\*\* FREE PREVIEW VERSION \*\*

[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** |
| dd.mm.yyyy | 0.1 | EUGDPRAcademy | Basic document outline |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of contents**

[1. Purpose, scope and users 3](#_Toc113871779)

[2. Reference documents 3](#_Toc113871780)

[3. Secure development and maintenance 3](#_Toc113871781)

[3.1. Risk assessment for the development process 3](#_Toc113871782)

[3.2. Securing the development environment 3](#_Toc113871783)

[3.3. Principles for engineering secure systems 3](#_Toc113871784)

[3.4. Secure coding 4](#_Toc113871785)

[3.5. Security requirements 4](#_Toc113871786)

[3.6. Security requirements related to public networks 4](#_Toc113871787)

[3.7. Checking and testing the implementation of security requirements 4](#_Toc113871788)

[3.8. Repository 5](#_Toc113871789)

[3.9. Version control 5](#_Toc113871790)

[3.10. Change control 5](#_Toc113871791)

[3.11. Protection of test data 5](#_Toc113871792)

[3.12. Required security training 5](#_Toc113871793)

[4. Managing records kept on the basis of this document 5](#_Toc113871794)

[5. Validity and document management 6](#_Toc113871795)

[6. Appendices 6](#_Toc113871796)

# 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) and/or the personal data processing activities.

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

# Reference documents

* ISO/IEC 27001 standard, clauses A.5.33, A.8.11, A.8.25, A.8.26, A.8.27, A.8.28, A.8.29, A.8.30, A.8.31, A.8.32, and A.8.33
* EU GDPR Article 32
* Risk Assessment and Risk Treatment Methodology
* Supplier Security Policy
* [Change Management Policy]/[Security Procedures for IT Department]
* 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
* the risks a new development methodology and/or programming language might bring if used in the organization
* the risks related to licensing requirements

## 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.]

## Principles for engineering secure systems

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

\*\* END OF FREE PREVIEW \*\*

To download full version of this document click here: <https://advisera.com/27001academy/documentation/secure-development-policy/>