Risk management policy

Scope:

This policy covers the risks of breaches in a company, that can have impact on company assets, reputation and can cause some financial fines.

Document Owner and Approval:

Owner: The policy owner is Chief compliance officer.
Approval: This policy should be approved by CISO.

Responsibilities:

Compliance engineer is responsible for annual policy review and update.
InfoSec manager is responsible for choosing frameworks and best practices for implementation in the company.
Senior SOC engineer is accountable for implementation this policy statements in work processes in the company.
Security Engineer is responsible for using this policy statements in daily processes in the company.

Policy statements:

Introduction knowledges

Cybersecurity threat - Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Vulnerability - A vulnerability is a weakness in an IT system that can be exploited by an attacker to deliver a successful attack. They can occur through flaws, features or user error, and attackers will look to exploit any of them, often combining one or more, to achieve their end goal.

Likelihood - refers to the probability or frequency with which a specific threat will exploit a vulnerability and cause harm.

Assets - are the valuable resources that an organization needs to protect, including sensitive data, intellectual property, systems, applications, and infrastructure.

Impact - potential harm or consequences that could result from a successful cyber attack or security breach.

Controls - controls refer to measures to reduce, or mitigate security risks and protect information assets from unauthorized access, disclosure, alteration, or destruction.

Risk = Likelihood * Impact Level

How to classify threats at our company:

Threat Frequency	Description
Very Low	Threat events are expected to occur extremely rarely, with little to no historical occurrences or evidence of similar incidents.
Low	Threat events occur infrequently, with occasional historical occurrences or evidence of sporadic incidents.
Medium	Threat events occur with some regularity, showing a moderate frequency of historical occurrences or evidence of occasional incidents.

Threat Frequency	Description
High	Threat events occur frequently, with a notable history of occurrences or evidence of regular incidents.
Very High	Threat events occur very frequently, with a high frequency of historical occurrences or evidence of persistent, ongoing incidents.

How to classify vulnerabilities at our company:

Probability of vulnerability being breached (Level)	Probability of vulnerability being breached (Description Statements)
Very High	The vulnerability is EXPECTED to be exploited or triggered in most circumstances
High	The vulnerability will PROBABLY be exploited or triggered in most circumstances
Medium	The vulnerability MIGHT be exploited or triggered at some time but is not expected
Low	The vulnerability COULD be exploited or triggered at some time
Very Low	The vulnerability MAY be exploited or triggered in exceptional circumstances

Impact Levels:

Level	Budget impact
Very High	More than 30,000$
High	10,000$ - 30,000$
Medium	5,000$ -10,000$
Low	1,000$ - 5000$
Very Low	Less than 1,000$

Likelihood = Threat * Vulnerability

Table 3.5.3: Likelihood matrix

		Probability of vulnerability being breached				
		Very Low	**Low**	**Medium**	**High**	**Very High**
Frequency of threat occuring	Very Low	Very Low	Very Low	Low	Low	Medium
	Low	Very Low	Low	Low	Medium	High
	Medium	Low	Low	Medium	High	High
	High	Low	Medium	High	High	Very High
	Very High	Medium	High	High	Very High	Very High

Risk Level = Likelihood * Impact

		Impact Level				
		Very Low	**Low**	**Medium**	**High**	**Very High**
Likelihood	Very Low	Very Low	Very Low	Low	Low	Medium
	Low	Very Low	Low	Low	Medium	High
	Medium	Low	Low	Medium	High	High
	High	Low	Medium	High	High	Very High
	Very High	Medium	High	High	Very High	Very High

There we have a list of popular attacks on company assets, their characteristics and how we can mitigate risks:

	Treat	Vulnerability	Likelihood	Impact	Initial Risk	Controls	Residual Risk
UBS dropping	Very High	Very High	Very High	Very High	Very High	Employees education Write policy about using unauthorized devices in a company Use antivirus	Low
Tailgating attack	Medium	Very High	High	Very High	Very High	Employees education Physical security guard	Very Low

						Use key cards with doors that admit only one person in one time	
Phishing	Very High	Very High	Very High	High	Very High	Employees education Install software that will detect phishing actions and connect it to SIEM	Medium

Enforcement:

If employees don't follow the policy, it will cause data breaches, financial losses for company and financial fines for employees that don't follow the policy.