Technical and Organizational Security Measures (Security Schedule)

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Company shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

1. the pseudonymisation and encryption of personal data;
2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

More specifically, data Company's security controls shall include:

Domain	Practices
Information Security Policy	○ Varonis maintain written privacy and security policies, which is consistent in material respects with the requirements of this document and with prevailing industry standards. Such policies support and ensure the confidentiality, integrity, and availability of the Data. Varonis hereby warrants and undertakes that it has and that it will maintain throughout the term of the Agreement a written, comprehensive information security program that complies with applicable laws and information security standards. ○ Policies are reviewed and approved by management periodically. ○ Information Security roles and responsibilities are documented and communicated to the relevant personnel. ○ Varonis designated an Information Security Officer who is operationally responsible for assuring that Varonis complies with security policies, and applicable standards and regulations.
Access Control	○ All Varonis system that handles customer data are secured with the described security measures. ○ Access to customer data is managed through a secure authentication. A formal user registration and de-registration procedures for granting and revoking access to information systems and services is maintained. ○ Access to customer data is provided on the need to know basis. Access by Varonis personnel who no longer requires access to perform the Services is terminated. ○ Formal management review of user access rights is performed at regular intervals. ○ Password policy is enforced to company networks and assets. Password Policy include, and not limited to the settings of password age, length, history, complexity requirements, and account lockout duration. ○ Session time-out is enforced on company assets. ○ Administrative and privileged access is restricted to trained and authorized employees of the Data Processor.

Operations Security	○ Information backup is conducted regularly, to allow adequate recovery of information in cases of damage to the information or its systems. Backups are protected using industry best practices encryption, and access control. ○ Periodic restoration tests are performed for scoped data. ○ Varonis perform periodic technical vulnerability scans on networks, and applications that process, store, or transmit Customer's Data. Remediation of vulnerabilities is monitored and performed according to a defined procedure. ○ Malware protection is implemented on Varonis' assets to avoid malicious software gaining unauthorized access to Customer Data. ○ Changes to production infrastructure and networks are monitored and controlled though a change management process. Changes are reviewed and approved prior to implementation and recorded after it. ○ Audit logs recording user activities, exceptions, faults, and information security events are produced, kept, and monitored.
Cryptography	○ Varonis encrypt customer data that is transmitted over public networks, as well as implementing encryption of data at rest. ○ Strong and non-deprecated versions of encryption algorithms and key lengths are used and monitored. ○ Keys and secrets are maintained secured. Access to the Keys and secrets is limited to a minimal number of users on a need-to-know basis. ○ All keys are periodically rotated.

Physical and environmental security	○ Facilities and processing centers are equipped with physical security systems and monitoring as required by security standards (such as ISO/IEC 27001 and/or SOC 2 Type 2), local laws, and regulations. ○ Varonis limit physical access to its electronic information systems and the facilities in which they are housed, and safeguard those facilities against unauthorized physical access, tampering, and theft. ○ Clean desk policy is designed to prevent inadvertent disclosure of personal data. ○ Varonis validates that its cloud service providers maintain physical security policy that is aligned with security industry best-practices, and audited periodically by external third-party auditors (i.e., SOC 2, ISO27001)
Communications Security	○ Varonis applies the principle of least required access for allowed network communications. ○ All network communications are protected with confidentiality and integrity. ○ All network communications are monitored for security incidents Remote access to customers' data is established using a secure, and strong authenticated connection. ○ Restrictions are in be placed in front of externally exposed applications and endpoints.
System Acquisition, development, and maintenance	○ Varonis follows formal Secure Software Development cycle. ○ Rules for the secure software development and systems is established and applied to engineering within the organization. ○ Testing of security functionality is carried out during the development phases. ○ Acceptance testing programs and related criteria is established and maintained for systems, upgrades, and new versions.
Supplier Relationships	○ business arrangements with suppliers, involving their access to Varonis' information, systems and applications shall be based on a formal agreement, consisting of all necessary security and confidentiality relevant to the interaction between Varonis and the suppliers. ○ Technology service providers undergo a security risk assessment and approved by the CISO department. ○ Varonis ensure all suppliers which holds customer’s data are operating, and providing their service, at a security level that is no less stringent than those outlined in this document.

Information Security Incident Management	○ Varonis shall have an updated policy and procedures to assign responsibilities of Varonis personnel and identification of parties to be notified in case of an information security incident, is in place. Customers can report security incidents related to the scoped services to soc@varonis.com ○ Varonis is regularly monitoring security events and alerts from production systems to identify abnormal user and system behavior. ○ Varonis maintains a record of security breaches with sufficient information to allow customers to meet any of its own obligations under relevant data privacy and data security laws and other contractual obligations.
Business continuity management	○ Varonis has a procedure to rebuild cloud environment and recover customer data in case of a disaster causing a destruction before the time it was lost or destroyed. ○ Infrastructure capacity and applicable third-party services are regularly monitored to minimize service disruption. ○ Varonis ensures that all dependent cloud service providers have adequate measures for disaster recovery
Compliance	○ Periodically, Varonis will conduct an independent third-party review (such as ISO/IEC 27001 and/or SOC 2 Type 2) of its security policies, and procedures related to the Services provided to Customer. The list of certificates is available in the Trust Center.
Human Resources	○ New hire process is established and includes screening checks and employee's commitment to confidentiality for employees with access to customer data. ○ Employees undergo periodic security awareness training and are updated on procedures to report security incidents.
Asset Management	○ Asset inventory is maintained and includes ownership and labelling where applicable. ○ Policy for Acceptable use of assets is developed and implemented in accordance with industry best practices. ○ Restrictions are in place to prohibit data transfer to removable media. ○ Varonis ensures that its service providers maintain a secure disposal process when such data is no longer needed.