# Information Security Risk Assessment Policy

## A Table of Contents

A. Context ..... 2
B. Policy ..... 3
C. Procedure ..... 4
1. Risk Assessment ..... 4
2. Risk Register ..... 4
3. Control Register ..... 5
4. Risks Matrix ..... 5



**MENU Technologies AG** · Dammstrasse 19 · 6301 Zug, Switzerland · +41 41 723 2041 · hello@menu.app

# A. Context

Protecting personal data and our company assets is a main priority of ours to preserve the trust of our customers & partners and safeguard our intellectual property. As such, we are commited to regularly reviewing our information security measures and assessing potential risks through a structured process.

This document defines the framework used at MENU to identify, assess and manage information security risks, ensuring they are controlled in a manner that balances the resources required to implement the controls to their risk of resulting in a negative business impact.

This policy applies to all information systems at MENU and to all MENU personnel with access to MENU information systems.

If you have any questions about this document, please address them to your line manager or information-security@menu.app

## B. Policy

- Information security risks are assessed at least annually (or for specific events, as defined in this document) and treated & controlled based on their probability and impact
- Information security risks are known and communicated to the Security Management.

# C. Procedure

## 1. Risk Assessment

The Risk Assessment identifies information security risks, assesses the probability of them occurring and their business impact and defines controls to address them based on their inherent risk.

The Risk Assessment is maintained by the Security Management. The Risk Assessment has to be updated at least:

- For the introduction of a new significant information system impacting the organization's security
- For every modification to systems or processes changing recorded threats or risks
- Anually

## 2. Risk Register

The Risk Register is part of the Risk Assessment and lists all identified risks/threats to MENU's information systems.

The Risk Register should document the following information on every identified risk:

- **Risk Title:** Title describing the threat/risk
- **Description:** Description of the risk
- **Cause:** Actions that will cause the risk
- **Effect:** The negative results of the risk for MENU and/or it's customers
- **Owner:** Person responsible for the risk and manging the risk mitigation efforts
- **Probability:** How likely the risk is to occur, as defined in the legend below
- **Impact:** Business impact of the risk's result, as defined in the legend below
- **Inherent Risk:** Risk (High – Medium – Low) based on the Probability and Impact assessment

**Probability**

| Rating | Definition |
|---|---|
| Likely | Will occur within the next 1-6 months |
| Possible | Will occur within the next year |
| Remote | Will occur within the next 5 years |
| Extremely Remote | Will occur within the next 10 years |

**Impact**

| Rating | Definition |
|---|---|
| Catastrophic | >20 customers affected. Significant national and international media coverage of event lasting for months. Significant regulatory implications and censure will require significant remediation activity |

| | |
|---|---|
| | to be undertaken. Large-scale changes to operations or control environment required. |
| Critical | 10-20 customers affected. Significant local media coverage of event lasting for weeks, possible limited national coverage. Some regulatory implications or criticism will require remediation activity to be undertaken. Large changes to operations or control environment required. |
| Significant | 2-10 customers affected. Limited local media coverage of event lasting for days. Limited regulatory implications or censure, possible re-work/remediation. Some changes to operations or control environment required. |
| Important | <2 customers affected. No media coverage of the event. No regulatory implications or censure. No changes to operations or control environment required. |

## 3. Control Register

The Control Register is part of the Risk Assessment and lists implemented controls to treat one or more risks.

Suggested controls are approved by the CTO based on their proportionateness.

The Control Register should document the following information on every implemented control:

- **Control Title:** Title describing the control
- **Objective:** Describes the goal of the control
- **Procedure:** How the control is implemented

Per risk that the control mitigates, the following information should be documented:

- **Owner:** Person responsible for implementing & managing the control for the given risk
- **Frequency:** How often the control is performed
- **Level:** How the control is performed (Pervasive, Transacitonal or Monitoring)
- **Type:** If the control is automated or performed manually
- **Timing:** If the control is implemented Preventative, Detective or Corrective

## 4. Risks Matrix

The Risks Matrix is part of the Risk Assessment and documents the resulting impact & probability of the risk based on the implemented controls, as well as assesses the performance of each control.

The Risks Matrix should document the following information for every risk:

- **Resulting Impact:** Impact of the risk, after implemented controls, as defined in the legend above *(Risk Register)*

- **Resulting Probability:** Probability of the risk occuring, after implemented controls, as defined in the legend above *(Risk Register)*

Per control implemented for a risk, the following information should be assessed & documented:

- **Mitigation:** How much the control reduces the severity/likelyhood of the risk (Low, Medium or High)
- **Design:** Effectiveness of how control was implemented (Effective, Partially Effective or Not Effective)
- **Performance:** How the implmeneted control performs for the identified risk, based on previous experience (Effective, Partially Effective or Not Effective)
- **Effectiveness:** Overall effectiveness of implemented control