SECURITY MEASURES SOURCE.AG

1. **INTRODUCTION**

At Source.ag, we place significant importance on information security to protect against unauthorized access, use, disclosure, alteration, and destruction of data, from both external threats and malicious insiders. We prioritize safeguards that ensure confidentiality including privacy, integrity, and availability of information, and continuously strive to maintain industry's information security best practices and apply controls to protect our clients and ourselves. To this end, we maintain a comprehensive cybersecurity program structured around the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)[1]. We employ a Defense in Depth strategy that covers all layers of both our software development & delivery process as well as our operational & business processes.

This Schedule E (Security Measures) acts as a supplement to the Agreement between the Customer and Source.ag. In the event of conflict between this Schedule and the body of the Agreement, the latter shall prevail. Capitalized terms used herein that are not defined shall have the meaning set forth in the Agreement. We review our security measures and policies continually, including through external auditing. This document is reviewed accordingly.

The goal of this document is to provide high-level insights of our approach to information security and practices to secure data, systems, and services. Security measures are continuously evolving, and as such, additional measures can be implemented at Source.ag's discretion.

2. **ASSETS & NETWORK SECURITY**

At Source.ag, we have developed an organizational understanding and implemented measures to manage security risk regarding systems, assets, data, and capabilities, enabling awareness, and business continuity, starting with measures that protect our assets and network.

- Proven industry-standard encryption methods and cryptographic tooling (e.g. TLS 1.3/HTTPS), are leveraged to secure systems and Services.
- Network(s) are segmented, and infrastructure is kept up to date.
- Industry standard firewalls are in place to manage and limit access to Source.ag's cloud environment, SaaS-solutions including all systems and data storage infrastructure.
- All computing resources with internet access are limited and protected.
- Authentication between applications and databases in respect of the Services is executed through secret keys that are frequently rotated to limit risk of credential leakage.
- Source.ag's (third party) cloud environment is segregated into multiple separate accounts to limit impact of security incidents in one environment (e.g., development) on other environments (e.g., production).
- Development and testing of new features and bug fixes only takes place in environments that are completely separated from the production environment, effectively separating production and non-production environments.
- All code that is deployed to production has been reviewed and approved by at least one of our senior developers.
- Automated tests and checks are run for each code change before it gets accepted into the main code base.
- Access to our production systems is limited to senior developers only.
- A secure configuration process for network infrastructure and Source.ag's assets is in place through peer-reviewed infrastructure-code, and is updated as changes occur.
- Assets and software are securely managed, by means of version control and allowing access to administrative interfaces only over secure network protocols, such as SSH and HTTPS.
- Automatic patch management is in place for operating systems and applications, and performed by a third party on a monthly basis at the minimum.

[1] For more information about the NIST Cyber Security Framework got to

- We run automated vulnerability scans on our software dependencies to catch Common Vulnerabilities and Exposures (CVEs) and patch these as soon as reasonably possible.
- An audit log management process is in place, in which the collection and retention of audit logs is defined for all of Source.ag's assets, including adequate storage and maintenance.
- All laptops used by Source employees are managed by an industry-standard Mobile Device Management solution and security measures on the laptops are enforced following best practices set by CIS[2].
- All laptops by Source employees are protected by industry-standard endpoint protection.
- All data on all laptops is encrypted.

3. **DATA PROTECTION & PRIVACY**

At Source.ag, we prioritize privacy and data security, and do our utmost to prevent unauthorized access or modification to our systems and data. To that end, we have developed and implemented safeguards to ensure delivery of services and prevent security incidents from taking place, accounting for people, process, and technology.

- All Customer Data is stored in data centers operated by Amazon Web Services located in Germany. Some critical network infrastructure - but no Customer Data - is located in data centers operated by AWS in the United States.
- Segmentation is in place for Customer Data, which is also stored separately from the cloud resources needed for day-to-day operations and is accessible on a per-use-case basis.
- Raw data of different Customers is stored separately.
- Communication between the Customer's systems and Source.ag's systems are protected using industry best practices for encryption.
- As much as reasonably possible and without negatively impacting the functionality of the Services, all Customer Data is encrypted at rest.
- All removable media and end-user devices are encrypted.
- In case of loss or theft of employees' end-user devices, mechanisms are in place for swift reporting and remote wiping, and relevant accounts are promptly disabled, followed by mandatory password changes.

4. **SECURITY OF SERVICES**

Your data is only as secure as our Services through which you provide and use that data. At Source.ag, we adhere to accepted industry standards for security.

- We use specialized industry standard SaaS solutions to provide secure identity and access management in our Services.
- We don't store passwords or other means to access our Services, and instead leverage AWS Cognito for authentication.
- User credentials are communicated, managed and shared through standard mechanisms offered by AWS Cognito.
    - Users receive their initial password by mail, and are forced to change their password upon first login.
    - Users can change their own password as long as they have access to the email inbox to which their Source account is registered.
- Customers have full control over who can access their data through our Services through a fine-grained permission system.

[2] Center for Internet Security. See: https://www.cisecurity.org/

5. **PEOPLE & ACCESS MANAGEMENT**
People make up the heart of our company, and that is why we find it critical to train our workforce on security measures to help them understand proper cyber hygiene and risks associated with their actions. As a result, we have developed measures not only to enhance awareness, but also to identify, authenticate, and authorize users to our systems by means of identity and access management (IAM).

- Access to both internal and external tooling are centralized as much as reasonably possible, by means of Single Sign-on, limiting access privilege based on role.
- Access to source code is limited to authorized personnel only.
- Both remote and physical access to assets is managed and protected, using measures such as multi-factor authentication (MFA) and secure virtual private network (VPN) connections.
- Access to administrative accounts, remote networks, and externally exposed applications (clients) require enforcement of MFA.
- Clear onboarding procedures are in place for granting access to organizational assets upon new hire, rights grant, or role change of a user.
- Clear offboarding procedures are defined and applied to enable quick and complete revoking of access to Source.ag's systems for employees that leave our company.
- Employees are trained on authentication best practices, such as credential management.
- Use of a company-wide password manager (e.g., 1Password) is mandatory and employees are encouraged to generate unique and complex passwords for each different service they use.
- Strong password rules are in place, such as complexity requirements, forced password changes, and history configurations.
- Employees are trained to recognize some of the most common attack vectors, such as phishing. Employees are required to follow Security Awareness training at least every 6 months.

6. **SECURITY MONITORING**
At Source.ag, we are concerned with the integrity and availability of business information. In the events of a security incident, measures have been developed and implemented to minimize the impact on business continuity. As such, measures and services are in place to support the timely identification of security events, limit their potential impact, and recover from any security incident.

- An audit management process is in place and enabled on all of Source.ag's infrastructure to collect audit logs, including but not limited to, username, timestamp and actions taken
- All production changes are verified and monitored by at least two of Source.ag's developers before pushed to production.
- Incident alert thresholds are established and monitored.
- A process is in place to continuously monitor network access, operation, and performance of our Services by means of automatic alerting in the occurrence of detected error conditions in logs.
- A key person is designated to manage Source.ag's incident handling process, whereas management is responsible for the coordination of the incident response.
- Automated backups are performed on a weekly basis for all key assets in-scope and these backups are routinely tested.
- The security of our infrastructure and architecture is routinely audited by a reputable external party, the results of which are used to update our security measures and roadmap.
- We have procedures in place for business continuity in the event of a cyber attack or outage.

7. **PHYSICAL SECURITY**
   We take our physical security just as seriously as our Information security, so we aim to ensure no unauthorized access is possible at any time.
   - Source.ag employees work in private, non-shared offices which are kept locked at all times when no employees are present
   - We have a written policy for physical security requirements for usage of our offices

8. **CONSIDERATIONS REGARDING YOUR OWN SECURITY PRACTICES**
   Information security is not only our priority, but it is everyone's shared responsibility. While we can take measures to secure our assets and infrastructure, it is a shared responsibility to keep our services secure and prevent unauthorized access and tampering of data across data and systems shared between us. To maintain essential functions as much as possible during and after a security event, and prevent such events altogether, we rely on your adoption of information security measures, for instance:

   - Aligning your information security controls to international standards, such as the NIST CSF, Center of Internet Security (CIS) Critical Controls, and ISO 27001.
   - Ensuring that only authorized users have access to the firm's and Source.ag data.
   - Protecting computer equipment and keeping authentication credentials safe, such as usernames and passwords, using methods such as anti-malware software, a firewall, and up-to-date operating systems.
   - Notifying Source.ag in case of actual or suspected compromise to your systems or data.
   - Establishing a contact person that drives information security at your firm.
   - Maintaining governance to decide on risk management priorities, and mitigate risk.
   - Consider leveraging managed services to expand your security capabilities, such as monitoring, scanning, testing and assessments.

Furthermore, in case a security incident happens on your end, please contact us immediately so we can work together to contain the fallout and resolve the issue. You can reach us through regular Customer Support channels and by emailing us at security@source.ag