simplifire

This Data Security Policy should take you less than 10 minutes to read!

What is the purpose of this document?

This document outlines how Simplifire protects itself from threats, including computer security threats, and how it handles situations when they do occur.

Other questions that will be answered from here:

1. What is Simplifire's high-level approach to data security?

Simplifire uses a highly secure cloud infrastructure-as-a-service platform that is certified to broadly regarded IT security standards ISO 9001 and ISO 27001. The data center and all infrastructure used by Simplifire are based in Switzerland. Our activities are also fully in line with Swiss data protection legislation, as well as the relevant laws of the European Union.

Simplifire has security measures aimed in particular at:

- Protecting data confidentiality
- Guaranteeing its integrity
- Auditing key transaction points.

Simplifire security is based on several measures:

2. How is the setting up of an account authorized?

Verification is performed by referencing a security table located in a remote and secure database, "Authoritative", meaning the authority to view certain sections of Simplifire, is based on company, user, role, data and data status.

For Groups, Simplifire registers a single superuser for each company ("the Group Coordinator"). Further registrations are handled internally by the client company, using administration facilities provided by Simplifire. This means that ex employees can be removed from the Group and will no longer have access to their accounts.

For individual users not within a Group, or companies with a single user, that individual or single user has the same access rights as a Group Coordinator.

3. What is "authentication" and how does Simplifire use it to limit the risk of someone else accessing your account?

Authentication is a means of ensuring that the visitor to a site is actually who (s)he claims to be. It also allows the platform to assign the correct access rights to that visitor. Access rights affect what a user can and cannot do on the platform. In Simplifire for example, (s)he may be allowed to set up a contract with users within his/her Partner network, but (s)he may not be allowed to set up a contract with users outside of his or her network.

The authentication process in Simplifire is based on a User ID and password. User ID is the User's email address. Before Simplifire allows activation of the account, it verifies that the email address exists and is available to the User.

Simplifire guides the first-time User by guiding password choices. The User may at any time change his/her password in the system. Each time, the password is tested to ensure it:

These multiple quality criteria are designed to make the password difficult to guess by outsiders. Simplifire does not store Users' passwords in plain text. Instead it makes use of a one-way encryption function that receives a string as input (in our case the password) and generates another, random looking string. The generation (one-way-encryption) is such that it is impossible to return from the results of the input (and therefore to expose a password). Only encrypted form of a password is stored by Simplifire. Therefore, it is not possible for the Simplifire team to read it. In case the password is lost or forgotten, the User can reset it (delete previous password and provide a new one) using the email address given during registration process.

Users can also choose enhanced protection for their account, by opting in to so called two factor authentication (2FA). 2FA in Simplifire is implemented using time-based one-time passwords (TOTP) and requires having any kind of TOTP aware app on their mobile phones (like 'Google authenticator', Authy, 'Microsoft Authenticator', 'LastPass', '1Password' etc.)

When you try to log in, you are then put through the following authentication process:

In this way we work together to reduce the risk of wrong authentication by ensuring that only a person meeting the following qualifications can log in to Simplifire:

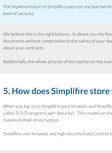
4. What is encryption and how does Simplifire use it to preserve confidentiality?

Encryption is the process of modifying text or data into a form unreadable to anyone without a proper key or password. There are many ways to encrypt information which rely on different algorithms and formulae.

In Simplifire, all your contract documents are stored in encrypted form, using up to date encryption technology. This means that unless someone gains access to your account (by compromising your password and mobile) they will not be able to read any of your documents in the database, since they are not stored there in human-readable form. Simplifire uses a number of encryption keys so that you can share the content of your contracts only with the people you choose. It reduces the chance of attacks as there is not a single specific key to break and get access to all the information.

The approach used to encrypt contract data is based on a method called «Pretty Good Privacy», or PGP. This is a time tested and proven method of protecting e-mail communication, end-to-end. In Simplifire this means that every platform User has two, correlated cryptographic keys generated for it during registration. They are called 'public and 'private' keys. With this, Simplifire allows a sender to encrypt the data they are sending in a way that only allows the intended recipient person to decrypt the content.

Imagine User A is trying to send a contract to User B in a way, that no-one else can read it. With the use of a public/private key pair, User A encrypts the content with public key of User B, and from that moment only User B, who has his private key, can decrypt it.



The implementation in Simplifire uses not one but two levels of encryption and additional cryptographic keys to further enhance the level of security.

We believe this is the right balance. It allows you the flexibility of sharing your contract with someone, and of text mining your documents without compromise to the safety of your documents from third parties with whom you do not want to share information about your contracts.

Additionally, the whole process of encryption or key management is transparent for you, the User.

5. How does Simplifire store your data?

When you log on to Simplifire, your browser and Simplifire servers initiate a secure pipeline for communication using a technology called TLS (Transport Layer Security). This creates an encrypted 'stream of data travelling from your browser to Simplifire at the maximum level of encryption.

Simplifire uses firewalls and high security Data Centres to store and operate its servers.

6. Does Simplifire use cookies and how are they protected?

Both the Simplifire platform and the website use cookies to perform login processes and to maintain the User session. With security in mind, Simplifire has been built in such a way that it does not store any data in that cookie, just an ID. Every piece of information is stored only on the server and encrypted, and does not travel backwards and forwards between client and server.

7. How does Simplifire stay up-to-date on data security?

All systems are regularly updated with the latest operating system vendor security patches. In that way, our Information Management System is continually improved. We also conduct annually a risk assessment of Simplifire's cyber security resilience, benchmarked against best practice security standards. The process results in mitigation measures and the revision of controls to respond to technological developments and evolving threats. It considers particular risks of Simplifire's business operations related to cyber security, our business information collected or stored, our IT landscape, and the availability and effectiveness of controls to protect information and IT landscape.

8. How would Simplifire respond to an incident?

In the event of security or privacy incidents that may implicate unauthorised access to your data, we have in place an Incident Response Plan, including appropriate reporting channels, such as 24/7 contact lines. Our breach detection and containment procedures entail assessing whether the breach could have consequences for Users and determining who needs to be notified of the breach, including individual data subjects, or other stakeholders. To this end, we use the most effective communication channels depending on the severity and scale of the breach, including our public website when appropriate. We involve all relevant internal and external stakeholders in our attempt to minimise the harm to Simplifire and affected individuals. We monitor the threat environment and have prepared lines of communication both internally and externally. Our plans aim to mitigate and resolve such incidents in order to minimise harm to the company and to data subjects.

9. I am outside of Switzerland - can I use Simplifire legally without violating encryption export restrictions?

Use of Simplifire does not require the export of any encryption technology. Users simply require a browser and Internet connection.

10. Can this Policy be amended without you being told?

Yes, it can and it will be. Our approach to Data Security is key to our business, and we will keep challenging ourselves. Simplifire will from time to time amend this Security Policy and will do so routinely on an annual basis. If there are material changes to it, Platform Users will be informed in platform, and the Security Policy will be re-published on the Website.

11. How do you consent to this Policy?

By using the Simplifire Services or the Website, you consent to Simplifire's Security Policy.

12. How can you contact us?

Notices@Simplifire.world

13. Latest revision date

Latest revision date of this document is 1 February 2020.

14. Technical footnote 1: technical specification of the encryption in Simplifire

For hashing (one way encryption) the Argon2 algorithm is used (winner of 2015 hashing algorithm contest and highly regarded algorithm). In two-way encryption implementations are based on Elliptic Curve Diffie Hellman.

Simplifire forces Users to use at least 12-character passwords. The required length and the possibility to use not only alphanumeric characters, but also special characters lets Users create strong passwords. To put that in perspective, to 'guess' a12-char password which has letters+numbers and special character on todays personal computer, using 'brute force' computing power would take over 500 years straight.

For internal operations and encryption key management, Simplifire is using even more complicated passwords, meaning that today's personal computer would need thousands of billions of years to brute force the answer.

15. Technical footnote 2: operating protocols used by Simplifire

Communication between Simplifire clients and the application is based on the HTTP/1.1 Internet standard. The customer initiates a connection through an HTTPS request, the connection uses 128-bit TLS encryption when accessing any area within the application. The TLS protocol ensures communications security in three ways:

1. The identity of the communicating servers must be known.
2. Powerful algorithms detect truncated or tampered data.
3. The content sent is encrypted and therefore private.

Transactions with Simplifire are encrypted automatically and secured with 128 bits. By using this state-of-the-art encryption function and corresponding strong algorithms, your confidential data stay confidential and unaltered when sent over the Internet.