anyRM Solutions GmbH
Panoramastr. 1
10178 Berlin, Germany

Website: http://www.anyrm.de
Phone: +49 (0)30 609845 901
info@anyrm.de

INFORMATION SECURITY POLICY

Effective date: September 5, 2023

Table of contents

1. Introduction

This Information Security Policy outlines the principles and guidelines governing information security practices at anyRM Solutions GmbH. anyRM Solutions GmbH has an ethical, legal, and professional duty to ensure that all the information it holds conforms to the principles of confidentiality, integrity, and availability. We must ensure that the information we are responsible for is safeguarded against inappropriate disclosure, is accurate, timely, and attributable, and is available to those who should be able to access it.

anyRM Solutions GmbH has established an Information Security Management System (ISMS) to achieve these goals. One of the central components of an ISMS is the present Information Security Policy document, which the management of anyRM Solutions GmbH has released.

2. Importance of Information Security

At anyRM Solutions GmbH, information security stands as a fundamental benchmark for the quality with which we manage data. Our critical strategic and operational business processes are intricately intertwined with Information Technology (IT). Our primary goal is to ensure the security of data and IT systems, encompassing both technical and commercial dimensions. Equally paramount is our commitment to safeguarding the confidentiality and integrity of both company data and sensitive customer information – a spectrum ranging from employee records to technical documents.

Avoiding incidents that could have a significant financial impact or harm our reputation is a top priority. If our applications encounter disruptions in their proper functioning, it can give rise to substantial challenges. Likewise, any issues pertaining to the accuracy or privacy of the information we utilize are equally of the utmost seriousness. It's important to maintain the availability, confidentiality, and integrity of information, our applications, and IT systems. This imperative extends not only to external threats but also to internal vulnerabilities. Furthermore, a robust information security framework affords us distinctive advantages within the market.

3. Purpose, scope, and users

This Security Policy aims to safeguard information against internal and external threats, ensuring uninterrupted business operations and mitigating potential harm arising from security incidents to a significant degree. Information can manifest in diverse forms, encompassing electronically stored or transmitted data and physical paper documentation.

This policy applies to all employees, contractors, and third-party service providers who have access to anyRM Solution GmbH information assets, regardless of the medium or format in which they are stored. It covers all information assets owned, operated, or controlled by anyRM Solution GmbH, including electronic, physical, and verbal information, as defined in the ISMS Scope Document.

Users of this document are all employees of anyRM Solutions GmbH within the scope of ISMS, as well as relevant external parties.

4. Information Security Objectives

All activities aimed at upholding and enhancing information security are directed towards safeguarding the fundamental values of confidentiality, integrity, and availability of information, with a specific emphasis on our customer data.

Confidentiality: Ensuring that sensitive and confidential information is only accessible to authorized individuals and is protected from unauthorized disclosure.

Integrity: Maintaining information accuracy, consistency, and reliability throughout its lifecycle to prevent unauthorized alteration or tampering.

Availability: Ensuring that information and IT systems are accessible and usable when needed by authorized users while minimizing downtime.

Risk Management: Identifying, assessing, and mitigating information security risks to an acceptable level to protect against potential threats and vulnerabilities.

Compliance: Adhering to relevant laws, regulations, standards, and contractual obligations related to information security.

Incident Response: Establishing procedures to effectively detect, respond to, and recover from security incidents to minimize their impact.

Enhancing the security of our software products: As a software development company, constantly improving the IT security of our products is very important to us. Our goal is to systematically strengthen the knowledge of IT security in our development teams and to establish a cross-team group of experts who advise internally on the secure implementation of new functions and regularly conduct security tests of our software products or have them operated by third parties.

Awareness and Training: Educating employees and stakeholders about information security best practices, policies, and procedures to foster a security-conscious culture.

Continuous Improvement: Regularly reviewing and enhancing our information security management system based on lessons learned, emerging threats, and changes in the business environment.

Third-Party Risk Management: Ensure third-party vendors and partners adhere to the same information security standards to prevent potential vulnerabilities.

Privacy Protection: Safeguarding personal and sensitive data, adhering to privacy regulations, and respecting individuals' rights.

5. Objectives Measurement

anyRM Solutions GmbH will measure the fulfillment of all its objectives. The Chief Information Security Officer is responsible for setting the methods for measuring the achievement of the goals – the measurements will be performed at least once a year, and the Chief Information Security Officer will analyze and evaluate the measurement results and report them to the Managing Director as input materials for the Management Review. The Chief Information Security Officer is responsible for

recording the details about measurement methods, periodicities, and results in the Measurement Report.

6. Fundamental Standards and Security Strategy

The policy is aligned with the ISO/IEC 27001:2022 requirements and based on the IT-Fundamental Protection Methodology (IT-Grundschutz-Methodik) of the German Federal Office for Information Security (BSI).

The security strategy adopted by anyRM Solutions GmbH aims to attain and sustain an appropriate level of security aligned with the associated risks while ensuring efficient resource utilization. An information security management process is being introduced to achieve this goal, drawing from the foundational IT protection principles outlined by the German Federal Office for Information Security (BSI). This approach constitutes a continuous cycle, with particular emphasis on data protection.

This process comprises the following integral steps:

Planning: Defining precise specifications for the security process and the Information Security Management System (ISMS).

Implementation: Establishing the ISMS framework, establishing and executing a comprehensive security concept and security process.

Verification: Assessing the achievement of security objectives to ensure successful outcomes.

Maintenance: Incorporating corrective measures to enhance the efficacy of the security process and the security organization, optimizing the overall system.

This strategy embodies anyRM Solutions GmbH´s commitment to bolstering security while navigating the economic constraints and adhering to the framework provided by BSI, culminating in a safeguarded environment that duly prioritizes data protection.

7. Information Security Organizational Structure

Within the framework of ISMS, the following roles and their corresponding responsibilities are defined:

Company Management: The company's top leadership, represented by the managing director, acknowledges their overarching responsibility for the management and maintenance of the Information Security Management System (ISMS). This entails integrating information security into all business processes, overseeing risk management (including identifying security-critical business processes and information and determining risk-handling strategies), and adopting the information security policy within their respective domains at anyRM Solutions GmbH. The company management commits to providing the necessary financial and human resources to implement essential infrastructure organizational, and technical measures. They are also accountable for ensuring that all employees of anyRM Solutions GmbH and relevant external parties are well-acquainted with this Policy. The company management conducts ISMS reviews at least annually or whenever significant changes arise, with the purpose of evaluating the suitability, adequacy, and effectiveness of the ISMS.

IS Management Team (ISMS Team): To ensure robust information security, anyRM Solutions GmbH has established an IS Management Team (ISMS Team) led by the Information Security Officer (ISO). This team encompasses the Information Security Officer, the Data Protection Officer, the Head of IT, and the IT Team's competent administrative and operational staff. The IS Management Team convenes regular meetings to align and enhance security measures. It holds the authority to define information security policies and monitor their implementation. The team operates under the direct supervision of the managing director and provides routine reports to them. Financial and time resources are allocated to the IS Management Team to facilitate ongoing training and up-to-date knowledge. Team members actively engage in the early stages of IT security-related projects to ensure security aspects are addressed during the planning phase.

Chief Information Security Officer (CISO): The Chief Information Security Officer coordinates ISMS activities and monitors performance. Directly accountable to the managing director, the CISO arranges and conducts information security training and programs to raise employee awareness. The CISO counsels management and pertinent company departments on information security matters and collaborates closely with the Software Development Department. By continuously monitoring technical and organizational advancements in information security, the CISO recommends necessary measures in conjunction with IT management. Additionally, the CISO is engaged from project inception to integrate security-relevant aspects during the planning stage. Any security incidents or vulnerabilities must be reported to the CISO.

Data Protection Officer (DPO): The Data Protection Officer ensures adherence to data protection laws, regulations, and policies, overseeing compliance with the General Data Protection Regulation (GDPR) and other relevant data protection frameworks. They offer expert guidance to the organization, management, and employees on data protection matters. The DPO devises and maintains data protection policies, procedures, and guidelines tailored to the organization's requirements. They ensure that all relevant parties are informed and trained on optimal data protection practices. Collaborating closely with the CISO, the DPO contributes to the organization's overall benefit.

Head of IT: At the forefront of operational IT security, the Head of IT assumes a pivotal role in guaranteeing the secure operation of IT systems and the effective implementation of appropriate security measures. Working closely with the CISO, this role takes into careful consideration the unique aspects and prerequisites of information security. His responsibilities span the deployment of fitting security measures, and he ensures the early involvement of the CISO in all IT projects.

Employees: Each employee at anyRM Solutions GmbH plays a role in upholding information security by exercising responsibility and adhering to relevant laws, regulations, guidelines, policies, instructions, and contractual obligations concerning information security. They diligently manage IT systems, data, and information accurately and responsibly. Asset integrity, availability, and confidentiality rest upon their respective owners. In cases of anomalies, employees must promptly report them to the CISO. Additionally, all users of IT systems at anyRM Solutions GmbH must be acquainted with and adhere to the current Information Security Policy.

8. Information security requirements

This Policy and the entire ISMS comply with legal and regulatory requirements relevant to the organization in the field of information security, as well as with our contractual obligations.

9. Support for ISMS implementation

Hereby, the company management, represented by the Managing Director, declares that ISMS implementation and continual improvement will be supported with the adequate resources to achieve all objectives set in this Policy and satisfy all identified requirements.

10. Document management and effective date

The owner of this document is the Chief Information Security Officer, who must check and, if necessary, update the document at least once a year.

This Information Security Policy of anyRM Solutions GmbH comes into effect on September 4, 2023