**Appendix 3 – Form – Risk Assessment and Treatment Report**

**Change history**

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

**Table of contents**

[1. Purpose, scope and users 2](#_Toc415648868)

[2. Reference documents 2](#_Toc415648869)

[3. Process of assessment and treatment of information risks 2](#_Toc415648870)

[3.1. Purpose of risk management 2](#_Toc415648871)

[3.2. Risk assessment and risk treatment scope 2](#_Toc415648872)

[3.3. Time period 2](#_Toc415648873)

[3.4. Participants in the process and collection of information 2](#_Toc415648874)

[3.5. Brief overview of the applied methodology 3](#_Toc415648875)

[3.6. Overview of documents used during the risk assessment and risk treatment process 3](#_Toc415648876)

[4. Validity and document management 3](#_Toc415648877)

[5. Appendices 3](#_Toc415648878)

# Purpose, scope and users

The purpose of this document is to give a detailed overview of the process and documents used during risk assessment and treatment of information risks in [organization name] in the period [specify period].

Risk assessment was applied to the entire Information Security Management System (ISMS).

This document is intended for top management of [organization name], [job title responsible for information security], owners of information assets, and everyone involved in planning, implementing, monitoring and improving the ISMS.

# Reference documents

* ISO/IEC 27001 standard, clauses 8.2 and 8.3
* ISMS Scope Document
* Information Security Policy
* Risk Assessment and Risk Treatment Methodology

# Process of assessment and treatment of information risks

The entire risk assessment and risk treatment process has been carried out according to the Risk Assessment and Risk Treatment Methodology document.

## Purpose of risk management

The purpose of risk assessment is to identify all assets, their vulnerabilities, and threats that could exploit such vulnerabilities, as well as to evaluate these parameters in order to establish the criticality of individual risks.

The purpose of risk treatment is to define systematic means of reducing or controlling such risks.

## Risk assessment and risk treatment scope

Risk assessment and risk treatment was carried out in [name of organizational units], in accordance with the ISMS Scope document.

## Time period

Risk assessment was implemented in the period from [day/month/year] to [day/month/year]. Risk treatment was implemented from [day/month/year] to [day/month/year]. Final reports were prepared during [specify period].

## Participants in the process and collection of information

The risk assessment and risk treatment process was managed by [name and job title], with expert assistance provided by [if expert assistance was used, provide name and company].

During risk assessment, information was collected through questionnaires and interviews with responsible persons, i.e. asset owners from all organizational units.

## Brief overview of the applied methodology

Briefly, the process was conducted in the following way:

* all assets were identified, as well as their owners
* threats were identified for each asset, and corresponding vulnerabilities were identified for each threat
* risk owners were identified for each risk
* consequences of the loss of confidentiality, integrity and availability were evaluated using values 0 to 2
* the likelihood of risk occurrence, i.e. that the threat will exploit the vulnerability, was evaluated using values 0 to 2
* the level of risk was calculated by adding up consequence and likelihood
* risks valued 3 and 4 were determined as unacceptable risks
* for each unacceptable risk, a risk treatment option was considered, and controls which can reduce the risk to an acceptable level were selected from Annex A of the ISO/IEC 27001 standard
* after controls were applied, residual risks were assessed

## Overview of documents used during the risk assessment and risk treatment process

The following documents were used or drawn up during the implementation of risk assessment and risk treatment:

* Risk Assessment Table (Appendix 1) – for each combination of assets, vulnerabilities and threats, this table shows the values for consequence and likelihood, and calculates the risk
* Risk Treatment Table (Appendix 2) – shows the options for risk treatment, selection of controls for each unacceptable risk, and the level of residual risk

# Validity and document management

This document is valid as of [date]. Owner of this document is [job title].

# Appendices

* Appendix 1: Risk Assessment Table
* Appendix 2: Risk Treatment Table

[job title]

[name]

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

[signature]