Impero Security Whitepaper

TABLE OF CONTENTS

INTRODUCTION

Impero is a Danish company founded in 2013 and based out of Aarhus, Denmark. We develop and deliver a Software-as-a-Service solution for managing Risk and Compliance. The software is referred to as Impero or the solution.

Impero operates with distributed teams having employees in Denmark, France, Germany, and UK.

With the multiple locations and many activities off site there is a strong focus on securing the company devices and data through strong mobile device management, and the company resources that are hosted by Microsoft Azure and Microsoft O365. Control objectives and control activities at Microsoft are not covered by this report.

Security is a crucial part of our solution, and is reflected in our people, processes, and way of working. This document explains how we provide security to our customers and protect their data.

ORGANIZATIONAL SECURITY

Employee background checks

Each employee undergoes a process of background verification. We scrutinize their criminal records, previous employment records if any, and educational background. Until this check is performed, the employee is not granted access to sensitive information.

Security awareness

Each employee, when inducted, signs a confidentiality agreement and acceptable use policy, after which they undergo training in information security, privacy, and compliance.

We provide training on specific aspects of security, that they may require based on their roles. We educate our employees continually on information security, privacy and keep them updated regarding the security practices of the organization.

Working with external consultants and third parties

External consultants and third parties that requires access to Impero's company resources are also enrolled in Impero's security awareness program.

PROTECTING CUSTOMER DATA

Secure by design

Security plays a vital role in Impero's development lifecycle. Before any code is deployed to our production environments, a number of security measures has been taken.

- All our developers have in-depth knowledge of and conform to OWASP in their everyday work.
- All code is subject to code review
- A series of unit and integration tests have to run successfully
- Release candidates are thoroughly tested by Impero's test team
- Segregation of duty is enforced in a number of areas, e.g. developers do not have access to the production environment
- Impero's frontend and backend codebases are coded in languages with a high level of type safety (Typescript and Rust), which by design helps reducing the number of software defects
- Linkage between committed code and related user stories in our development management solutions ensures full traceability

Encryption

Encryption in transit

Impero uses the highest recommended standards of encryption. All data transiting between the Impero servers and the client's browser is encrypted using TLS 1.2, with only the most secure ciphers enabled (AES encryption and SHA-256 signatures as a minimum). This comes at the expense of compatibility with legacy browsers like older versions of Internet Explorer but ensures maximum protection of the traffic.

Encryption at rest

Impero stores data both in a Postgres relational database and in the Azure blob storage (for uploaded files). Both are encrypted using the AES-256 cipher by our hosting provider Azure.

Password storage

Passwords are not stored in the database. A hashed, salted version of the password (using the Argon 2 cryptographic hash algorithm) is saved instead. In addition, a pepper (server-side secret, site-wide) is used to generate the hash. The pepper is stored on a separate server from the database.

Web application security

Authentication

Impero users may, depending on company policy, authenticate using:

- Login + password
- Login + two-factor authentication (password + SMS)
- Single sign-on SSO (based on OpenID Connect)

Passwords are subject to complexity requirements. Should an organization elect to use 2-factor authentication, the application will send a random 4-letter code (which will expire in one minute).

Session management

The application saves session information in cookies. Cookies are only accessible over an encrypted connection, and the cookie containing the session identifier is not available from browser-side scripts.

A server-side session registry ensures that users only access the application using a single browser at a time, mitigating the risk of users forgetting to close a session on a public terminal. In addition, sessions with no activity are invalidated (the user needs to login) after 60 minutes.

XSS attacks

Impero relies on the React rendering library for most of its user interface. This protects the application from most XSS attacks. Some legacy parts of the application use a server-side templating system with built-in escaping, as well as client-side escaping.

SQL injection

Impero uses an SQL query builder which generates parametrized SQL queries. In addition, hand-written SQL is thoroughly reviewed and is also parametrized.

External security validation

Web application security assessment

Assessments are conducted periodically by a leading external provider. The assessment covers all relevant aspects of security within the solution and the deployed environment. Any potential findings are reviewed, and mitigation plans are initiated. Following mitigation, a verification test is performed. Amongst others the assessments ensure that we have adequate safeguards within the following areas:

- SQL Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- Security Misconfiguration
- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Using Known Vulnerable Components
- Logging and Monitoring

Security compliance audits

An ISAE 3000 statement on the IT general computer controls operated (ITGC) by Impero is prepared annually by an external audit partner. Part of the internal controls performed by Impero is a review of relevant audit statements covering the Azure resources. Among these statements is the SoC2 report that covers but is not limited to:

- Backup and restore
- Infrastructure
- Firewall
- Patching
- Anti-Virus
- Physical Security

Hosting

Hosting is provided by the Azure cloud. This includes both the web application, any additional services such as logging, and all stored data.

Network security

Impero is hosted on virtual machines provided by Azure, using different operating systems. All servers have systems for automatically applying security patches and rebooting if necessary.

Impero servers sit behind a firewall. Only necessary ports are open. In the network behind the firewall, all traffic is end-to-end encrypted (including connections to the database). Servers themselves use a secure configuration, with only necessary services enabled, and rely on SSH keys for remote login (when the operating system is compatible).

Monitoring and logging

Impero stores logs for different purposes, both at server-, web server software- and application-level. These logs can be used for tracking customer issues or identifying malicious activity. In addition, Impero relies on Azure's monitoring features and in particular its Security Center.

Device and access management

Impero requires all devices enrolled in the companies MDM solution before getting access to company resources. This goes for workstations as well as smart devices. The MDM solutions ensure that the devices comply with the security standards set forth by Impero and enforces continues monitoring. Impero's security policies are comprehensive and include requirements such as:

- Encryption at rest on all devices
- Up-to-date anti-malware software and antivirus protection
- Compliance with the password policy
- Use of a long pin and locking when idle for smart devices

Access to company resources is granted on the principle of least privilege and role-based permission and should always reflected the job responsibility. Access rights are subject to recertification.

For further risk mitigation, Impero enforces multi-factor authentication in order to access company resources including the Azure environments.

Responding to Security Incidents

Impero has established policies and procedures addressing security incidents.
There are additional procedures in place dealing with violations of information security policies, software malfunctions or security weaknesses.

In case of an incident, affected customers will be contacted by the Impero Customer Success Team.

CONCLUSION

Impero always strives to have the best security posture. We continually look out for improvements to our development practices and security processes, in order to deliver the most secure solution to you and keep your data safe. For any additional queries in relation to this document please don't hesitate to contact support@impero.com.