

4.14.1 Secure Software Development Policy

Contents

1. Definitions	2
2. Purpose	2
3. Scope	2
4. Policy	2
5. Non-compliance	3
6. References	4

Version	Adjustment Date	Approved By	Approval Date
2.1	18/12/2025	Saud Alsulami	2/1/2025



1. Definitions

For purposes of this "Secure Software Development Policy" the following definitions apply:

- **Secure Coding Standards:** a set of guidelines, practices, and rules that developers must follow to write code that is resistant to security vulnerabilities and threats.
- **Access Rights Segregation:** the practice of separating and controlling access permissions to different environments (e.g., development, testing, production) to prevent unauthorized access and minimize the risk of data breaches.
- **Code Review:** a systematic examination of software source code by peers or security experts to identify and remediate security vulnerabilities, coding errors, and adherence to coding standards.
- **Anonymization:** Anonymization is the process of removing or obfuscating personally identifiable information (PII) or sensitive data from datasets used in development and testing environments to protect privacy and confidentiality.

2. Purpose

The purpose of the Secure Software Development Policy is to establish guidelines and requirements for the development of software applications that prioritize security, safeguard sensitive data, and align with Taqnyat's cybersecurity objectives.

3. Scope

The scope of the Secure Software Development Policy encompasses all software development activities within the organization and emphasizes secure coding practices, access rights management, and compliance testing to enhance software security and reduce cybersecurity risks.

4. Policy

- 4.1. Software developers must adhere to approved secure coding standards and practices throughout the software development lifecycle. This includes:
- Utilizing secure coding guidelines and best practices to mitigate common vulnerabilities.
 - Employing approved libraries and APIs with known security controls.
 - Regularly updating and patching software components to address security vulnerabilities.
 - Conducting code reviews to identify and remediate security issues.

- 4.2. Access rights to different software development and testing environments shall be segregated and allocated based on the principle of least privilege. This includes:
 - Restricting access to development, testing, and production environments to authorized personnel only.
 - Implementing access controls to ensure that developers have access only to the resources necessary for their roles.
 - Ensuring that sensitive production data is not used in development or testing environments unless anonymized or obfuscated to protect confidentiality.
- 4.3. Software developed within the organization must undergo rigorous testing to verify compliance with cybersecurity requirements. This includes:
 - Conducting vulnerability assessments and security testing to identify and remediate security weaknesses.
 - Verifying that the software aligns with the organization's security policies and standards.
 - Ensuring that data input validation, authentication, authorization, and encryption mechanisms are implemented correctly.
 - Conducting penetration testing and code reviews to uncover potential vulnerabilities.
 - Regularly monitoring and assessing the security posture of software applications throughout their lifecycle.
- 4.4. The code is uploaded to the staging environment by the technical advisor, who ensures there are no errors or issues with the code. The code is then scanned on SonarQube.
- 4.5. After verifying the code's functionality on the staging environment, the technical advisor uploads the code to the production environment.
- 4.6. The code should be uploaded to the production environment using a secure and encrypted connection to ensure a safe transfer, such as using a VPN.
- 4.7. Any security incidents discovered in the development life cycle must be handled as per Incident Management policy.

5. Non-compliance

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment, and related civil or criminal penalties.



6. References

- ISO 27002
- National Cybersecurity Authority's (NCA) ECC standards
- SANS
- NIST



Internal Use Only