirements	
41.	An expiry time should be added to the OTP value so that the value will expire after a certain time and the value of the expiry time should not exceed 5 minutes.
42.	A lockout feature should be implemented in case the user has inserted too many wrong OTP values in the reset password functionality.
43.	The OTP value should not be used more than once.
44.	OTP request should only hold user ID, phone number or email address should be fetched from the DB.
45.	OTP has to be 6 digits.
5.11. Security Logging and Auditing	
46.	Are the website security transactions audited for adequate time?
47.	Are logs securely transmitted to a preferably remote system for analysis, detection, alerting, and escalation?
48.	All system components should be time-synchronized.
GSB portal: Regarding granting you permissions on the GSB environment, please be informed that the systems accessing the data through the interconnectivity system must adhere to the following requirements:	
49.	They must be free of any security vulnerabilities, verified by conducting penetration testing and vulnerability assessments.
50.	They must implement a user authentication mechanism for internal users using a username, password, and OTP.
51.	They must maintain logs for all login attempts and queries, with a mechanism to prevent modification of these logs.
52.	Access to the system must be restricted to pre-approved IP addresses only.

53.	There must be an agreed-upon policy from all parties for querying, and the data team, and the Information Security Directorate, should be informed.
54.	The system must not be published outside the organization under any circumstances.
55.	Conduct a penetration test with the Ministry's Information Security Directorate after completing the development.
General	
56.	Design 3-Tier Architecture
57.	Use SANAD registration and log in wherever possible
58.	Deliver a list of servers for both production and staging environments. The document should describe the functionality of these servers and should define all the ports needed on each machine in the 3 layers and the IP addresses it communicates with (to configure host-based FW)
59.	At least 2 inputs (3 inputs for CSPD) for Any data will be returned through API
60.	Web servers' configuration files should not hold any application data.
61.	The system should be protected by the WAF.
62.	Hard-coded credentials are not allowed
63.	Do not publish Admin pages; these should only be used inside SGN
64.	All back-office employees should have OTP
65.	VPN: only approved accessing the private cloud access from the Gov-entity only. Then Gov-entity provide an external party a VPN protected by MFA. any other cases need exptions and security team approval.
66.	• Assure micro-segmentation is in place for all VM's • Antivirus in place on all VMs
67.	• The system should be protected by the WAF • X-Forwarded IP Address should be configured
68.	Define all data used with its security level as defined in the Data Classification policy (embedded in (سياسة استخدام موارد تكنولوجيا المعلومات) and apply security controls as per the policy
69.	Comply to the policies: - سياسة استخدام موارد تكنولوجيا المعلومات - سياسة أمن الموردين - سياسة أمن المعلومات العامة