# Information security policy for ORGANIZATION X

CyberPilot

# Information security policy for ORGANIZATION X

*These policies can serve as inspiration for your own IT security policy or be copied and implemented directly in your organization – it is entirely up to you. However, be aware to change the X to the name of your organization.*

*Enjoy! :-)*

*Best regards,*
*The CyberPilot team*

## Purpose

The security policy defines the framework for the management of information security in X.

## Validity

The security policy applies to all employees in X and the entire access to X's information systems.

## Objectives

- X works actively with the management of information security with the purpose of securing availability, systems, and data
- X endeavors to comply with ISO 27001:2013 / ISO27002:2013
- X uses a risk-based approach where the level of protection and its cost must be based on the business risk and impact assessment that must be carried out annually as a minimum
- An IT-security handbook must be prepared and continuously updated. This handbook shall contain descriptions of implemented actions when it comes to information security and references to relevant policies, guidelines, and procedures
- X aims to comply with relevant legislation, including e.g. GDPR
- X intends to comply with agreements set with external parties, including data processing agreements
- X strives to prepare a yearly statement i.e. ISAE3402, ISAE3000, ISO-certificate, etc.
- This information security policy shall be reviewed on an annual basis

## Organization and responsibilities

- **The board of directors** has the ultimate responsibility for the information security in X.
- **The executive board** is responsible for management principles and delegates specific responsibilities for protective measures, which includes ownership of information systems.
- **Ownership** is set for every critical information system. The owner establishes how

protective measures are used and managed in compliance with the security policy.

- **The IT-department** consults, coordinates, controls, and reports on the status of the security. The IT-department prepares guidelines and procedures.
- **The individual employee** is responsible for complying with the security policy and being informed about it in the "IT-usage policy".

## Waiver

Waivers for X's information security policy and guidelines are approved by the IT-department based on the guidelines laid out by the executive board.

## Reporting

- The IT-department informs the executive board about all relevant security breaches
- Status of waivers are included in the IT-department's annual report to the executive board
- The executive board reviews the security status annually and reports to the board of directors afterward

## Violation

Intentional violation and abuse are reported by the IT-department to the HR-department and the closest authority with lead responsibility.

Violation of the information security policy and supporting guidelines may result in employment law consequences.