Sherpany Security Whitepaper

SHERPANY

www.sherpany.com

Table of contents

Abbreviations

Abbreviation	Full Term
GDPR	General Data Protection Regulation
FINMA	Swiss Financial Market Supervisory Authority
ISAE	International Standard on Assurance Engagements
ISMS	Information Security Management System
ISO	International Standards Organization

Authors

This document was created by Marc Walzer and Mathias Brenner.

Name	Marc Walzer	Mathias Brenner
Role	Security and Data Protection Officer	CTO
E-Mail	marc.walzer@sherpany.com	mathias.brenner@sherpany.com
Phone	+41 44 515 89 50	+41 44 515 89 69

Document Purpose and Structure

The typical user of the Boardroom services entrusts us with very sensitive information. Therefore invest heavily in the security and resiliency of our infrastructure, application and business operations.

We recognize that security has to be integrated across the company within the development lifecycle, the IT-operations and the business processes. This paper outlines some of the measures and processes that are in place to safeguard the valuable information of our customers.

It starts with a description of our End-to-End Security approach where we the reader is guided along the path of an uploaded document, once it enters the highly secured environment of the Boardroom solution. Subsequent are the organizational measures we have implemented in our IT as well as our Business departments in order to achieve the ISO 27001, ISAE 3000 Type II and FINMA Outsourcing certifications. Finally, we look at our set-up which allows us to reach a guaranteed availability of 99.9%.

End-to-End Security Approach

In our experience the easiest way to understand our security concept is, if we start along our use-case with the login-process and then follow the file on its way through our cloud onto the different devices of the end-users.

2-Factor-Authentication

To mitigate the risk of unauthorized access to a Sherpany account, a second factor - beside the password - is required in order to authenticate for the Boardroom application. While we offer the broadly used option of an SMS token which is sent to the mobile phone associated with the user, we recommend to our customers to use the innovative, more secure and very convenient alternative named SoundProof. This is a mobile phone-based two-factor authentication solution which does not require the user to interact with his phone (zero-touch). It works by by comparing the unique ambient sounds as they are captured for 3 seconds by the two devices at the time of login.
This zero-touch approach authenticates the user securely and conveniently within a few seconds.

Strong Password and Login Policy

We do not solely rely on the significant advantages the 2-Factor-Authentication provides and thus have implemented supporting measures to protect the user-accounts. They include:

- Enforced requirement to chose a strong password
- Overall maximum session duration
- Locking of accounts after several unsuccessful login attempts
- Active monitoring of suspicious login activities
- Strong encryption of stored user-credentials
- Possibility for IP-Whitelisting for access to individual boardrooms

Secure and Platform Independent Access

The Sherpany Boardroom is accessible via a variety of user-interfaces. The possibility to login via browser enables the customer to access our service platform independent and without having to install anything. Additionally there is a iOS and Windows app available. The native mobile apps are optimized for the respective devices and give the possibility to work offline aswell. All applications have been developed with a strong focus on security and locally stored information is protected through multiple layers of encryption.

Data in Transit

Once you have securely logged in, you can upload your file. While upload itself is simple from the user's perspective, behind the scenes the Sherpany Boardroom is working to optimize the performance and security of data in transit.

Any information including user and login data (email address, password) and documents (download, upload) that is transmitted from a device to Sherpany servers (and back) is protected through SSL-TLS-256 encryption. To prevent man-in-the-middle-attacks, we use certificate pinning.

The Sherpany Cloud

Once the information has reached the Sherpany cloud, it is subject to a very strict logical data-separation in combination with very restrictive permissioning. As an additional layer of security, every file is encrypted with military grade encryption methods and an individual encryption-key, which is stored in a dedicated environment named the Sherpany Vault. This highly secure solution stores and tightly controls access to tokens, passwords and certificates, as well as encryption keys and handles leasing, key revocation, key rolling and auditing. Access to the Vault is logged, monitored, audited and limited to selected employees who undergo comprehensive background checks.

Our infrastructure runs on Openshift by Redhat Enterprise. Built on containers, it inherits the significant security advantages that come with their strict modularization. Within this highly scalable and already out of the box very secure environment, we run further top-notch **security solutions** as for example:

- ModSecurity Web Application Firewall (deployed as Reverse Proxy)
- Security Information and Event Management System
- Intrusion Detection and Prevention System
- Next-Generation-Antivirus
- DDOS mitigation

In collaboration with our Threat Intelligence Team, DevOps and SecOps maintain and improve the security of our cloud on a daily basis.

In terms of availability our high-performance-setup offers a great amount of flexibility, scalability and resiliency. On top of the physical redundancies which are outlined below, we have several logical measures in place to ensure our availability of 99.8%. These include:

- Redundant load balancers and computing nodes
- Master/slave database clusters, replicated in real-time across data centers
- Resilient storage technologies
- Multiple log databases replicated in real-time across data centers
- Segmented clusters of application servers handling different functions
- Infrastructure that enables updates without downtimes
- Easily scalable hardware and software setup

Audit Trail

The Sherpany Boardroom automatically logs all file and user activities and maintains a complete audittrail of all activity within an account. The log entries are date/time stamped, tracked by username, IP address and action taken. We provide this logs through a functionality called auditor-self-service which enables us to deliver the audit log not solely to the administrator but also to other roles like auditor or information security officers. This concept is a big advantage in terms of security and compliance, because it supports the 4-eyes-principle by default.

Backup, Replication and Disaster Recovery

In order to be able to deliver a high availability and fast recovery-times and with the knowledge that business continuity is important to our customers, the environment of the Boardroom solution runs on a geo-redundant setup. This means that not only our hardware is resilient to device failure, but with two redundant and geographically independent data centers we are prepared to lose a whole data-center without any major downtime. Additionally to the replication between the two sites, we backup our data daily and are able to restore it at any given time.

Remember that backups are protected througt encryption and stored in a secure environment.

To be prepared for disaster scenarios not only on a technical level, we regularly perform failover and restore tests.

Independent assurance

We do not expect our customers to blindly trust us in terms of security. Therefore we work together with industry leaders in security and undergo regular audits through independent auditors. Among our partners are:

Partner	Area
Ernst & Young	Security Testing
Redguard AG Security	Security Testing
Cobalt Labs Inc. Security	Security Testing
GoSecurity GmBh	Consulting
TÜV SÜD	Audit
BDO Switzerland	Audit

Additionally we are an active member of the Information Security Society Switzerland (ISSS). We use this platform to exchange know-how and best-practices with other security enthusiasts and/or members of our industry.

Sherpany holds the following certifications:

ISO 27001

ISO/IEC 27001:2013 (ISO 27001) is the international standard that describes best practice for an ISMS (information security management system). Achieving accredited certification to ISO 27001 demonstrates that a company is following information security best practice, and provides an independent, expert verification that information security is managed in line with international best practice and business objectives.

An ISMS is a system of processes, documents, technology and people that helps to manage, monitor, audit and improve your organisation’s information security. It helps you manage all your security practices in one place, consistently and cost-effectively. At the heart of an ISO 27001-compliant ISMS is business-driven risk assessments, which means you will be able to identify and treat security threats according to your organisation’s risk appetite and tolerance.

When most cloud companies talk about ISO 27001 certification, they’re talking about the data centers that they hire to host their services. Obviously, it is critical that these data centers meet high standards for security and availability. At Sherpany, we maintain the ISO 27001 certification and audits for the development, maintenance and operation of our plattform as well, beyond the hosted data centers. So, we’re ISO 27001 throughout the stack – something that few other cloud-based service companies can boast.

ISAE 3000 Type II

ISAE 3000 is the assurance standard for compliance, sustainability and outsourcing audits. Service organization report on how they deal with security, privacy or fraud by an ISAE 3000 report containing information on the internal processes and controls. The ISAE 3000 report is audited by professional audit firms to provide assurance that the controls included are actually in place and operate effectively. From 2015 on Sherpany is being audited and certified annually by BDO Switzerland. Sherpany undergoes an comprehensive audit annually and is then obligated to provide proof of compliance with the ISAE 3000 report.

FINMA Outsourcing

FINMA is Switzerland's independent financial-markets regulator. It is charged with protecting creditors, investors and policyholders. FINMA is responsible for ensuring that Switzerland's financial markets function effectively. Its circular regarding outsourcing affects banks and insurances and consists of eight main requirements which address a variety of topics including security, banking secrecy and audit. As many of our customers are are subject to the FINMA regulations and thus need to comply to its outsourcing requirements, we have decided to make their life easier and let ourselves certify by an independent auditor (BDO Switzerland). This saves us and our customers valuable time, since we do not have to proof our compliance in every individual case.

Security Testing

Since we do not only want to rely on our skilled developers, mature development lifecycle and quality assurance processes, we mandate multiple independent security auditors to perform penetration tests on a regular basis. This is not only a very valuable investment in the security of our service, but it also covers various compliance requirements of our customers.

On top of the security testing that we mandate on a regular basis, we offer our customers to perform their own pentests of the Sherpany plattform. This does result in a better assurance for the respective customer and an overall higher security level of our service.

Sherpany Secure Development Lifecycle

Ultimately, a commitment to security has to start with the software development process itself. Therefore we have implemented DevSecOps into our development lifecycle. This means that our Development Team, DevOps, SecOps and the CISO department work hand in hand to introduce security already very early in the development process. As a result, we can eliminate or identify weaknesses right where they arise - in the code.

These are some of the security controls which grew out the cross department collaboration into our development lifecycle:

- Highly skilled developers with a good understanding of security
- On the job training for our developers (internal/ external trainings, conferences, collaboration with the community, ...)
- Regular security trainings which cover the OWASP top 10 among other things
- Code reviews (4-eyes-principle)
- Automated testing
- Manual testing through our QA team
- Integration tests
- User acceptance tests
- Weekly vulnerability assessments
- Several penetration tests of all our application during the year
- Annual infrastructure penetration test

Data Center Security

Both data centers are located in Switzerland and offer a top-notch hosting environment with multiple layers of security. Our customers benefit from this locations, because of Switzerlands political and financial stability, modern infrastructure as well as strict and business friendly legislation.

To prevent unauthorized access to the provided infrastructure, the data center providers have implemented extensive physical security measures. These include:

- All equipment is secured within locked cages or vaults
- Multiple layers of access controls including but not limited to keys, ID, biometric scanning
- 24-hour onsite monitoring and guards
- Mantraps
- Bulletproof windows
- CCTV with video archives
- Access control lists
- Access and surveillance audit logs

On top of the outstanding security level the data centers provide, there are various measures in place to ensure a very high availability. These include:

- A redundancy for all critical components, including cooling systems, power, internet providers, connectivity, and other essential systems.
- Uninterruptible power supply
- Emergency backup generators
- Advanced fire suppression
- Flood control

Both locations are ISO 27001 certified which guarantees sufficient control and independent audit through the supply-chain.

Sherpany Information Security Framework

As it is important to not only rely on technical security measures, we have implemented an sophisticated control/process framework to protect our valuable information also on an organizational layer. A few highlights of this layer are:

- A formal incident management process that ensures an effective and efficient reaction and compliance with contractual and regulatory requirements
- A formal incident communication process, which ensures that all stakeholders are properly informed
- Background checks on all our employees
- Awareness trainings across the whole company to create a basic understanding of information security
- Social engineering tests to prepare the staff for possible social engineering threats
- A whistleblower policy to ensure that concerns are handled appropriately
- Regular access reviews
- Regular trainings of crisis situations

Access to customer data

Sherpany Customer Support or Engineering may occasionally need access to some of your data to provide support and address technical issues. Here, too, we have policies and controls in place to strictly limit that access to the least access necessary to provide superior support (a “least privilege” strategy).

Sherpay carefully enforces role-based segregation of access and the 4-eyes-principle. For example, access to customer data is limited to specific and carefully selected employees, and includes limited views, such as:

- Ability to see the metadata, but not the content of a Boardroom
- Ability to edit and view user account information (contact info, account status), but not files.

Exceptions to role-based access policies may be granted on a case-by-case basis and strictly following the four-eye principle. All customer data access is always logged, monitored and audited.

Compliance

As a Swiss company with several customers from the heavily regulated financial industry, we are well aware of the compliance requirements which affect us and our customers. With the knowledge of the importance of this topic and many years of experience, we have grown to a compliance specialist in our area of work. Thus we have developed several tools that help us to meet the compliance requirements we face in a very efficient and effective way. Some of our almost daily faced cases are:

- GDPR
- Local data protection laws
- FINMA regulations
- Banking secrecy