Appendix 3 – Risk Assessment and Treatment Report

Change history

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Created by</th>
<th>Description of change</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td></td>
<td>27001Academy</td>
<td>Basic document outline</td>
</tr>
</tbody>
</table>

Table of contents

1. PURPOSE, SCOPE AND USERS ..................................................................................................................... 2
2. REFERENCE DOCUMENTS ........................................................................................................................... 2
3. PROCESS OF ASSESSMENT AND TREATMENT OF INFORMATION RISKS ....................................................... 2
   3.1. PURPOSE OF RISK MANAGEMENT ................................................................................................... 2
   3.2. RISK ASSESSMENT AND RISK TREATMENT SCOPE ...................................................................... 2
   3.3. TIME PERIOD ................................................................................................................................. 2
   3.4. PARTICIPANTS IN THE PROCESS AND COLLECTION OF INFORMATION .................................... 2
   3.5. BRIEF OVERVIEW OF THE APPLIED METHODOLOGY ................................................................. 3
   3.6. OVERVIEW OF DOCUMENTS USED DURING THE RISK ASSESSMENT AND RISK TREATMENT PROCESS ........................................................................................................................... 3
4. VALIDITY AND DOCUMENT MANAGEMENT ............................................................................................ 3
5. APPENDICES .................................................................................................................................................. 3
1. 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.

2. Reference documents

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

3. 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.

3.1. Purpose of risk management

The purpose of the process is to identify and evaluate potential threats to the organization, as well as to determine the level of risk and the measures necessary to protect the organization from these threats.

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

3.2. Risk assessment and risk treatment scope

The focus of risk assessment and risk treatment will be on those areas of the organization which are critical to its operations and which have the highest risk.

3.3. Time period

Risk assessment was implemented in the period from [day/month/year] to [day/month/year]. Risk treatment was implemented in the period from [day/month/year] to [day/month/year].

3.4. Participants in the process and collection of information
The risk assessment and risk treatment process was managed by [name and job title], with expert

3.5. Brief overview of the applied methodology

Briefly, the process was conducted in the following way:

- all assets were identified, as well as their owners

- 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

- standard, as well as from other security control sources deemed relevant

- after controls were applied, residual risks were assessed

3.6. Overview of documents used during the risk assessment and risk treatment process

- 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

4. Validity and document management

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

5. Appendices

- Appendix 1 – Risk Assessment Table
- Appendix 2 – Risk Treatment Table