RecMan

Information Security Policy

Version	*3.1*
Version date	*2024-08-21*
Created by	*CISO & CTO*
Owner	*CISO*
Reference	*ISO/IEC 27001:2023: A.5.1, 6.2* *SOC 2: CC1.3*
Confidentiality level	*PUBLIC*

Content

1 Purpose and Scope

This policy communicates information security policies and provides a common understanding of RecMan's approach to protecting information and assets. These rules intend to guide clients, contractors, employees, and RecMan. Inappropriate use exposes RecMan to cyber attacks, compromises network systems and services, and creates financial and reputational risk and legal and compliance issues. An Information Security System is a structured approach to protecting RecMan's information and systems from unauthorised access, misuse, or damage. It encompasses policies, procedures, technologies, and controls to maintain data confidentiality, integrity, and availability.

The Information Security Policy is a master document for all company policies and procedures. All other policies aim to support this policy by describing requirements and processes and setting definite rules for ensuring high information security.

This policy applies to the entire company and the information stored, communicated, and processed. All employees, contractors, consultants, and other workers at RecMan and its subsidiaries are responsible for exercising good judgment regarding appropriate information, electronic devices, and network resources by RecMan policies, standards, and local laws and regulations.

This document's target audience includes all RecMan employees, contractors, subcontractors, partners, third-party vendors, clients, and relevant external parties. This encompasses any individual or organisation interacting with or handling information related to RecMan operations.

2 Information Security Roles and Responsibilities

- **The Chief Executive Officer (CEO)** oversees the implementation of legal requirements, communicates information security matters with clients, approves information security objectives and documentation, manages data retention, identifies performance deficiencies, executes disciplinary actions, and manages various HR processes such as candidate hiring and offboarding. The CEO also handles purchasing corporate assets, manages relationships with suppliers and partners, and oversees Disaster Recovery and Business Continuity processes.
- **The Chief Technology Officer (CTO)** provides technical support for security processes, manages data retention, controls access privileges, approves and implements changes, oversees backups and vulnerability management, manages network security, leads security development efforts, defines and tests security requirements, and provides technical expertise during incident response.
- **The Chief Information Security Officer (CISO)** ensures compliance with regulations, determines scope and objectives, measures, controls and implements security processes, updates and approves security documentation, conducts risk assessments, manages teleworking security, provides security awareness training, manages hiring and termination

processes, oversees data classification and erasure, maintains access registries, and supports incident management, audits, and corrective actions.

- **The Information Security Team** plays a vital role in driving Information Security initiatives forward, conducting regular audits to ensure compliance with established procedures for information processing.
- **Asset Owners** are responsible for preserving the integrity, availability, and confidentiality of assets under their control.
- **All employees** must diligently adhere to this Information Security Policy, actively prevent security incidents or vulnerabilities, and promptly report any concerns to the CISO or CTO.

More detailed information can be found in Information Security Responsibilities.

3 Information Security Objectives

RecMan establishes the following objectives for Information Security:

- Provide a secure and reliable cloud-based Software-as-a-Solution for all users who require assurance and confidence that the solution is fit for their purpose and needs
- Promote and motivate a mindset for acknowledging the importance of information security to all interested parties
- Protect the RecMan brand and reputation
- Minimise the impact of potential security incidents
- Prevent the incident recurrence
- Enhance compliance with relevant laws, regulations, and industry standards

CISO is responsible for establishing the methods for measuring the achievement of these objectives. Evaluation will be conducted at least once a year, and the CISO will report the results of these measurements to the CEO and other relevant parties.

CISO is responsible for reviewing the Information Security objectives, documenting them in the Information Security Objectives Plan, and setting new ones annually. All objectives shall be reviewed at least once a year and approved by the CEO.

In addition to setting and measuring objectives, the CISO should evaluate Key Performance Indicators (KPIs) at least annually to ensure a strong security posture. These KPIs should be appropriately documented in the Measurement/KPI Register and communicated to the CEO.

Any company member can propose objectives for security controls or groups of controls. The CEO must review and approve the proposed objectives.

4 Information Security Requirements

The Information Security System must adhere to legal and regulatory requirements relevant to the organisation in the field of information security, ensuring compliance with applicable laws and regulations. Additionally, it must fulfil contractual obligations established with external parties. The document Legal, Regulatory, Contractual and Other Requirements outlines all contractual and legal requirements.

5 Continuous Improvement

RecMan is committed to continuously improving its information security practices. The company conducts various types of analysis to identify discrepancies between current security measures and desired outcomes, following SOC 2 and ISO 27001 security requirements. These analyses contribute to the company's continuous improvement process, where identified gaps are addressed through targeted action plans for enhancement. Multiple sources are utilised for continuous improvement, including incident management, internal and external audits, risk assessments, security assessments, and more. The company ensures alignment with legal and organisational requirements through these integrated processes, fostering ongoing adaptability and excellence in information security practices.

6 Risk Management Strategy

The organisation has established and documented a risk management program that includes guidance on identifying potential threats, rating the significance of the risks associated with the identified threats, and developing mitigation strategies for those risks. More information can be found in Risk Assessment and Risk Treatment Methodology.

7 Security Incident Reporting

All users must promptly report known or suspected security events or incidents, including policy violations and observed security weaknesses. Incidents should be reported immediately or as soon as possible by sending a message or email to the CISO or CTO or completing the appropriate incident reporting form within RecMan. In urgent situations, users are encouraged to call the CISO or CTO directly. When reporting an incident or observation, all relevant details must be provided.

8 Security Awareness Training

The CISO oversees the security awareness training process, which involves developing, implementing, and managing the training program. The general security awareness training program covers onboarding, annual sessions, and specific campaigns on GDPR and privacy, developer training, and policy acknowledgement. It applies to all directly hired employees. The CISO analyses training results to identify knowledge gaps and areas for improvement. For more information, please refer to the Security Awareness Training Policy.

9 Document Management

The owner of this document is the CISO, who must check and, if necessary, update it at least once a year. Additionally, the CISO is responsible for ensuring that all relevant parties know this document and that it aligns with the current organisational processes. Changes to this document shall be exclusively performed by the CISO or an individual appointed explicitly by the CISO for such tasks and approved by the CISO.

10 Disciplinary Actions

Violation of this document may result in disciplinary actions following the Disciplinary Procedure.

11 Version Control

Version	Date	Author	Description of change
1.0	2020-11-18	Gøran Sæland	Issued
1.0	2021-02-17	Gøran Sæland	Updated
1.0	2022-06-16	Lars Vegard Flo	Approved
2.0	2023-07-25	Gøran Sæland	Updated
2.0	2023-08-17	Gøran Sæland	Updated
2.0	2023-08-17	Lars Vegard Flo	Approved
2.1	2024-04-03	Gøran Sæland	Updated
3.0	2024-04-15	Gøran Sæland	Updated
3.0	2024-05-02	Gøran Sæland	Approved
3.1	2024-08-21	Gøran Sæland	Updated
3.1	2024-08-21	Gøran Sæland	Approved