[organization logo]

[organization name]

**SECURE DEVELOPMENT POLICY**

|  |  |
| --- | --- |
| Code: |  |
| Version: |  |
| Date of version: |  |
| Created by: |  |
| Approved by: |  |
| Confidentiality level: |  |

**Change history**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
| YYYY-MM-DD | 0.1 | Abdullah | Basic document outline |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of contents**

[1. Purpose, scope and users 3](#_Toc454543926)

[2. Reference documents 3](#_Toc454543927)

[3. Secure development and maintenance 3](#_Toc454543928)

[3.1. Risk assessment for the development process 3](#_Toc454543929)

[3.2. Securing the development environment 3](#_Toc454543930)

[3.3. Secure engineering principles 3](#_Toc454543931)

[3.4. Security requirements 4](#_Toc454543932)

[3.5. Security requirements related to public networks 4](#_Toc454543933)

[3.6. Checking and testing the implementation of security requirements 4](#_Toc454543934)

[3.7. Repository 4](#_Toc454543935)

[3.8. Version control 4](#_Toc454543936)

[3.9. Change control 4](#_Toc454543937)

[3.10. Protection of test data 5](#_Toc454543938)

[3.11. Required security training 5](#_Toc454543939)

[3.12. Information about secure development procedures and practices for cloud customers 5](#_Toc454543940)

[4. Managing records kept on the basis of this document 5](#_Toc454543941)

[5. Validity and document management 6](#_Toc454543942)

[6. Appendices 6](#_Toc454543943)

# Purpose, scope and users

The purpose of this document is to define basic rules for secure development of software and systems.

This document is applied to development and maintenance of all services, architecture, software and systems that are part of the Information Security Management System (ISMS).

Users of this document are all employees who work on development and maintenance in [organization name].

# Reference documents

* ISO/IEC 27001 standard, clauses A.14.1.2, A.14.1.3, A.14.2.1, A.14.2.2, A.14.2.5, A.14.2.6, A.14.2.7, A.14.2.8, A.14.2.9, A.14.3.1
* ISO/IEC 27017 standard, clauses 14.2.1 and 14.2.9
* ISO/IEC 27018 standard, clause A.9.2
* Risk Assessment and Risk Treatment Methodology
* Supplier Security Policy
* [Change Management Policy]/[Operating Procedures For Information and Communication Technology]
* Training and Awareness Plan

# Secure development and maintenance

## Risk assessment for the development process

In addition to the risk assessment performed according to the Risk Assessment and Risk Treatment Methodology, [job title] must periodically perform the assessment of the following:

* the risks related to unauthorized access to the development environment
* the risks related to unauthorized changes to the development environment
* technical vulnerabilities of the IT systems used in the organization
* the risks a new technology might bring if used in the organization

## Securing the development environment

[Identify internal as well as external requirements; describe here how access to the development environment will be restricted only to authorized employees, how it will be separated from the testing and production environment, how the backups are made.]

## Secure engineering principles

[job title] will issue procedures for secure information system engineering, both for the development of new systems and for the maintenance of the existing systems, as well as set the minimum security standards which must be complied with.

The same secure engineering principles will be applied to outsourced development, and defined through the contracts as defined in [Supplier Security Policy].

## Security requirements

When acquiring new information systems or developing or changing existing ones, [job title] must document security requirements in the Security Requirements Specification (see Appendix).

## Security requirements related to public networks

[job title] is responsible for defining security controls related to information in application services passing over public networks:

* the description of authentication systems to be used
* the description of how confidentiality and integrity of information is to be ensured
* the description of how non-repudiation of actions will be ensured

[job title] is responsible for defining controls for online transactions, which must include the following:

* how misrouting will be prevented
* how incomplete data transmission will be prevented
* how unauthorized message alteration will be prevented
* how unauthorized message duplication will be prevented
* how unauthorized data disclosure will be prevented

## Checking and testing the implementation of security requirements

[job title] is responsible to define the methodology, responsibilities and the timing of checking whether all the security requirements from the Security Requirements Specification have been met, and whether the system is acceptable for production.

## Repository

[Describe here where the code and all other files related to development are kept, and how they are protected from unauthorized access and unauthorized change.]

## Version control

[Define here what is the system of version control (numbering, dates, etc.), and how it is enforced in your development environment.]

## Change control

Changes in the development and during the maintenance of the systems must be done according to the [Change Management Policy]/[Operating Procedures For Information and Communication Technology].

## Protection of test data

Confidential data, as well as data that can be related to individual persons must not be used as test data. Exceptions may be approved only by [job title], in which case [job title] must define how such test data are protected.

## Required security training

[job title] defines the level of security skills and knowledge required for the development process and proposes the trainings to [job title]. [job title] includes appropriate trainings in the Training and Awareness Plan.

## Information about secure development procedures and practices for cloud customers

[Define here, according to organization’s Information Classification Policy, which elements of this policy can be made available to cloud customers to ensure to them the organizations’ commitment with the secure development of services and systems provided in the cloud environment].

For any additional information required by cloud service customers regarding the development process, [job title] must decide whether such information can be sent according the Information Classification Policy.

# Managing records kept on the basis of this document

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Record name | Storage location | Person responsible for storage | Controls for record protection | Retention time |
| [List of risks related to development process] | [job title]'s computer | [job title] | [only [job title] can access those files] | 3 years for lists that are no longer valid |
| [Procedures for secure information system engineering] | [organization’s intranet] | [job title] | [only [job title] can publish and edit those files] | 5 years for procedures that are no longer valid |
| [Testing plans] | [organization’s intranet] | [job title] | [only [job title] can publish and edit those files] | 5 years for tests that have been performed |

# Validity and document management

This document is valid as of [date].

The owner of this document is [job title], who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

* number of incidents arising from failed security controls built into the systems

Previous versions of this procedure must be stored for a period of 5 years, unless specified otherwise by legal or contractual requirement.

# Appendices

* Security Requirements Specification

[job title]

[name]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[signature]