System Acquisition and Development Lifecycle Policy

Version 1 - Approved by Youssef Ouyhya

Contents

1. Objective

The objective of this policy is to provide a framework to ensure that software development activities performed in CNTXT are aligned with integrated information security considerations throughout the development lifecycle. CNTXT is committed to developing robust systems which are reliable while ensuring that security is an integral part of information systems throughout all phases of acquisition, development, and maintenance.

2. Scope

This document focuses on the development process for the software products developed or acquired by CNTXT. This document is to be followed by all CNTXT employees, sub-contractors, and partners who participate, either wholly or partially, in the product development process.

3. Policy Statement

CNTXT shall ensure that security is integral to its information systems throughout all phases of the acquisition, development, and maintenance life cycle. Security should be considered at every stage of an information system's life cycle (e.g., feasibility, planning, development, implementation, maintenance, retirement, and disposal) to:

- Ensure conformance with all appropriate security requirements
- Protect enterprise data throughout its life cycle of system development
- Prevent the introduction of new risks when the system is modified
- Ensure proper removal/disposal of data when the system is retired

4. System Acquisition, Development & Maintenance

4.1 System Development Life Cycle

Security shall be considered and included in all phases of the Software development lifecycle, including Requirement analysis, Design, Development, Testing, Implementation, Operations, and Maintenance.

4.2 Requirement Gathering

- Security and privacy requirements needed for the new product or application shall be defined at the requirements definition stage.
- Legal and regulatory implications and security requirements related to confidential data collection and usage done by the proposed system shall be considered.
- CNTXT shall consider requirements for ensuring the reliability and availability of information systems. Where availability cannot be guaranteed using existing architecture, redundant components or alternative architectures should be considered.

4.3 System Design

- It is important to identify threats and potential vulnerabilities early in the design phase of the software lifecycle. Areas of system misuse and ways in which protective measures could be bypassed shall be identified.
- The operating environment, internal and external interfaces of the system, sub-systems and components, data input and output from these sub-systems, and how the components of the software work together should be identified.
- Software shall be designed to operate with minimum privileges necessary.
- Application permissions, privileges, and access controls shall be designed to strictly adhere to the user roles defined.

4.4 System Development

- CNTXT shall establish a separate development environment, which is physically and logically isolated from the production environment and shall appropriately protect the development environment.
- During system development, developers shall be instructed to observe caution in the below areas:
    - Check the validity of incoming data
    - Check the validity of outgoing data
    - Adhere to memory management best practices
    - Secure practices during authentication and session management
    - Use best practices for errors and exception management
- Source code shall be protected from unauthorized access and source code version shall be controlled using automated mechanisms

5. Security in Development & Support Processes

5.1 Secure Application Development Principles

As a part of secure development principles, CNTXT shall consider:

- Best practices and latest libraries for each programming language used.
- Security in the application version control and code repository.
- Training developers on the secure coding aspects.
- Ensure developers' capability of avoiding, finding, and fixing vulnerabilities wherever possible.

5.2 Security Requirements for Information Systems

- Changes to systems within the development lifecycle should be controlled by the use of formal change control procedures.
- The introduction of new systems and major changes to existing systems should follow a formal process of documentation, specification, testing, managed implementation, and quality control.
- This process should include an analysis of the impacts of changes and the specification of security controls needed.
- This process should also ensure that existing security procedures are not compromised, and that support programmers are given access only to those parts of the system necessary for their work, and that formal agreement and approval for any change is obtained.
- During change control procedures the following diligence is to be considered:
    - Ensuring changes are submitted by authorized users.
    - Reviewing controls and integrity procedures to ensure that they shall not be compromised by the changes.
    - Identifying all software, information, database entities, and hardware that requires amendment.
    - Identifying and checking critical code to minimize the likelihood of known security weaknesses.
    - Ensuring authorized users approve changes prior to implementation.
    - Ensuring that the system documentation is updated on the completion of each change, wherever applicable.
    - Maintaining version control for all software updates.
    - Maintaining a record of all change requests.
    - Ensuring that Standard Operating Procedures and user manuals are changed as necessary to remain appropriate, as applicable.
    - Ensuring that the implementation of changes takes place at the right time and does not disturb the business processes involved.
    - Testing of new software should be done in an environment segregated from both the production and development environments. The tests should include patches, service packs, and other updates.
    - Automated updates should not be used on critical systems as some updates can cause critical information systems to fail.
    - Where automatic updates are considered, the risk to the integrity and availability of the system should be weighed against the benefit of speedy deployment of updates.
    - Technical review of applications after operating platform changes.

    - When underlying operating platforms are changed, business-critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security.
- As far as possible and practicable, vendor-supplied software packages should be used without modification. Where a software package needs to be modified, the following points should be considered:
    - The risk of built-in controls and integrity processes being compromised.
    - Whether the consent of the vendor should be obtained.
    - The possibility of obtaining the required changes from the vendor as standard program updates.
    - The impact if the organization becomes responsible for the future maintenance of the software as a result of changes.
    - Compatibility with other software in use. If changes are necessary, the original software should be retained, and the changes applied to a designated copy.
    - A software update management process should be implemented to ensure the most up-to-date approved patches and application updates are installed for all authorized software.
    - All changes should be fully tested, so that they can be reapplied, if necessary, to future software upgrades. If required, the modifications should be tested and validated by an independent evaluation body.

5.3 Secure Engineering

- Security system engineering principles include security at all the architecture layers (business, data, applications, and technology), balancing the need for information security with the need for accessibility.
- New technology should be analyzed for security risks and the design should be reviewed against known attack patterns.
- Systems should be regularly reviewed to ensure that they remain up to date to address any new potential threats and be scalable.
- Security engineering principles should be applied, where applicable, to outsourced information systems through the contracts and other binding agreements between the organization and the third party to whom the organization outsources.

5.4 Establishing Secure Development Environments

- The Engineering Team should establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development life cycle.
- A secure development environment includes people, processes, and technology associated with system development and integration.
- Engineering Team should assess risks associated with individual Information system development efforts and provide requirements for secure development environments for specific system development efforts, considering:
    - Sensitivity of data to be processed, stored, and transmitted by the system.
    - Applicable external and internal requirements, e.g., regulations or policies.
    - Security controls already implemented by the CNTXT that supports information system development.
    - Trustworthiness of personnel working in the environment.
    - Degree of outsourcing associated with system development.
    - The need for segregation between different development environments.
    - Control of access to the development environment.
    - Backups should be stored at secure offsite locations.
    - Control over the movement of data from and to the environment.

6. System Testing

- New and updated systems require thorough testing and verification during the development processes, including the preparation of a detailed schedule of activities and test inputs and expected outputs under a range of conditions.
- For in-house developments, such tests should initially be performed by the Engineering Team. Independent acceptance testing should then be undertaken (both for in-house and for outsourced developments) to ensure that the system works as expected and only as expected. This testing should be performed before making the change in the production environment.

- The extent of testing should be decided by the Engineering Team in concurrence with business requirements considering the importance and nature of the system.
- The testing should also be conducted on integrated systems. The Engineering team can leverage automated tools, such as code analysis tools or vulnerability scanners, and should verify the remediation of defects.
- Testing should be performed in a test environment to ensure that the Information system shall not introduce vulnerabilities to the CNTXT environment and that the tests are reliable.

7. Test Data

- The use of operational data containing personally identifiable information or any other confidential information for testing purposes should be avoided.
- If personally identifiable information or otherwise confidential information is used for testing purposes, all sensitive details and content should be protected by removal or modification.
- The following guidelines should be applied to protect operational data when used for testing purposes:
    - The access control procedures, which apply to production application systems, should also apply to test application systems.
    - Operational information should be erased from a test environment immediately after testing.
    - The copying and use of operational information should be logged to provide an audit trail.

8. Document Security Classification

Company Internal (please refer to the Data Classification policy for more details).

9. Non-Compliance

Compliance with this policy shall be verified through various methods, including but not limited to automated reporting, audits, and feedback to the policy owner. Any staff member found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment or contractual agreement. The disciplinary action shall depend on the extent, intent, and repercussions of the specific violation.

10. Responsibilities

The Information Security Officer is responsible for approving and reviewing policy and related procedures. Supporting functions, departments, and staff members shall be responsible for implementing the relevant sections of the policy in their area of operation.

11. Schedule

This document shall be reviewed annually and whenever significant changes occur in the organization.

End of System Acquisition and Development Lifecycle Policy. For version history, please see the next page.

Version history

Version	Log	Date
1 Current	Policy version approved by Youssef Ouyhya	26 Oct, 2024
1	New Policy version Created	26 Oct, 2024