INFORMATION SECURITY POLICY

Version January 2025

PURPOSE

This SIG Information Security Policy aims to give transparent and accurate information about how and to what extent Software Improvement Group B.V. (hereinafter: '*SIG*') protects confidential information of its customers or other stakeholders (hereinafter collectively: '*Company*') disclosed to or otherwise obtained by SIG, as well as how and to what extent SIG protects its own confidential information. This, also as set in the mutual non-disclosure agreements where SIG is a party, SIG as receiving party will protect disclosing party's (which could be Company) confidential information against disclosure in the same manner and with the same degree of care, but not less than a reasonable degree of care, with which it protects confidential information of its own. Also, such mutual non-disclosure agreements generally state that both parties will exercise proper and due care regarding the processing and storage of the confidential information.

DEFINITIONS

a. '*Credentials*' means any device, method, or process whose purpose is to authenticate, limit, or control access to Company information and SIG systems, including user names, passwords, passphrases, token codes, or answers to challenge questions.
b. '*Company Data*' means source code and related information and documentation of Company systems that shared with SIG for the purpose of carrying out source code analysis and consultancy services.
c. '*Data*' means both Company Data and SIG Data.
d. '*Industrial Accepted Encryption*' means industry acceptable and supported encryption standards and includes, without limitation, at least 256-bit minimum encryption or with equivalent strength, and the use of strong key management processes that include access control over keys.
e. '*Information Security Management System*' means part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security.
f. '*SIG Data*' means methodologies, source code and other confidential material, documentation, information or know-how of SIG.

INFORMATION SECURITY GOVERNANCE

SIG implements and maintains an Information Security Management System (ISMS), which is ISO/IEC 27001 certified, to govern the information security management and aim to ensure appropriate levels of confidentiality, integrity and availability of Data. Furthermore, SIG Sigrid® Assurance Platform has obtained annual SOC2 Type II reports since 2022.

STORAGE

a. SIG will ensure that Company Data is stored, processed and resides in the European Union. Or that Company Data may be accessed by SIG at a location indicated by Company as agreed upon in writing on a case by case basis. SIG will not disclose Company Data available to third parties without Company's written permission. Any deviation from the previous two sentences regarding Company Data is subject to written agreement between Company and SIG.
b. SIG utilizes state-of-the-art data centers to store Data. All Data stored in these data centers is encrypted with Industrial Accepted Encryption.

ACCESS

SIG applies effective access control measures over all systems used to store, transmit or process Data.

a. SIG uses complex and secure passwords or passphrases in any instance where it can set or control the password in question.
b. SIG ensures that all access to Company Data is enforced with MFA.
c. SIG protects the Credentials from loss, theft, or unauthorized disclosure.
d. SIG ensures that Credentials are revoked when there is no longer a legitimate business need to possess such Credentials.
e. SIG ensures that user access rights/privileges to Company Data will only be granted on a need-to-know basis consistent with role-based authorization.
f. SIG ensures that passwords are protected using Industrial Accepted Encryption.

ENCRYPTION

SIG applies Industrial Accepted Encryption to encrypt all Data in transit and at rest.

a. SIG uses Industrial Accepted Encryption to encrypt Data when receiving, transmitting or communicating data across the Internet, on a wireless network, or outside SIG's infrastructure.
b. SIG ensures that Data is encrypted with Industrial Accepted Encryption while in storage in any medium, including, but not limited to, servers, desktop, laptops, portable storage media and back-up media.

NETWORK SECURITY

SIG applies effective network security controls over all systems used to transmit and process Data.

a. SIG maintains operational firewalls at all network perimeters, including, but not limited to, internal networks and public networks.
b. SIG maintains, monitors, and updates a network-based Intrusion Detection / Prevention System to Company facing services.

DATA CENTER SECURITY

Following current best practices in the IT-market, SIG uses standardized hardware that is managed by specialized service providers in state-of-the-art data centers.

a. SIG only uses services providers that are ISO/IEC 27001 certified for hosting Data.
b. SIG deploys virtual private servers that SIG manages itself to ensure the security.
c. By employing Industrial Accepted Encryption, the facilities provided by the service providers are used in such a way that these service providers cannot see what data SIG stores and processes on their facilities.

VULNERABILITY MANAGEMENT

SIG implements and maintains a vulnerability management program using a risk-based approach over all systems used to transmit and process Data.

SECURE SOFTWARE DEVELOPMENT

SIG follows a defined software development process to ensure secure software development. The software development life cycle consists of version control, release management, and security activities that include but are not limited to architecture, static code analysis, code review, penetration testing and remediation.

HUMAN RESOURCES

SIG adopts standard employment screening procedures on all SIG personnel. All personnel receive regular security trainings to ensure the security awareness and sufficient information security knowledge.

SECURITY INCIDENT HANDLING

SIG implements and maintains an effective security incident handling process. Upon discovering or being notified of a breach of Company Data, SIG will notify Company within 24 hours.

DESTRUCTION

At any time on receipt of a written request from the Company, SIG shall permanently destroy the Company Data directly or indirectly in possession of SIG. The regular backups that may include certain Company Data will be completely removed in 6 weeks. All the backup data of any Data is encrypted using Industrial Accepted Encryption.

Version January 2025