# Hosting and Security Overview

| | |
|---|---|
| **Version** | *4.1* |
| **Version date** | *2024-08-21* |
| **Created by** | *CTO & CISO* |
| **Approved by** | *CTO* |
| **Reference documents** | *Information Security Policy* |
| **Confidentiality level** | *PUBLIC* |

# Content

# 1 Purpose and Scope

This document is a transparent resource, offering a comprehensive overview of RecMan hosting and security practices. Its information is publicly accessible and intended for sharing with all interested parties.

This document has been prepared by Lars Vegard Flo (CTO) and Gøran Sæland (CISO). This document gives a brief technical overview of the application RecMan and its current hosting environment. RecMan is a dynamic application and is constantly making changes regarding technology, partners, and hosting.

# 2 Certifications and Ongoing Improvements

RecMan's infrastructure is GDPR compliant and secured by industry-leading authentication services, ensuring data safety and encryption. We are ISO 27001 certified and have obtained a SOC 2 report from an independent auditor.

# 3 Hosting Providers

RecMan utilises Amazon Web Services, Inc. (AWS) as its hosting provider.

# 4 Security Partners

RecMan collaborates with several security partners, including UnderDefense, Detectify, NetSentries, Nemko, Boulay, CloudNation, AWS, and NST Cyber.

# 5 Data Retention, Destruction, and Management

RecMan has established a robust data retention and destruction policy that complies with regulatory standards and security requirements. Legal requirements, industry regulations, and specific data usage determine the data retention period. Operational data is retained for one year,

confidential data aligns with its intended purpose, and critical data is stored indefinitely. We ensure secure data deletion when contracts end or at the client's request, following strict guidelines. Additionally, we apply strong industry-standard encryption mechanisms to safeguard data in transit and at rest.

# 6 User Authentication

RecMan provides various authentication methods for user access, including traditional username and password authentication, multi-factor authentication (MFA), and single sign-on (SSO) authentication. MFA options include Vipps, BankID Norway, BankID Sweden, BankID Finland, Yubikey (hardware MFA), and SMS codes. SSO options include Azure AD (Microsoft SSO) and Google Workplace (Google SSO).

# 7 Threat Detection and Antivirus

In collaboration with AWS, RecMan ensures robust cloud-based detection and prevention of cybersecurity threats. Every file uploaded to a RecMan account with this feature activated undergoes in-depth scanning to identify and prevent potential threats.

Internally, we implement a multi-layered approach to device and endpoint security. Our Mobile Device Management (MDM) solution enforces security policies and protects corporate devices, while our advanced Endpoint Detection and Response (EDR) solution continuously monitors all endpoints for cyber threats. These systems allow for real-time threat detection, automated incident response, and remote device security management, ensuring the integrity of our infrastructure and protecting our and our clients' data.

# 8 Vulnerability and Patch Management

We take a comprehensive approach to vulnerability management and regularly assess vulnerabilities using code review, external scanning tools, and penetration testing.

Code reviews are conducted, and tools for vulnerability scanning are used, ensuring a thorough assessment of our systems and applications. Identified vulnerabilities are systematically evaluated and prioritised. High and critical vulnerabilities are addressed promptly, while medium, low, or informational vulnerabilities are managed based on a risk-based model. After remediation, we schedule rescan/retests to verify successful mitigation.

We conduct penetration and application testing monthly and with major application releases to ensure ongoing security. We also perform cloud assessments, focusing on cloud-based resources that align with industry-agreed cybersecurity standards. In addition, we monitor and apply patches for our servers with every security release from software and hardware vendors.

# 9 Secure Development Maintenance

RecMan follows a structured development cycle, progressing from the development environment (dev) to the testing environment (stage) and finally to the production environment (prod). All new code is developed in a development environment. When writing new code or making changes to existing code, this is deployed to the test environment where someone other than the programmer who wrote these changes will test these features. When carefully tested and approved, the code is deployed to production.

The development environment contains “dummy data” only. The testing environment will contain dummy data and customer data when needed, but only with the customer's approval.

RecMan has issued procedures for secure information system engineering, both for developing new systems and maintaining existing ones. Developers use VPN to access databases, caching, and data storage during development.

# 10 Backup and Recovery

We use AWS-provided backup solutions, including the RDS database and S3 backup plans. These database backups and S3 bucket files are efficiently managed. Additionally, we export data from our databases to S3 bucket files. Automated daily backups are carried out regularly, ensuring data redundancy across multiple locations. Backups require some time to restore. Backups are snapshots and will delay up to several minutes, depending on location.

In addition to our backup and restore routines, we maintain an Incident Response Plan and Business Continuity and Disaster Recovery Plan (BCDR). These plans are designed to address various scenarios, from database corruption and data breaches to natural disasters, and are regularly tested to ensure their effectiveness. We conduct periodic testing and simulations to assess our readiness to respond to incidents and verify the functionality of our BCDR processes.

# 11 Logging and Monitoring

RecMan has defined logging and monitoring procedures to ensure the security and integrity of its cloud service. We utilise AWS CloudTrail for logging. Logs are initially stored in AWS CloudWatch, each service having its own log group. These logs are aggregated into AWS OpenSearch for centralised log searching, where they are retained for several months. Alert mechanisms are in place to notify the team of critical events based on log content. For more information, see the documentation at AWS.

# 12 Scalability, Flexibility and Availability

We use auto-scaling to adjust the number of instances based on traffic and load requirements. This approach allows us to scale our infrastructure to meet the demands seamlessly. All data centres and zones are located within the EU/EEA, meaning that data is processed, backups are performed, and data is stored at multiple locations. Our locations are mainly in Norway, Sweden, France, Germany, and Ireland, but changes may occur for optimisation reasons and to gain access to new technology.

The RecMan solution is always running on more than one availability zone, meaning that if one zone is experiencing issues - another will immediately take over without the end user noticing. For more information, see the documentation at AWS.

We have essential DDoS protection to mitigate potential threats and ensure the continuous availability of our services.

# 13 Operating Procedures

RecMan has established operating procedures for ICT, including change management. The following process regulates changes to operational or production systems: Changes must be authorised before implementation. Afterwards, changes are thoroughly tested to ensure system stability before being deployed into production. Comprehensive change records are documented throughout the process.

# 14 Security Awareness and Training

RecMan conducts security awareness training sessions for its employees. Developers are also required to undergo appropriate training. Developers participate in external security penetration testing and receive information from UnderDefense about best practices for the development lifecycle. Quality Assurance (QA) staff undergo training from UnderDefense to gain knowledge about basic security testing and how to use automated tools in the development lifecycle.

# 15 Document Management

The CTO owns this document and must check and, if necessary, update it at least once a year.

# 16 Version Control

| Version | Date | Author | Description of change |
|---|---|---|---|
| 1.0 | 2018-03-20 | Lars Vegard Flo | Issued |
| 2.0 | 2019-10-25 | Lars Vegard Flo | Updated |
| 3.0 | 2021-08-18 | Gøran Sæland | Updated |
| 3.0 | 2022-09-05 | Lars Vegard Flo | Approved |
| 3.1 | 2023-03-14 | Gøran Sæland | Updated |
| 3.1 | 2023-03-14 | Lars Vegard Flo | Approved |
| 4.0 | 2023-10-16 | Gøran Sæland | Updated |
| 4.0 | 2023-11-07 | Lars Vegard Flo | Approved |
| 4.1 | 2024-08-21 | Gøran Sæland | Updated |
| 4.1 | 2024-08-21 | Lars Vegard Flo | Approved |