ISO 27001 Implementation

Security Practices Overview

wultra

List of Contents

Introduction

Our mission is to help banks and fintech companies build secure digital applications and give their customers peace of mind when trusting them with their money. Aware of this utterly important goal, we consider the security of our customers and partners' data of the utmost importance and commit ourselves to take appropriate measures to protect the data and continuously evaluate and improve them.

In terms of security, we aim to be transparent. That is why we've prepared this document summarising the fundamental technical and organisational principles of how we protect our assets and information.

Security Framework

In October 2019, we became an ISO/IEC 27001:2013 certified company. The Standard defines the Information Security Management System requirements and establishes the Plan - Do - Check - Act framework we are fully committed to implementing and maintaining. We continuously improve the security of our assets by evaluating the currently taken measures, planning the future improvements of the ISMS system, implementing the designed changes, assessing them and implementing additional measures based on the control results.

Our security goal is to prevent or at least dramatically eliminate all risks that could negatively affect the Company's business and information confidentiality, integrity

ISO 27001:2013

ISO/IEC 27001 is an information security standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It specifies a management system intended to bring information security under management control. It designs security management best practices and comprehensive security controls. It is based on developing and implementing an Information Security Management System (ISMS) in a company.

and availability. We also aim to have active controls of prompt negative events reporting and a clearly defined business continuity plan. We openly declare that we act accordingly to valid legislation and civil service requirements as well as with the ISO 27001 requirements. Furthermore, we aim to maintain the ISMS management beyond the valid legislation requirements.

The security rules and processes defined by the ISO 27001 standard are binding to everyone in the Company and all subjects that cooperate with us.

Organisational Security

Through the implementation of the Information Security Management System (ISMS), we incorporate security measures into all Company processes and regularly train all employees on them.

The ISMS Manager, Security Administrator and Security Manager cooperate on the ISMS implementation, development and examination. The company Representative makes sure there are enough resources to maintain Information Security. Together with the Security Administrator, they initiate plans and programmes to increase security consciousness in the Company.

Security Policies

To describe and summarise our security measures, we define and regularly review the Security Policies. The Policies set up rules for putting the security measures into practice and define key responsibilities and rights of the employees in all aspects of the business so that they become an integral part of the job duties.

The Security Policies reflect the work environment needs, constant processes' improvement, and the need to meet modern security standards.

Security Risk Management

A list of all Company assets is maintained and regularly updated. Possible risks that result from threats exploiting their vulnerabilities are identified, evaluated and prioritised to be able to take relevant measures to mitigate the risks and avoid negative events.

Outsourcing and Third-Party Risk Management

Each external vendor is checked and proved before the cooperation begins. Essential Information Security requirements are included in all contracts with our vendors.

Interested Parties

The overview of interested parties is regularly reviewed and updated. The requirements of the interested parties are considered, and measures are taken to meet them.

Employees’ Security Awareness

All employees are regularly trained on the ISMS rules and policies. The training is compulsory and conducted at the beginning of the employment relationship and then in regular intervals.

Professional Development

All employees are encouraged to broaden their skills in their professional careers and security area. To stay up to date with the latest trends, they attend further training, conferences or knowledge-sharing meetings.

Operational Measures

We set up several protective measures to prevent all our assets from misusing, damaging, or stealing. These measures include physical premises, network and credentials security, and other relevant procedures. To maintain the high quality of our services and ensure trust in them, we apply and review access management policies, design measures to prevent hacking activities and malware infections, and to avoid data leakage. Our overall system security ensures data integrity, availability and confidentiality.

Network Security

We protect the Company network and network services by a set of organisational and operational measures - we manage access to the network, monitor and protect logs, restrict access to network services and applications, regularly check encryption, network connections, and authentication means. The network separation principle is ensured.

Cryptography and Encryption

Where appropriate, we apply cryptography and encryption measures. Information stored digitally has to be cryptographically protected based on its classification level. All web applications containing sensitive and or personal information are based on HTTPS. The cryptographic protection has to be applied during the information saving, manipulation and transmission.

Device Management

All Company laptops are encrypted and monitored via the mobile device management system, through which they can be remotely managed, locked or deleted when lost or stolen. A strong password policy to protect the devices is applied.

SPAM and Anti-Malware Protection

Only trusted services and devices can be used in the Company. Besides the built-in anti-malware protection of the devices and SPAM filters of the services we use, it is recommended to install antivirus software. All suspicions of malicious software or activity have to be reported immediately.

Access Management

Only entitled employees can grant access to Company systems and accounts. Access rights are kept in evidence and processes of the access rights granting and removal are defined. The access rights are approved based on the need-to-have or need-to-know principles and are regularly reviewed.

Password Security and 2FA

Rules for complexity, length and strength of passwords are defined and are based on up-to-date best practices. It is required to use an approved password manager and 2FA whenever possible.

Security in the Software Development and Code Quality Review

Code edits in production repositories have to be approved in the form of a pull request on GitHub. At least one other developer controls edit quality during such approval process. During each pull request approval, there are also several automatic code quality controls. Our products undergo penetration tests by external and accredited security companies.

System Logs Reports and Monitoring

Logs to the Company systems are recorded and regularly reviewed. All logs are protected by the authorisation check, and only relevant security personnel have access to this information.

Information Classification

Two types of information are defined: Public and Classified. The Classified Information is further divided based on its sensitivity level and the level of protection against disclosure. Rules for information storage, handling and disposal for each classification level are set and have to be followed by all employees.

Prevention of Data Loss

All Company devices with sensitive data are encrypted and managed through the MDM system. Transportation of data via external media is generally restricted. Rules for access management and device protection against malicious software or websites are in place. Additionally, most systems are automatically backed up in the scope of the cloud services we use. The backups are carried out at least daily with data retention of at least three days.

Data Disposal

Rules for secure hardware disposal or reuse and policies for secure data and sensitive information disposal are set. The period of how long the documents and information are stored is generally based on the legislation requirements. Only eligible employees can handle or destroy the data. Disposal logs are recorded.

Vulnerability Management

Vulnerabilities of all Company assets are regularly reviewed. Employees are trained to report all new vulnerabilities immediately after they detect them. If a security vulnerability is detected, it is necessary to install a patch on all affected devices promptly, based on its severity.

Anomalous Activity Monitoring

To detect any abnormal activity in our systems, we monitor logs about activities in our systems. Measures aimed to prevent any suspicious activities are in place.

Business Continuity Management

We establish guidelines to handle possible negative incidents. The rules and procedures are described in the Business Continuity Plan (BCP) and are regularly reviewed and updated if necessary. All employees are trained in the procedures. The BCP's primary goal is to promptly react to such a situation, eliminate potential damages, and prevent the escalation of the negative event.

Scope

Areas that the Business Continuity Plan covers are identified during the process of regular assets inventory review, risk management and risk treatment. Generally, our BCP covers two categories of possible negative events: those related to the physical home-office location and working conditions and those related to data loss or data breach.

Employee Training

The Business Continuity Plan is accessible 24/7 to all company workers, who are also regularly trained about the procedures. The training takes place once in two years and immediately after any change of the BCP. Every new colleague is made familiar with the guidelines during their onboarding process.

Business Continuity Plan Review and Validation

To have the Business Continuity Plan up to date and effective, the BCP is annually reviewed to determine whether it still meets its objectives and is applicable in given situations.

Physical Security

To ensure that all sensitive Company assets are securely stored, rules and policies for their storage are implemented.

All sensitive Company assets (mainly documents and hardware) must be stored in a properly secured location managed by the Company Representative and accessible only to authorised employees. Additionally, all employees are trained to secure their devices and potentially sensitive documents in their home offices. Clear Screen and Clean Desk Policy is applied in the Company.

As for the office, all visitors must always be supervised by the Company Representative or another authorised person during their visit and not left unattended.

Third-Party Validation

An external certified and credible auditor annually reviews our application of the ISO 27001:2013 norm during the surveillance audit. Every three years, we undergo a recertification audit.

Besides the compliance audits, we conduct a penetration test of our solutions. The tests are performed by independent and certified entities. The results are reviewed by the Company Representative and relevant employees and are included in the product development. Our clients may request executive summaries of the penetration test results.

We also welcome our customers to perform a client-side penetration test of our solutions.

Conclusion

Employee safety and information and assets protection for the benefit of customers, owners and other interested parties is a crucial responsibility that Wultra has towards all its stakeholders.

We are committed to continuously improving our employees' safety, and network, premises, data and procedures security. We do our best to prevent damages caused by criminals or careless or irresponsible behaviour. We perform all our activities in a way to protect our employees, information and assets in full compliance with the law and public service bodies.

We are fully aware that it is a long-term commitment that requires continuous improvement of our processes and tech stack regarding security software development, IT technologies and market conditions. We embrace this responsibility and continue to do our best to maintain the trust given to us by our employees, clients, partners, vendors and other interested parties.