# Software development plan for XXX

|  |  |
| --- | --- |
| Created on xxxx-xx-xx by |  |
| Modified on xxxx-xx-xx by |  |
|  |  |
| Revision |  |
| Classification |  |
| Approved on xxxx-xx-xx by |  |

Contents

[Software development plan for XXX 1](#_Toc455039118)

[1. Document scope 3](#_Toc455039119)

[2. Responsibilities 3](#_Toc455039120)

[3. Software description and security requirements 3](#_Toc455039121)

[4. Architecture 3](#_Toc455039122)

[4.1 Data stored by the service 3](#_Toc455039123)

[4.2 Components used by the software 4](#_Toc455039124)

[4.3 External data sources 4](#_Toc455039125)

[4.4 Logging and log format 4](#_Toc455039126)

[5. Environment 4](#_Toc455039127)

[5.1 Development environment 4](#_Toc455039128)

[5.2 Test environment 4](#_Toc455039129)

[5.3 Production environment 4](#_Toc455039130)

[5.4 Source code 4](#_Toc455039131)

[6. Development workflow, testing and reviews 5](#_Toc455039132)

[6.1 Development workflow 5](#_Toc455039133)

[6.2 Testing plan 5](#_Toc455039134)

[6.3 Review 5](#_Toc455039135)

[7. Implementation 5](#_Toc455039136)

[7.1 Installation 5](#_Toc455039137)

[7.2 Configuration 6](#_Toc455039138)

[7.3 Backup policy 6](#_Toc455039139)

[7.4 Incident and error handling 6](#_Toc455039140)

[Appendix A: requirements and feasibility study 7](#_Toc455039141)

[Requirements and feasibility study of software XXX 7](#_Toc455039142)

[The feasibility study 7](#_Toc455039143)

[Security and risk analysis 7](#_Toc455039144)

[Architectural design 7](#_Toc455039145)

[Requirement specifications 7](#_Toc455039146)

# Document scope

This is the software development plan for XXX. The purpose of this document is to define the practices of software development via recognition of important aspects concerning quality control, security and privacy, to name but a few. These practices will help to ensure the quality and security standards are met.

This software development plan is approved by XXX and is checked against organization’s software development requirements for security and quality. This document is reviewed XXX times a year by XXX.

# Responsibilities

The persons responsible of the software are listed in the following table. The security training is organized by the organization based on this role.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Role** | **Name** | **Email** | **Phone** | **Responsibility** |
| e.g. software owner, developer, architect |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table 1: roles and responsibilities

# Software description and security requirements

*Write a short description of what this software is and what are the basic security requirements. Describe the likely threats and how they should be mitigated.* The recognized threats are listed in the following table:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat** | **Criticality** | **Attack area** | **Effectiveness** | **Counter measures** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table 2: threats

Based on the requirements of the software, the security level for software development is: **Basic / Raised / High**

# Architecture

The architectural overview will contain information, which will define how the software will be built as well as its operation environment. This information will play an important role in all stages of the software’s lifecycle, including the planning, implementation and update stages.

## 4.1 Data stored by the service

The software stores data described in table 3.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Data** | **Contains personal information** | **Contains secret information** | **To be preserved after service decommission?** | **Security level and value** | **Data is stored in** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Table 3: data stored by the software

Based on table 3, the trust boundaries and communication between different trust boundaries as handles as follows: *describe which the trust boundaries are and how communication flows securely between them*.

According to classification the data itself is encrypted with technologies described in table 4. In addition, the connections to access the data must meet the security requirements described in the aforementioned table.

|  |  |  |
| --- | --- | --- |
| **Data** | **Data store encryption** | **Connection secured by** |
|  |  |  |
|  |  |  |
|  |  |  |

Table 4: data encryption

## 4.2 Components used by the software

The software uses a variety of components listed in table 5. These components are verified and updated against the organization’s component catalogue.

|  |  |  |  |
| --- | --- | --- | --- |
| **Name of the component** | **Licence** | **Timeliness** | **Updated by** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table 5: components

The components described in table 5 are kept updated with following procedures: *add detailed description of how the updates are monitored and applied, how and by who updates are monitored and classified etc.*

## 4.3 External data sources

The software uses external data sources (APIs) depicted in table 6. The security requirements column depicts how the data transfer is secured.

|  |  |  |  |
| --- | --- | --- | --- |
| **Title** | **Source** | **Security level** | **Security requirements** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table 6: external sources

## 4.4 Logging and log format

The software gathers log information from following components and actions: *describe which actions should be logged.* The following security incidents are logged and monitored:

The logs will collect the following information: *e.g. timestamp, significance, type, account, IP, result, description*. The conformity of timestamps across systems are ensured by xxx.

# Environment

## 5.1 Development environment

*Describe the details of the development environment and how it is secured and backed up.*

## 5.2 Test environment

*Describe the details of the test environment and how it is secured and backed up.*

## 5.3 Production environment

*Describe the details of the test environment and how it is secured and backed up.*

## 5.4 Source code

Source code is maintained in repositories described in the following table:

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **URL** | **Security level** | **Backup** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table 7: software repositories

The developers access the repositories with following accounts:

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Account** | **Repository name** | **Privileges** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table 8: user access to repositories

# Development workflow, testing and reviews

## 6.1 Development workflow

*Describe the basic development workflow, including the tools, definition of done, conventions, security requirements etc.*

## 6.2 Testing plan

*Describe how all changes to the software are tested. Especially, depict the required security tests. Document the automatic testing and required test cases and how test data is generated in secure way.*

This testing plan was reviewed by xxx.

## 6.3 Review

*Describe how smaller changes are reviewed in the development process. Add information on how releases are reviewed for quality and security requirements. Fill out table 9 for things to check during reviews: some examples are given.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Title** | **Description** | **Applied to** | **Customer output** |
| e.g. error handling | e.g. check that errors don’t expose information about the system | e.g. components x, y and z | e.g. print xxx |
| e.g. encryption | e.g. check that encryption level is sufficient | e.g. when data x is stored |  |
| e.g. cross-site scripting | e.g. check for XSS vulnerabilities | e.g. components x, y, z, w for user input | e.g. display user that the input was discarded |
|  |  |  |  |
|  |  |  |  |

Table 9: checklist for code reviews

# Implementation

## 7.1 Installation

*Describe how the software should be installed, what are the requirements etc.*

## 7.2 Configuration

*Describe the system and software configuration required by the software. Describe how the system should be hardened, if applicable.*

## 7.3 Backup policy

*Describe what is backed up and how, describe also how this backup plan is tested and how often.*

## 7.4 Incident and error handling

*Describe how incidents and errors are handled – note your organization’s requirements.*

# Appendix A: requirements and feasibility study

## Requirements and feasibility study of software XXX

This document describes the requirements of a software XXX. The details described here must build the basis of the software development practices and the architectural design. The requirements listed here must be reviewed in all stages of the software or service lifecycle, including the development, review, deployment and uncommissioning.

### The feasibility study

*Describe the purpose and criticality of the software, including connections, data and data confidentiality. Describe also the software’s importance from the organization’s point of view.*

### Security and risk analysis

*Analyze security requirements needed by the software, for example the confidentiality, integrity and availability should be described as a result.*

*Describe what should be the security level of the software: this will affect greatly on all aspects of the software’s lifecycle.*

*For the risk analysis, describe the worst case scenarios which could compromise the software or service.*

### Architectural design

*Describe the architecture: this will be affected by the security analysis and the organization’s specifications.*

### Requirement specifications

*Using the data above, add security requirements in addition to the functional ones.*