

Annex 5.8 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 <ol style="list-style-type: none">1. <u>1. Broken Access Control</u>2. <u>2. Cryptographic Failure</u>3. <u>3. Injection</u>4. <u>4. Insecure Design</u>5. <u>5. Security Misconfiguration</u>6. <u>6. Vulnerable and Outdated Components</u>7. <u>7. Identification and Authentication Failure</u>8. <u>8. Software and Data Integrity Failure++++</u>9. <u>9. Security Logging and Monitoring Features</u>10. <u>10 Server-Side Request Forgery</u> |
| 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. |

Minimum Baseline Security Standard

SDLC V1.0

| | |
|--------------------------------|--|
| 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 CAPTCHA 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 |
| Users Passwords | |
| 16. | Use a strong password policy and provide strong password setting guides, For example, 8 4 Rule. |
| 17. | Store passwords as encrypted hashed values? |
| 18. | Lock the account locked after three failed logins |
| Viruses and Malware | |
| 19. | 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 | |
| 20. | Are account configuration default settings changed for both the hosting environment and content management system |
| Error Messages | |
| 21. | The error message displays information that the visitor needs, without revealing the structure of any component of the website. |
| 22. | Detailed errors kept in the server log? |
| Secure APIs | |
| 23. | Do APIs use HTTPS? |
| 24. | Use token-based API authentication like OAuth 2.0 |
| 25. | Tokens should have an expiration time |
| 26. | Configure limit rate on API. i.e. have a limitation on how many times the client is allowed to call it? |
| 27. | Validate API parameters |
| 28. | IDs should be opaque and globally unique. For example, rather than using the ID "1002 "and "1003 "use "r5t844fsg6fssf2vfrb9bd8". |
| 29. | Add a timestamp to the Request, so it only accepts requests within a reasonable timeframe. |
| 30. | Filter the API-returned data on the backend side. |

Minimum Baseline Security Standard

SDLC V1.0

| | |
|--|---|
| 31. | Prevent request manipulation |
| 32. | Publishing Swagger files is not allowed |
| User Authentication and Authorization | |
| 33. | Use MFA authentication |
| 34. | Use SANAD authentication services whenever possible Use LDAP protocol to validate admins on the admin portal |
| OTP requirements | |
| 35. | 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. |
| 36. | A lockout feature should be implemented in case the user has inserted too many wrong OTP values in the reset password functionality. |
| 37. | The OTP value should not be used more than once. |
| 38. | OTP request should only hold user ID, phone number or email address should be fetched from the DB. |
| 5.11. Security Logging and Auditing | |
| 39. | Are the website security transactions audited for adequate time? |
| 40. | Are logs securely transmitted to a preferably remote system for analysis, detection, alerting, and escalation? |
| 41. | All system components should be time-synchronized. |
| General | |
| 42. | Design 3-Tier Architecture |
| 43. | Use SANAD registration and log in wherever possible |
| 44. | 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) |
| 45. | Web servers' configuration files should not hold any application data. |
| 46. | The system should be protected by the WAF. |
| 47. | Hard-coded credentials are not allowed |
| 48. | Do not publish Admin pages; these should only be used inside SGN |
| 49. | All back-office employees should have OTP |
| 50. | <ul style="list-style-type: none">Assure micro-segmentation is in place for all VM'sAntivirus in place on all VMs |
| 51. | <ul style="list-style-type: none">The system should be protected by the WAFX-Forwarded IP Address should be configured |
| 52. | 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 |
| 53. | Comply to the policies: - سياسة استخدام موارد تكنولوجيا المعلومات |

Minimum Baseline Security Standard

SDLC V1.0

| | |
|--|--|
| | <ul style="list-style-type: none">- <u>سياسة أمن الموردين</u>- <u>سياسة أمن المعلومات العامة</u>- <u>MODEE minimum security baseline</u> |
|--|--|

- VPN connection is prohibited and if there is a need, the access should provided from the entities only with multi-factor protected and the VPN connection must be from Jordan.