

Secure Development Policy

Policy Owner: Dotan Simha

Effective Date: Aug 28, 2024

Purpose

To ensure that information security is designed and implemented within the development lifecycle for applications and information systems.

Scope

All Software Products Guilda Ltd. applications and information systems that are business critical and/or process, store, or transmit Confidential data. This policy applies to all internal and external engineers and developers of Software Products Guilda Ltd. software and infrastructure.

General requirements

This policy describes the rules for the acquisition and development of software and systems that shall be applied to developments within the Software Products Guilda Ltd. organization.

System change control procedures

Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures. Change control procedures and requirements are described in the Software Products Guilda Ltd. Operations Security Policy.

Significant code changes must be reviewed and approved by Dotan Simha before being merged into any production branch in accordance with the process found here: https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/

Change control procedures shall ensure that development, testing and deployment of changes shall not be performed by a single individual without approval and oversight.

Software version control

All Software Products Guilda Ltd. software is version controlled and synced between contributors (developers). Access to the central repository is restricted based on an employee's role. All code is written, tested, and saved in a local repository before being synced to the origin repository.

Technical review of applications after operating platform changes

When operating platforms are changed, business critical applications shall be reviewed and tested to ensure that there is no adverse impact on organizational operations or security.

Restrictions on changes to software packages

Modifications to third-party business application packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.

Secure system engineering principles

Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.

At a minimum, the following secure-by-design and privacy-by-design principles shall be applied:

Secure-by-design principles:

1. Minimize attack surface area
2. Establish secure defaults
3. The principle of Least privilege
4. The principle of defense in depth
5. Fail securely
6. Don't trust services
7. Separation of duties
8. Avoid security by obscurity
9. Keep security simple
10. Fix security issues correctly

Privacy-by-design principles:

1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality - Positive-Sum, not Zero-Sum
5. End-to-End Security - Full Lifecycle Protection
6. Visibility and Transparency - Keep it Open
7. Respect for User Privacy - Keep it User-Centric

Engineering documentation and technical references can be found in the process here: https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/

Software developers are expected to adhere to Software Products Guilda Ltd.'s coding standards throughout the development cycle, including standards for quality, commenting, and security.

Secure development environment

Software Products Guilda Ltd. shall establish and appropriately protect environments for system development and integration efforts that cover the entire system development lifecycle. The following environments shall be logically or physically segregated:

- Production
- Test / Staging
- Development

Outsourced development

Software Products Guilda Ltd. shall supervise and monitor the activity of outsourced system development. Outsourced development shall adhere to all Software Products Guilda Ltd. standards and policies.

System security testing

Testing of security functionality shall be performed at defined periods during the development life cycle. No code shall be deployed to Software Products Guilda Ltd. production systems without documented, successful test results and evidence of security remediation activities.

Application vulnerability management

Application code should be scanned prior to deployment. Patches to address application vulnerabilities that materially impact security should be deployed within 90 days of discovery.

System acceptance testing

Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.

Prior to deploying code, a Release Checklist MUST be completed which includes a checklist of all Test Plans which show the completion of all associated tests and remediation of identified issues.

Protection of test data

Test data shall be selected carefully, protected and controlled. Confidential customer data shall be protected in accordance with all contracts and commitments. Customer data shall not be used for testing purposes without the explicit permission of the data owner and the CTO.

Acquisition of third-party systems and software

The acquisition of third-party systems and software shall be done in accordance with the requirements of the *Software Products Guilda Ltd. Third-Party Management Policy*.

Developer training

Software developers shall be provided with secure development training appropriate to their role at least annually. Training content shall be determined by management but shall address the prevention of common web application attacks and vulnerabilities. The following threats and vulnerabilities should be addressed as appropriate:

- Prevention of authorization bypass attacks
- Prevention of the use of insecure session IDs
- Prevention of Injection attacks
- Prevention of cross-site scripting attacks
- Prevention of cross-site request forgery attacks
- Prevention of the use of vulnerable libraries

Exceptions

Requests for an exception to this Policy must be submitted to the CTO for approval.

Violations & enforcement

Any known violations of this policy should be reported to the CTO. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Version history

Version	Date	Description	Author	Approver
1.0	Aug 28, 2024	Version 1.0	Dotan Simha	Dotan Simha