

# Security at Merinio

## Overview

Merinio is a tech company working to disrupt human resource management and shift replacement workflows in companies with over 50 employees. We replace an error-prone human centric process with an intelligent automated SaaS-based alternative. Our company provides transparency, efficiency and security by implementing the most recent advancements in security wherever possible.

## Organizational security

As an operations management platform, ensuring the most secure environment possible is of the utmost importance. We need our customers to feel safe using the platform in order to revolutionize their management. At Merinio, we take the relevant precautions.

All employees and founders must sign confidentiality agreements, pass a rigorous vetting process and be up to date in the relevant security threats related to their position in the company before being given access to any company system. Employees and founders are kept informed of the latest vulnerabilities and security requirements by a peer to peer training process and all employees are required to contribute to the training of the team.

Employees must use an approved password management application and generate complex passwords for any interaction with company systems.

Upon termination, all accesses are immediately revoked.

## Application Security and Reliability

The platform is based on a containerized production environment using images built in-house as well as multi-zone availability with automatic failover, providing uptime as detailed in the service agreement.

The latest encryption protocols available to the customer are always used and the platform can only be accessed over a secure HTTPS connection.

All source code belonging to the platform and any relevant admin tools are checked in regularly to a version-controlled repository. All changes are subject to peer review and automated continuous

integration testing before any code is merged to the production version of the platform. Static analysis is used to detect potential bugs and vulnerabilities.

During the normal course of operation, the production platform will encounter issues that could not have been detected in a development environment. Merinio takes all relevant steps in order to minimize downtime and accelerate resolution of all reports of degraded service.

Error tracking platforms are used with real time interfaces, ensuring that the operations team always has enough information to react quickly and efficiently. All interactions with the platform are logged with detailed information, enabling easy reproduction of any situation.

Access to the platform is regulated using industry standard token based authentication, all connections to the API must be accompanied by a signed token, preventing forged credentials and unauthorized access. Tokens expire regularly and must be refreshed often, minimizing the risk of credential hijacking. Administrative access by Merinio employees and founders is protected by a combination of multi-factor authentication and a standard credential pair.

All storage volumes for the database are encrypted and protected by SCRAM-SHA1 authorization. TLS/SSL encryption is used for all connections, ensuring customer data is always encrypted in transit. Logical divisions between different customers prevent any cross-access of data as well as information stored in any form. Multiple daily backups as well as multiple availability zone replicas ensure that customer data can always be restored in the event of a disaster.

To operate efficiently and reliably, Merinio relies on 3<sup>rd</sup> party suppliers. All suppliers where a potential risk is possible are thoroughly analyzed in order to ensure their reliability and security practices. Merinio takes appropriate steps to ensure that all suppliers maintain an acceptable level of security.

## Conclusion

At Merinio, security is a primary concern because our users expect nothing less than the most secure and confidential platform for their data. We take the responsibility of protecting this data with pride and do our best in all facets of our operation to maintain the trust of our users.