CUSTOMER DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") forms an integral part of the Agreement ("**Main Agreement**") between Varonis Systems, Inc. and its subsidiaries. (**"Company**") and between the counterparty agreeing to these terms ("**Customer**"; each "**Party**" and together "**Parties**") and applies to the extent that Company processes Personal Data on behalf of the Customer, in the course of its performance of its obligations under the Main Agreement.

If you are accepting this DPA on behalf of Customer, you warrant that: (a) you have full legal authority to bind Customer to this DPA; (b) you have read and understand this DPA; and (c) you agree, on behalf of Customer, to this DPA. If you do not have the legal authority to bind Customer, please do not accept this DPA.

All capitalized terms not defined herein shall have the meaning set forth in the Main Agreement.

1. **Definitions**

1.1 "**Approved Jurisdiction**" means a member state of the European Economic Area, or other jurisdiction as may be approved as having adequate legal protections for data by the European Commission currently found here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

1.2 **"Data Protection Law**" means, as applicable, any and/or all applicable domestic and foreign laws, rules, directives and regulations, on any local, provincial, state or deferral or national level, pertaining to data privacy, data security and/or the protection of Personal Data, including the Privacy and Electronic Communications Directive 2002/58/EC (and respective local implementing laws) concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), including any amendments or replacements to them, including the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("**GDPR**"), and including the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. ("**CCPA**").

1.3 "**Data Subject**" means an individual to whom Personal Data relates. Where applicable, Data Subject shall be deemed as a "**Consumer**" as this term is defined under the CCPA.

1.4 **"EEA**" means those countries that are member of the European Economic Area.

1.5 "**Permitted Purposes**" mean any purposes in connection with Company performing its obligations under the Main Agreement.

1.6 "**Security Incident**" shall mean any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed. For the avoidance of doubt, any Personal Data Breach (as defined under the GDPR) will comprise a Security Incident.

1.7 “**Security Measures**” mean commercially reasonable security-related policies, standards, and practices commensurate with the size and complexity of Company’s business, the level of sensitivity of the data collected, handled and stored, and the nature of Company’s business activities.

1.8 "**Standard Contractual Clauses**" mean the standard contractual clauses for the transfer of personal data to data processors established in third countries adopted by the European Commission Decision EC/2010/87: Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (as amended, superseded or replaced from time to time).

1.9 “**Sub-Processor(s)**” mean any Affiliate, agent or assignee of Company that may process Personal Data pursuant to the terms of the Main Agreement, and any unaffiliated processor, vendors or service provider engaged by Company.

1.10 The terms "**Business**", “**Controller**”, "**Personal Data**", “**Processor**”, “**Process**”, “**Processing**” and "**Service Provider**" shall have the meanings ascribed to them in the Data Protection Law, as applicable.

2. Application of this DPA

2.1 This DPA will only apply to the extent all of the following conditions are met:

(A) Company processes Personal Data that is made available by the Customer in connection with the Main Agreement (whether directly by the Customer or indirectly by a third party retained by and operating for the benefit of the Customer);

(B) The Data Protection Law apply to the processing of Personal Data.

2.2 This DPA will only apply to the services for which the Parties agreed to in the Main Agreement ("**Services**"), which incorporates the DPA by reference.

3. Parties' Roles

3.1 In respect of the Parties' rights and obligations under this DPA regarding the Personal Data, the Parties hereby acknowledge and agree that the Customer is the Controller or Processor (as well as, as applicable, the Business or Service Provider, as these terms are defined under the CCPA) and Company is a Processor or Sub-Processor (as well as, as applicable, the Service Provider, as this term is defined under the CCPA), and accordingly:

(A) Company agrees that it shall process all Personal Data in accordance with its obligations pursuant to this DPA;

(B) The Parties acknowledge that the Customer discloses Personal Data to Company only for the performance of the Services and that this constitutes a valid business purpose for the processing of such data.

3.2 If Customer is a Processor, Customer warrants to Company that Customer’s instructions and actions with respect to the Personal Data, including its appointment of Company as another Processor and concluding the Standard Contractual Clauses, have been authorized by the relevant controller.

3.3 Notwithstanding anything to the contrary in the DPA, Customer acknowledges that Company shall have the right to collect, use and disclose data:

(A) Collected in the context of providing the Services, for the purpose of the operation, support or use of its services for its legitimate business purposes, such as account management, technical support, troubleshooting, security, protecting against fraudulent or illegal activity.
(B) Collected in the context of using the Services, for the purpose of analytics, market research, product improvement and development, provided however that the foregoing shall be based solely on the processing of aggregated and/or anonymized information.
(C) Collected directly from any individuals in the context of surveys, interviews, testing or research activities, for the purpose of product improvement and/or development (including any feedback).
(D) Collected from the Customer's authorized representatives (e.g. employees) and/or authorized users, strictly for the purpose of administrating the business and/or contractual relationship with the Customer, including for billing, audit and recordkeeping purposes.

3.4 To the extent that any data referred under section 3.3 is considered as Personal Data, then Company shall be regarded as an independent Controller of such data under the Data Protection Laws.

4. **Compliance with Laws**

4.1 Each Party shall comply with its respective obligations under the Data Protection Law.
4.2 Company shall provide reasonable cooperation and assistance to Customer in relation to Company's processing of Personal Data in order to allow Customer to comply with its obligations as a Data Controller under the Data Protection Law.
4.3 Company agrees to notify Customer promptly if it becomes unable to comply with the terms of this DPA and take reasonable and appropriate measures to remedy such non-compliance.
4.4 Throughout the duration of the DPA, Customer agrees and warrants that:
(A) Personal Data has been and will continue to be collected, processed and transferred by Customer in accordance with the relevant provisions of the Data Protection Law;
(B) Customer is solely responsible for determining the lawfulness of the data processing instructions it provides to Company and shall provide Company only instructions that are lawful under Data Protection Law;
(C) the processing of Personal Data by Company for the Permitted Purposes, as well as any instructions to Company in connection with the processing of the Personal Data ("**Processing Instructions**"), has been and will continue to be carried out in accordance with the relevant provisions of the Data Protection Law; and that
(D) The Customer has informed Data Subjects of the processing and transfer of Personal Data pursuant to the DPA and obtained the relevant consents or lawful grounds thereto (including without limitation any consent required in order to comply with the Processing Instructions and the Permitted Purposes).

5. **Processing Purpose and Instructions**

5.1 The subject matter of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, shall be as set out in the Agreement, or in the attached Annex 1, which is incorporated herein by reference.

5.2 Company shall process Personal Data only for the Permitted Purposes and in accordance with Customer's written Processing Instructions (unless waived in a written requirement), the Agreement and the Data Protection Law, unless Company is otherwise required to do so by law to which it is subject (and in such a case, Company shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest).

5.3 To the extent that any Processing Instructions may result in the Processing of any Personal Data outside the scope of the Agreement and/or the Permitted Purposes, then such Processing will require prior written agreement between Company and Customer, which may include any additional fees that may be payable by Customer to Company for carrying out such Processing Instructions. Company shall immediately inform Customer if, in Company's opinion, an instruction is in violation of Data Protection Law.

5.4 Additional instructions of the Customer outside the scope of the Agreement require prior and separate agreement between Customer and Company, including agreement on additional fees (if any) payable to Company for executing such instructions.

5.5 Company shall not sell, retain, use or disclose the Personal Data for any purpose other than for the specific purpose of performing the Services or outside of the direct business relationship between the Parties, including for a commercial purpose other than providing the Services, except as required under applicable laws, or as otherwise permitted under the CCPA (if applicable) or as may otherwise be permitted for service providers or under a comparable exemption from "sale" in the CCPA (as applicable), as reasonably determined by Company. Company's performance of the Services may include disclosing Personal Data to Sub-Processors where this is relevant in accordance with this DPA. The Company certifies that it, and any person receiving access to Personal Data on its behalf, understand the restrictions contained herein

6. **Reasonable Security and Safeguards**

6.1 Company represents, warrants, and agrees to use Security Measures (i) to protect the availability, confidentiality, and integrity of any Personal Data collected, accessed or processed by Company in connection with this Agreement, and (ii) to protect such data from Security Incidents. Such Security Measures include, without limitation, the security measures set out in Annex 2.

6.2 The Security Measures are subject to technical progress and development and Company may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the services procured by Customer.

6.3 Company shall take reasonable steps to ensure the reliability of its staff and any other person acting under its supervision who has access to and processes Personal Data. Company shall ensure that persons authorized to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

6.4 Company is responsible for performing its obligations under the Agreement in a manner which enables Company to comply with Data Protection Law, including implementing appropriate technical and organizational measures to ensure a level of security appropriate to the risks that are presented by the processing of Personal Data, in particular protection

against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

7. **Security Incidents**

7.1 Upon becoming aware of a Security Incident, Company will notify Customer without undue delay and will provide information relating to the Security Incident as reasonably requested by Customer. Company will use reasonable endeavors to assist Customer in mitigating, where possible, the adverse effects of any Security Incident.

8. **Security Assessments and Audits**

8.1 Company audits its compliance with data protection and information security standards on a regular basis. Such audits are conducted by Company's internal audit team or by third party auditors engaged by Company, and will result in the generation of an audit report ("**Report**"), which will be Company's confidential information.

8.2 At Customer's written request, and subject to obligations of confidentiality, Company may satisfy the requirements set out in this section by providing Customer with a copy of the Report and/or with Company's SOC 2 Type II report, so that Customer can reasonably verify Company's compliance with its obligations under this DPA. Customer shall rely on the Report and/or the SOC 2 Type II report for validation of proper information security practices and shall not have an additional right to audit Company's compliance unless such right is specifically granted to Customer under applicable law. The foregoing shall not apply solely in the case of a Security Breach resulting in a material business impact to Customer or in connection to a Supervisory Authority specific request. In such event, Customer shall provide Company with 30 days prior written notice (insofar as possible) and the details of any 3rd party auditor on its behalf, for approval.

9. **Cooperation and Assistance**

9.1 If Company receives any requests from individuals or applicable data protection authorities relating to the processing of Personal Data under the Agreement, including requests from individuals seeking to exercise their rights under GDPR or CCPA, Company will promptly redirect the request to Customer. Company will not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If Company is required to respond to such a request, Company will promptly notify Customer and provide Customer with a copy of the request, unless legally prohibited from doing so. The Customer is responsible for verifying that the requestor is the data subject whose information is being sought. Company bears no responsibility for information provided in good faith to Customer in reliance on this subsection.

9.2 If Company receives a legally binding request for the disclosure of Personal Data which is subject to this DPA, Company shall (to the extent legally permitted) notify Customer upon receipt of such order, demand, or request. It is hereby clarified however that if no such response is received from Customer within three (3) business days (or otherwise any shorter period as dictated by the relevant law or authority), Company shall be entitled to provide such information.

9.3 Notwithstanding the foregoing, Company will cooperate with Customer with respect to any action taken by it pursuant to such order, demand or request, including ensuring that confidential treatment will be accorded to such disclosed Personal Data. Customer shall cover all costs incurred by Company in connection with its provision of such assistance.

9.4 Upon reasonable notice, Company shall:

(A) Taking into account the nature of the processing, provide reasonable assistance to the Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Customer's obligation to respond to requests for exercising Data Subject's rights, at Customer's expense;

(B) Provide reasonable assistance to the Customer in ensuring Customer's compliance with its obligation to carry out data protection impact assessments or prior consultations with data protection authorities with respect to the processing of Personal Data, provided, however, that if such assistance entails material costs or expenses to Company, the Parties shall first come to agreement on Customer reimbursing Company for such costs and expenses.

10. **Use of Sub-Processors**

10.1 Customer provides a general authorization to Company to appoint (and permit each Sub-Processor appointed in accordance with this Clause to appoint) Processors and/or Sub Processors in accordance with this Clause.

10.2 Company may continue to use those Processors and/or Sub Processors already engaged by Company as at the date of this Agreement, subject to Company, in each case as soon as practicable, meeting the obligations set out in this Clause.

10.3 Company can at any time appoint a new Processor and/or Sub-Processor provided that Customer is given ten (10) days' prior notice and the Customer does not legitimately object to such changes within that timeframe. Legitimate objections must contain reasonable and documented grounds relating to a Processor and/or Sub-Processor's non-compliance with Data Protection Law. If, in Company's reasonable opinion, such objections are legitimate, Company shall either refrain from using such Processor and/or Sub-Processor in the context of the processing of Personal Data or shall notify Customer of its intention to continue to use the Processor and/or Sub-Processor. Where Company notifies Customer of its intention to continue to use the Processor and/or Sub-Processor in these circumstances, Customer may, by providing written notice to Company, terminate the Agreement immediately.

10.4 With respect to each Processor and/or sub-processor, Company shall ensure that the arrangement between Company and the Processor and/or Sub Processor is governed by a written contract including terms which offer at least the same level of protection as those set out in this Agreement and meet the requirements of article 28(3) of the GDPR and/or of the CCPA (as applicable);

10.5 Company will be responsible for any acts, errors or omissions by its Sub-Processors, which may cause Company to breach any of its obligations under this DPA.

10.6 Company will only disclose Personal Data to Sub-Processors for the specific purposes of carrying out the Services on Company's behalf. Company does not sell or disclose Personal Data to third parties for commercial purposes, except as required under applicable laws.

11. **Transfer of EEA resident Personal Data outside the EEA**

11.1 To the extent that Company processes Personal Data outside the EEA, then the Parties shall be deemed to enter into the Standard Contractual Clauses, in which event the Customer shall be deemed as the Data Exporter and the Company shall be deemed as the Data Importer (as these terms are defined therein):

11.2 Company may transfer Personal Data of residents of the EEA outside the EEA ("**Transfer**"), only subject to the following:

(A) The Transfer is necessary for the purpose of Company carrying out its obligations under the Agreement, or is required under applicable laws; and

(B) The Transfer is done: (i) to an Approved Jurisdiction, or (ii) subject to appropriate safeguards (for example, through the use of the Standard Contractual Clauses, or other applicable frameworks), or (iii) in accordance with any of the exceptions listed in the Data Protection Law (in which event Customer will inform Company which exception applies to each Transfer and will assume complete and sole liability to ensure that the exception applies).

11.3 With reference to Clause 9 and Clause 11(3) of the Standard Contractual Clauses (to the extent applicable), the Standard Contractual Clauses shall be governed by the law of the Member State in which the Data Importer is established.

12. **Data Retention and Destruction**

12.1 Company will only retain Personal Data for the duration of the Agreement or as required to perform its obligations under the Main Agreement, or has otherwise required to do so under applicable laws or regulations. Following expiration or termination of the Main Agreement, Company will delete or return to Customer all Personal Data in its possession as provided in the Main Agreement, except to the extent Company is required under applicable laws to retain the Personal Data. The terms of this DPA will continue to apply to such Personal Data. This section shall not apply to the activities that are the subject matter of section 3.1 herein.

12.2 Notwithstanding the foregoing, Company shall be entitled to maintain Personal Data following the termination of this Agreement for statistical and/or financial purposes provided always that Company maintains such Personal Data on an aggregated basis or otherwise after having removed all personally identifiable attributes from such Personal data.

12.3 Notwithstanding the foregoing, Company shall be entitled to retain Personal Data solely for the establishment or exercise of legal claims, and/or in aggregated and anonymized form, for whatever purpose.

13. **General**

13.1 Any claims brought under this DPA will be subject to the terms and conditions of the Main Agreement, including the exclusions and limitations set forth in the Main Agreement.

13.2 In the event of a conflict between the Main Agreement (or any document referred to therein) and this DPA, the provisions of this DPA shall prevail.

13.3 Changes. Company may change this DPA if the change is required to comply with Data Protection Law, a court order or guidance issued by a governmental regulator or agency, provided that such change does not: (i) seek to alter the categorization of the Company as the Data Processor; (ii) expand the scope of, or remove any restrictions on, either Party's

rights to use or otherwise process Personal Data; or (iii) have a material adverse impact on Customer, as reasonably determined by Company.

13.4 Notification of Changes. If Company intends to change this DPA under this section, and such change will have a material adverse impact on Customer, as reasonably determined by Company, then Company will use commercially reasonable efforts to inform Customer at least 30 days (or such shorter period as may be required to comply with applicable law, applicable regulation, a court order or guidance issued by a governmental regulator or agency) before the change will take effect.

By signature, the Parties acknowledge that they have read and understood the terms of this DPA and agree to be legally bound by it:

CUSTOMER		**COMPANY**	
Signature	_____	Signature	_____
Print Name	_____	Print Name	_____
Title	_____	Title	_____
Date	_____	Date	_____

ANNEX 1 TO DPA

This Annex forms an integral part of the DPA.

CATEGORIES OF DATA SUBJECTS:

- End users who use or interact with Customer's network, products and services.
- Individuals whose personal data is on client's systems or environments that are monitored by Varonis products

CATEGORIES OF PERSONAL DATA:

The data types that may be processed when using the services:

- **Incidental User data**: this refers to technical information and identifiers related to an end user's device or activity, such as: IP addresses, MAC addresses, user agent, Customer issued identifiers, path of files and file names.

PROCESSING OPERATIONS AND PURPOSES:

The purpose(s) of the processing are as necessary for the provision of the Services, pursuant to the Main Agreement.

DURATION:

The duration of the processing will be: until the earliest of (i) expiry/termination of the Main Agreement, or (ii) the date upon which processing is no longer necessary for the purposes of either Party performing its obligations under the Main Agreement (to the extent applicable).

ANNEX 2 TO DPA

This Annex forms part of the DPA and describes the technical and organisational security measures implemented by the data importer.

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:

Contents

1. Roles and Responsibilities

1.1 The executive management of Varonis, recognizing the importance of information security, shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.

1.2 Varonis designated an Information Security Officer who shall be operationally responsible for assuring that Varonis complies with all security policies, and applicable standards and regulations.

2. Information Security Policies

2.1 All Information Security policies shall be developed, reviewed, and approved by the CISO and Senior Management on an annual basis

2.2 Information Security policies are shared within the company portal with all employees. Employees should sign-off information security policies as part of the security awareness program

3. Risk Management

3.1 Varonis shall conduct risk assessments of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of personal information. As part of these risk assessments, Varonis shall determine the likelihood and probability of occurrence and the magnitude of each risk.

3.2 These risk assessments shall be documented and shall provide a baseline for subsequent reviews.

3.3 Varonis shall implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with applicable Security and Privacy Laws. As part of its Risk Management activities, Varonis shall develop and maintain an effective risk response and/or mitigation plan for each risk.

4. Mobile Device Management

4.1 Corporate mobile device applications shall be configured with security features to safeguard sensitive information.

5. Physical and Environmental Security

5.1 Varonis shall 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.

5.2 The entrance to sensitive areas, shall be restricted to authorized employees, and shall be logged.

5.3 Equipment shall be placed and hosted in a secure manner to minimize the risks from environmental threats and hazards.

5.4 All visitors to Varonis' premises shall register prior to accessing facilities and Data Centers, and accompany by Varonis' employee

5.5 Facilities and processing centers shall be equipped with fire alarms, fire distinguishers and other physical security systems as required by security standards, local laws, and regulations

5.6 Varonis shall have policies requiring a "clean desk/clear screen" designed to prevent inadvertent disclosure of personal data.

5.7 Printers shall be configured with a personal password, to access the printouts only pending the presence of the employee by the machine.

6. Access Control

6.1 Access rights to data is provided with least privileged access and on a need-to-know basis

6.2 All accounts, service and platform access shall be managed through a secure authentication control

6.3 Access to customer's data is:

- 6.3.1 Limited based on the principals described in 6.1
- 6.3.2 Regularly monitored by Varonis' Security Operations
- 6.3.3 Restricted to a minimal number of users

6.4 Access rights shall be reviewed periodically to ensure that the level of access is current, necessary, and appropriate.

6.5 Privileged accounts shall only be granted to those users who require such access to perform their job function.

6.6 Privileged accounts shall be strictly controlled, and their use shall be logged, monitored, and regularly reviewed.

6.7 A formal user registration and de-registration procedure for granting and revoking access to all information systems and services is developed and includes a procedure for terminating an employee's access, as part of the employee resignation process

6.8 Password policy shall be enforced to all company networks and assets

6.9 Varonis Corporate Password Policy shall include the settings of Password minimum and maximum age, Password Length, Password history, Complexity requirements, Account lockout duration, Account lockout threshold

6.10 Vendor supplied or default passwords shall be changed or removed prior to systems brought online into production

7. Asset Management

7.1 Varonis shall establish and maintain an inventory of all assets that are permanently or temporarily located at a corporate facility and cloud environments.

7.2 All employee-facing technology devices (i.e., desktop workstations, and laptops) must be labeled such that the device can be identified as belonging to a specific owner whose identity and contact information are known and documented.

7.3 All Varonis assets facilities shall be owned by the System or Business Owner.

7.4 Varonis has a process for new software request. Only approved software shall be used. The use of software is restricted and monitored by the Security Operations Center

7.5 Where applicable, Varonis will use industry best practices to wipe customer's data when such data is no longer needed.

8. Human Resources Security

8.1 All workforce members shall achieve clearance from Varonis

8.2 Varonis' clearance shall be achieved when the workforce member has:

- 8.2.1 Reviewed and acknowledged consent to abide by the Information Security Policies.
- 8.2.2 Completed the Information Privacy & Security Awareness Training and Examination.
- 8.2.3 Successfully passed a background check where legally permissible and according to Varonis' policy
- 8.2.4 Signing Varonis Non-Disclosure agreement

8.3 Varonis shall implement a periodic privacy and security awareness and training program for all members of its workforce.

8.4 Varonis shall further inform its personnel of possible consequences of breaching Varonis security policies and procedures, which will include (where legally permissible) disciplinary action, including possible termination of employment for Varonis employees and termination of contract

9. Supplier Relationships

9.1 All 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 requirements (such as, non-disclosure of Varonis' information, authentication, segregation of duties, input/output controls, audit logging & monitoring, right to audit, breach notification etc.) relevant to the interaction between Varonis and the suppliers.

9.2 To ensure services are delivered with the expected SLAs while maintaining the customers' data confidentiality & integrity, Varonis shall ensure all suppliers are operating, and providing their service, at a security level that is no less stringent than those outlined in this document

9.3 Technology service providers shall undergo a security risk assessment and approved by the CISO department

10. Operational Security

10.1 Varonis shall perform periodic vulnerability scans on internal and external networks and prior to system provisioning for production systems that process, store, or transmit Customer's Data

10.2 Remediation of vulnerabilities will be performed according to Varonis Global Vulnerability and Threat Management Policy

10.3 Malware protection shall be implemented on Varonis' assets

10.4 Monitoring and logging must support the centralization of security events for analysis and correlation

10.5 To the extent technically feasible, Varonis has implemented security measures to ensure that electronically transmitted personal information is not improperly modified without discretion until disposed of. Varonis shall safeguard the integrity of personal information during transmission using secure network communications protocols.

11. Change Management

11.1 Changes to production environments must be monitored and controlled though a change management process.

11.2 Changes must be reviewed and approved prior to implementation by the business owners and information security personnel

11.3 Change Management policy shall include the roles and responsibilities and separation of duties between requester, approver, and implementer

12. Cryptography

12.1 Varonis shall implement technologies and methodologies that make personal information unusable, unreadable and/or indecipherable to unauthorized individuals, including mechanisms to encrypt electronic information at rest and in transit.

12.2 Keys and secrets and maintained secured. Access to the Keys and secrets is limited to a minimal number of users on a need-to-know basis

13. Audits and Certifications

13.1 Periodically, Varonis will conduct an independent third-party review of its security policies, standards, operations, and procedures related to the Services provided to Customer. Independent Audits may include the following:

i. Penetration test
ii. ISO 27000 certifications
iii. SOC 2 Type II report

14. Backup and Restore

14.1.1 Information backup shall be conducted regularly, to allow adequate recovery of information in cases of damage to the information or its systems.

14.1.2 Backups will be protected using industry best practices. Access to backups will be according to industry best practices, and as described in point 6.1

14.1.3 Restoration tests will be performed for production applications and data on periodic basis

14.1.4 Retention policy for customer's data will be documented and described in Varonis relevant policy

15. Incident Response

15.1.1 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.

15.1.2 Varonis is regularly monitoring security events and alerts from production systems, and merges logs from various systems to identify abnormal user and system behavior

15.1.3 In case of an incident, Varonis will provide a report to customers 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

16. Application Security

Varonis has an established application security program and Secure Software Development Lifecycle policy that includes:

16.1.1 Identifying and tracking application security issues, threat mapping and developing appropriate mitigative actions.

16.1.2 Application Security Verification processes closely aligned with OWASP framework and include elements of the OWASP ASVS.

16.1.3 Functional Requirements- each new design element goes through security architecture review which includes threat mapping, applicable controls are included in the feature design and development.

16.1.4 Authentication and authorization controls are included on the Service endpoint level, functional security controls are verified during automated testing phases.

16.1.5 Restrictions are in be placed in front of Web Servers and exposed applications

16.1.6 Application security testing is performed on multiple levels using various technologies.

16.1.7 Periodic Penetration testing is performed on the complete application scope, remediation is prioritized and executed.

16.1.8 Additional Vulnerability assessment efforts are continuously performed to identify new threats and issues.

17. Network Security

17.1.1 All Varonis network locations shall be managed and monitored at secure restricted access locations.

17.1.2 Varonis shall perform network segregation and defense, capable of enforcing security policies and access controls throughout its networks.

17.1.3 Systems are configurable and allow filtering of traffic between domains, VLANS and security zones to prevent unauthorized access.

17.1.4 Varonis shall employ email protection tools to identify and block phishing, Spam, Business Email Compromise, and other attacks

17.1.5 All wireless access to Varonis' corporate network shall be authenticated an encrypted. Guest access shall be limited by time and provided only to public networks

17.1.6 Remote Access connections must be:

17.1.6.1 Established using a secured connection

17.1.6.2 Encrypted using industry standard cryptography

17.1.6.3 Authenticated with multi-factor authentication

17.1.7 Varonis shall maintain distinct operating environments: Development, QA, Staging, and Production - each with its own purpose and appropriate access control.

18. Business Continuity and Disaster Recovery

18.1 Business Continuity and Disaster Recovery plans shall be developed and documented to identify the critical functions to allow continuity of the service and to minimize losses in the event of disruption.

18.2 Business Recovery Plans shall address:

18.2.1 All critical functions, and key resources, including those provided by third parties.

18.2.2 All associated risks to those resources

18.2.3 Recovery Point Objective and Recovery Time Objective

18.2.4 Technology recovery of critical systems and documented plans of third parties

18.2.5 Pandemic Plan