[Company Logo]

[Company Name]

[Confidentiality Level]

PL– RISK MANAGEMENT POLICY

Version: 1.0

Commented [Olesia Ko1]: **ATTENTION: All fields in this document marked by square brackets [ ] must be filled in.**

Commented [Olesia Ko2]: Please specify the document Confidentiality Level:
Public
Internal
Confidential
Usually, it is the "**Internal"** level for most Policies and Procedures.

Commented [Olesia Ko3]: Please insert the actual version number.

Version History

Reviewer Name	Version - ddmmyyyy	Description of Updates

Table of Contents

Definitions

Term	Definition
Company	[Company Name]
Policy	[Policy Name]
Personnel	Company's employees and contractors
ISMS	Information Security Management System
Asset	is an IT equipment, tangible or intangible, controlled by the Company
Threat	is something that can damage or destroy an asset
Vulnerability	a weakness or gap in the Company's protection
Risk	a function of threats taking advantage of vulnerabilities to steal or damage assets
[Table Text]	[Table Text]

Commented [Olesia Ko4]: Please provide applicable to this document terms and acronyms, if needed.

Document Purpose

This Policy aims to define the basic principles and rules for information security risk management within the Company.

Scope

This Policy is valid for the entire Company.

Governance

The responsibility to manage and update this Policy is assigned to a Process Owner position.

Commented [Olesia Ko5]: Please insert the Process Owner position.

This Policy should be evaluated annually to ensure its adequacy and relevance regarding the Company's needs and goals.

Roles and Responsibilities

Role	Responsibility Description
[Process Owner]	is responsible for overall information security risk management governance within the Company including: • driving overall coordination of risk management processes • developing methodology for risk assessment

Commented [Olesia Ko6]: Please insert the Process Owner position.

	• supporting asset owners to identify risks and support the development of an action plan • monitoring the progress of the implementation of the action plan • providing timely updates to the risk map to the Top Management Board • processing exceptions
Top Management Board	is responsible for establishing an information security risk management program within the Company by providing the necessary resources and demonstrate a personal commitment to the maintenance and continual improvement, including: • reviewing and approving Risk Treatment Plan • handling escalations
Asset Owners	is responsible for • identifying and assessing the risks referential to the dedicated asset • developing action plans and reporting on the progress.

Overview

The overall goal of the Company's ISMS is to protect its information assets. The assets-threats-vulnerabilities risk methodology is the essence of the Company's risk management approach.

Information Security Risk Assessment

A risk assessment is the first phase of the risk management process. Information security risks are to be identified and captured in Risk Treatment Plan, tracked until closure. An Asset Register is a subject of the risk assessment process.

The [Process Owner] along with asset owners should perform risk assessment at least annually. The top Management Board should approve the risk Treatment Plan.

Commented [Olesia Ko7]: This section contains only an example, how risk assessment can be performed. You can use another methodology, but in this case, please delete the content from this section and fill it in with any other methodology description.

Commented [Olesia Ko8]: You can use software for this purpose or create a simple list. You should be ready to show the Risk Treatment Plan or software during the audit. All information should be up to date, and at least an annual review should be conducted.

Commented [Olesia Ko9]: Please insert the Process Owner position.

Below are the steps in the risk assessment process:

Step Name	Description
Information asset identification	Asset Register should be developed according to PL-Asset Management Policy.
Analysis of threats and vulnerabilities	Analysis of threats and vulnerabilities referential to the dedicated asset should be conducted.
Calculation of RPN (Risk Priority Number)	The RPN should be calculated by multiplying the impact value of the asset by the likelihood of the risk happening.

Risk Priority Number

To calculate the RPN, the following calculation is performed:

Likelihood x Impact = RPN

The likelihood is the probability of anticipated risk event occurrence.

The likelihood criteria are below:

Scale	Numerical Scale	Likelihood Value, %
Unlikely	1	1 - 20%
Possible	3	21 – 70%
Likely	9	71 – 100%

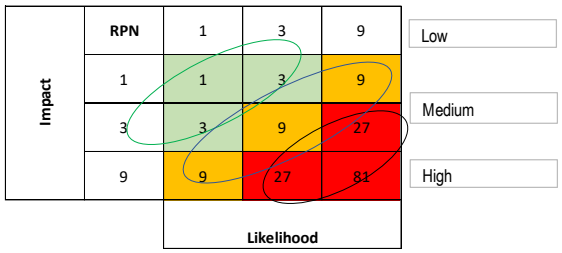
The impact is s the potential effect of a risk event occurrence.

The impact criteria are below:

Scale	Numerical Scale	Description
Low	1	Risk impact may cause a negligible effect
Medium	3	Risk impact may cause a moderate effect
High	9	Risk impact may cause a critical effect

The resulting number can be used to create an RPN, which can then be rated as Low, Medium, or High according to the heatmap below.

Risk Priority Number



There are three levels of information security risks:

RPN	Description
1-3	It is almost certain that the vulnerabilities will be exploited as there are no controls in place or it has happened in the past
9	The vulnerabilities may be exploited as some protection is in place.
27-81	It is unlikely that the vulnerabilities addressed will be exploited as the protection in place is considered to be good.

Risk strategy and Action Plan

Risk owner should be assigned once the risk is identified. The risk owner, with the assistance of [Process Owner], should determine the risk strategy and action plan.

Commented [Olesia Ko10]: Please insert the Process Owner position.

Risk strategy includes risk avoidance, mitigation, sharing, and acceptance.

Risk strategy and examples are in the table below.

Strategy	Description
Avoidance	Deciding not to engage in new initiatives or activities that would give rise to the risks.
Mitigation	Reducing the probability of occurrence or impact of a risk
Sharing	Sharing risk through contractual agreements with customers, vendors, or other business partners or outsourcing business processes.
Acceptance	Not taking any action unless the risk occurs.
Enhance	Increasing the probability and/or impact of positive risks.

Risk owners report action plan progress or changes to [Process Owner] regularly or upon request.

Commented [Olesia Ko11]: Please insert the Process Owner position.