DATA PROCESSING ADDENDUM

BY ACCEPTING THIS DATA PROCESSING ADDENDUM OR ACCESSING OR USING THE SERVICE, YOU ARE AGREEING TO THE TERMS AND CONDITIONS OF THIS DATA PROCESSING ADDENDUM.

IF YOU ARE USING ANY SERVICE AS AN EMPLOYEE, AGENT, OR CONTRACTOR OF A CORPORATION, PARTNERSHIP OR SIMILAR ENTITY, THEN YOU REPRESENT AND WARRANT THAT YOU HAVE THE AUTHORITY TO SIGN FOR AND BIND SUCH ENTITY IN ORDER TO ACCEPT THE TERMS OF THIS AGREEMENT. THE RIGHTS GRANTED UNDER THIS AGREEMENT ARE EXPRESSLY CONDITIONED UPON ACCEPTANCE BY SUCH AUTHORIZED PERSONNEL.

The Parties entered into the Underlying Agreement for SingleStore to provide Customer with services ("Services") which requires that Processor Processes Personal Data on behalf of Customer. This addendum together with its Appendices (together the "Data Processing Addendum" or "DPA") specify the obligations of the Parties when SingleStore is acting as Processor.

 Modifications to this DPA: From time to time, SingleStore may modify this DPA. Unless otherwise specified by SingleStore, changes become effective for Customer upon renewal of the then-current Subscription Term or entry into a new Service Order Form after the updated version of this DPA goes into effect. SingleStore will use reasonable efforts to notify Customer of the changes through communications via Customer’s Account, email or other means.

The “Effective Date” of this DPA is the date which is the earlier of (a) Customer’s initial access to any Service through any online provisioning, registration or order process or (b) the effective date of the first Service Order Form, as applicable, referencing this DPA.

In this DPA, SingleStore will act as a Processor and Customer will act as Controller. SingleStore may also process certain data about Customer or its users as a Data Controller, including in countries outside of the EEA, UK and Switzerland, in accordance with SingleStore’s privacy notice available at https://www.SingleStore.com/privacy-notice.

This DPA is entered into by and between SingleStore, Inc., a Delaware corporation (“SingleStore” or “Processor”) and the person or entity placing an order for or accessing the Service (“Customer” or “Controller”). Processor and Controller are individually referred to as “Party” and collectively as “Parties”. In consideration of the terms and conditions set forth below, the parties agree as follows:

1. Scope of contract and Distribution of Responsibilities

1.1 Processor shall Process Customer Personal Data only on behalf of Controller and at all times only in accordance with this DPA.

1.2 Within the scope of the Underlying Agreement and this DPA, each Party shall be responsible for complying with its respective obligations as Controller and Processor under Data Protection Laws.

1.3 Controller shall ensure that there is a lawful basis in respect of Processor’s Processing of the Customer Personal Data and Data Subjects have been provided with sufficient information to meet the requirements of Article 13/14 of the GDPR/UK GDPR in respect of such Processing (or the equivalent provisions in the Swiss Data Protection Laws).
1.4 The subject matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects are documented in Appendix A to this DPA.

2. Processing Instructions

2.1 Processor will Process Customer Personal Data in accordance with Controller’s instructions set out in the Underlying Agreement or other instructions given from time to time.

2.2 For the avoidance of doubt, any instructions that would lead to processing outside the scope of the Underlying Agreement, where applicable, shall be subject to the contract change procedure under the Underlying Agreement.

2.3 Processor shall promptly inform the Controller if, in Processor's opinion, an instruction infringes Data Protection Laws.

2.4 Processor shall not be liable for any DP Losses arising from or in connection with any Processing made in accordance with Controller’s instructions following Controller’s receipt of any information provided by Processor in this Section 2.

2.5 For the avoidance of doubt, the Processor has the right to process and analyze any Customer Personal Data in an anonymous format for the purposes of developing and improving the Processor’s product and services and for its own analytics and product improvement processes.

3. Processor Personnel

Processor will take appropriate measures to restrict its personnel from Processing Customer Personal Data without authorization. Processor will impose appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security, pursuant to applicable law.

4. Disclosure to Third Parties; Data Subjects Rights

4.1 Processor will not disclose Customer Personal Data to any third party (including any government agency, court, or law enforcement) except as set forth in this DPA or with written consent from Controller or as necessary to comply with applicable mandatory laws. If Processor is obliged to disclose Customer Personal Data to a law enforcement agency or third party, Processor agrees to (where possible) give Controller reasonable notice of the access request prior to granting such access, to allow Controller to seek a protective order or other appropriate remedy. If such notice is legally prohibited, Processor will take reasonable measures to limit the disclosure of Customer Personal Data to the minimum necessary and shall inform Controller promptly if and when such legal prohibition ceases to apply.

4.2 In case Controller receives any request or communication from a Data Subject which relates to the Processing of Customer Personal Data ("Request"), Processor shall provide the Controller with reasonable cooperation, information and assistance ("Assistance") in relation to any such Request where instructed by Controller.

4.3 Where Processor receives a Request, Processor shall (i) not directly respond to such Request, (ii) forward the request to Controller without undue delay and (iii) provide Assistance according to further instructions from Controller.

5. Assistance

5.1 The Processor will assist the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR/UK GDPR (or equivalent provisions in the Swiss Data Protection Laws) taking into account the nature of Processing and the information available to the Processor.
5.2 Where a Data Protection Impact Assessment ("DPIA") is required under applicable Data Protection Laws for the Processing of Customer Personal Data, Processor shall provide upon request Controller with reasonable cooperation and assistance needed to fulfill Customer’s obligation to carry out a DPIA related to Customer’s use of the Services, to the extent that Customer does not otherwise have access to the relevant information and such information is available to SingleStore.

5.3 The Controller shall pay Processor’s reasonable charges mutually agreed between the Parties for providing the assistance in Section 5, to the extent that such assistance is not reasonably able to be accommodated within the normal provision of the Services.

6. Information Rights and Audit

6.1 Processor shall, in accordance with Data Protection Laws, make available to Controller on request in a timely manner such information as is necessary to demonstrate compliance by Processor with its obligations under Data Protection Laws and this DPA.

6.2 SingleStore has obtained third-party certifications and audits set forth on our security page. Upon Controller’s written request and subject to the confidentiality obligations set forth in the Underlying Agreement, SingleStore will make available to Controller a copy of SingleStore’s then most recent third-party certifications or audits, as applicable.

6.3 Processor shall, upon reasonable notice, allow for and contribute to inspections of the Processor’s Processing of Customer Personal Data, as well as the technical and organizational measures (TOMs) (including data processing systems, policies, procedures and records), during regular business hours and with minimal interruption to Processor’s business operations. Such inspections are conducted by the Controller, its affiliates or an independent third party on Controller’s behalf (which will not be a competitor of the Processor) that is subject to reasonable confidentiality obligations.

6.4 Controller must provide Processor with any audit reports generated pursuant to any audit at no charge, unless prohibited by applicable law. Controller shall keep the audit reports confidential and may use the audit reports only for the purposes of meeting its audit requirements under Data Protection Laws.

6.5 Controller shall, prior to the conduct of an audit, submit an audit plan to Processor at least six (6) weeks (or such shorter period as required by law or by a Supervisory Authority) in advance of the proposed commencement date of the audit, setting out the proposed scope, duration and start of the audit. Processor will review the audit plan and will notify Controller within two (2) weeks of receiving the audit plan if it agrees with the plan or if it has any objections in respect of the same. Processor will work co-operatively with Controller to agree a final audit plan.

6.6 Controller shall pay Processor’s reasonable costs of allowing or contributing to audits or inspections in accordance with this Section 6 where Controller wishes to conduct more than one audit or inspection every 12 months. Processor will refer to Controller without undue delay any requests received from a Supervisory Authority that relate to the Processor’s Processing of Customer Personal Data.

6.7 Processor undertakes to cooperate with Controller in its dealings with a Supervisory Authority and with any audit requests received from a Supervisory Authority.

7. Data Incident Management and Notification

7.1 Processor shall implement appropriate and technical and organizational measures to ensure that Customer Personal Data is subject to a level of security appropriate to the risks arising from the Processing by the Processor or its sub-processors, taking into account the factors and measures stated in Article 32 of the GDPR/UK GDPR (or equivalent provisions in the Swiss Data Protection Laws) by meeting the information security standards set out in Appendix B.
7.2 In respect of a Personal Data Breach by Processor relating to Customer Personal Data, Processor shall:

a) notify Controller of a Personal Data Breach involving Processor or a subcontractor without undue delay (but in no event later than 72 hours after becoming aware of the incident);

b) make reasonable efforts to identify the cause of such incident and take those steps as Processor deems necessary and reasonable in order to remediate the cause of the incident to the extent that it is within SingleStore’s reasonable control;

c) provide reasonable information, cooperation and assistance to Controller in relation to any action to be taken in response to a Personal Data Breach under Data Protection Laws, including regarding any communication of the Personal Data Breach to Data Subjects and a Supervisory Authority.

7.3 The obligations contained in this Section 7 should not apply to Personal Data Breaches that are caused by Customer or Customer’s users.

8. International Data Transfer

8.1 Customer Personal Data that SingleStore Processes for the Customer as a Processor may be stored in or outside the EEA, UK or Switzerland depending on the SingleStore product.

8.2 Where there is a Restricted Transfer, the following applies:

a) the Standard Contractual Clauses are incorporated into this DPA and deemed executed by each of the Parties acting on their own behalf and on behalf of their affiliates (where applicable) without the need for any further signature from either Party. If there is any conflict between the Standard Contractual Clauses and this DPA, the Standard Contractual Clauses shall prevail.

b) The Standard Contractual Clauses shall cease to apply to the Processing of Customer Personal Data if and to the extent that the relevant transfer of the Customer Personal Data ceases to be a Restricted Transfer and will re-apply if and to the extent that the relevant transfer becomes a Restricted Transfer again.

UK interpretation of Standard Contractual Clauses

8.3 For the purposes of any Restricted Transfer(s) that are made by a data exporter established in the UK, the Standard Contractual Clauses shall be deemed to be amended (and/or insofar as possible will be interpreted) so that they operate to provide appropriate safeguards to the transfer(s) in accordance with Articles 46 of the UK GDPR and shall be read mutatis mutandis as appropriate.

8.4 The Parties agree that this Clause 8 incorporates the UK Addendum to the European Commission Standard Contractual Clauses issued by the ICO under or pursuant to section 119A(1) of the Data Protection Act 2018 (replaced and updated as necessary) and that, by entering into this DPA, the requirements of that addendum are binding on the Parties in accordance with clause 12 of that addendum. Pursuant to section 19 and Table 4 of the UK Addendum, the Parties agree that the data exporter and data importer may end the UK Addendum as set out in Section 19 of the UK Addendum.

Swiss interpretation of Standard Contractual Clauses
8.5 The Parties agree that the Standard Contractual Clauses shall be read according to all applicable requirements under Swiss Data Protection Laws and shall be read mutatis mutandis as appropriate. In particular, the Parties agree that in relation to any transfers of Customer Personal Data from Switzerland, the Standard Contractual Clauses shall be read in conjunction with the FDPIC’s decision and commentary on “the transfer of personal data to a country with an inadequate level of data protection based on recognized standard contractual clauses and model contracts”, dated 27th August 2021.

9. Particulars of the Standard Contractual Clauses

9.1 For the purposes of Standard Contractual Clauses optional Clause 7 (Docking clause), Clause 7 is included in the Standard Contractual Clauses.

9.2 For the purposes of Clause 9 of the Standard Contractual Clauses (Use of sub-processors), the parties choose Option 2: General Written Authorisation, and the advance time period for informing the Customer of a change in Sub-processor is seven (7) Business Days.

9.3 For the purposes of Clause 11 of the Standard Contractual Clauses (Redress) sub-clause (a), the optional clause is deleted.

9.4 For the purposes of Clause 13 of the Standard Contractual Clauses (Supervision), the parties choose Option (a).

9.5 For the purposes of Clause 17 of the Standard Contractual Clauses (Governing law), the parties choose Option 1, and the parties agree that this shall be the law of Ireland.

9.6 For the purposes of Clause 18 of the Standard Contractual Clauses (Choice of forum and jurisdiction) sub-clause (b), the parties choose the courts of Ireland.

9.7 The information required by Annex I Part A of the Standard Contractual Clauses (List of parties) can be found in the Underlying Agreement. The information required by Annex I Part B of the Standard Contractual Clauses (Description of transfer) can be found in Appendix A of this DPA. The information required by Annex I Part C of the Standard Contractual Clauses (Competent supervisory authority) is the Irish Data Protection Commissioner.

9.8 For the purposes of Annex II of the Standard Contractual Clauses and unless otherwise specified in the Underlying Agreement, the description of the technical and organizational measures for the security of the Customer Personal Data are set out at Appendix B to this DPA.

9.9 For the purposes of Annex III of the Standard Contractual Clauses the information is set out in the Sub-processor Schedule (available from SingleStore on request).

10. Appointment of sub-processors

SingleStore may appoint another processor (a sub-processor) to process Customer Personal Data on behalf of Customer subject to the following conditions:

a) SingleStore shall notify Customer of its intention to engage such sub-processor. Customer shall be deemed to have approved the engagement of the sub-processor if it does not notify SingleStore in writing objecting (acting reasonably) to such appointment within seven days of the date of SingleStore’s notification;

b) SingleStore’s engagement of the sub-processor shall be on legally binding terms which impose the same material obligations on the sub-processor as are imposed on SingleStore under this DPA; and
c) Where processing of Customer Personal Data constitutes a Restricted Transfer, SingleStore shall enter into standard contractual clauses approved by the European Commission in its decision (EU) 2021/914 of 4 June 2021 (Module 3 Processor to Processor) (with any necessary modifications required for extra-UK or extra-Swiss data transfers).

11. Term and Termination

This DPA becomes effective from the Effective Date and shall continue to operate for the duration of the Underlying Agreement.

12. Deletion or Return of Customer Personal Data

12.1 Controller may export all Customer Personal Data prior to the termination of the Customer's Account. In any event, following the termination of the Customer's Account, (i) subject to (ii) and (iii) below and the Underlying Agreement, Personal Data will be retained for a period of seven (7) days from such termination within which Controller may contact Processor to export Customer Personal Data; (ii) where the Controller does not use custom mailbox and uses the e-mail feature, if available within the Service(s), e-mails forming part of Personal Data are automatically archived for a period of three (3) months; and (iii) logs are archived for a period of thirty (30) days in the log management systems, post which logs are retired to a restricted archived cold storage for a period of eleven (11) months (each a "Data Retention Period"). Beyond each Data Retention Period, Processor reserves the right to delete all Personal Data in the normal course of operation except as necessary to comply with Processor's legal obligations, maintain accurate financial and other records, resolve disputes, and enforce its agreements. Personal Data cannot be recovered once it is deleted.

12.2 Customer may instruct Processor to delete the Personal Data at any time.

13. Miscellaneous

13.1 In case of any conflict, the provisions of this DPA shall take precedence over the provisions of any other agreement with Processor.

13.2 The limitation of liability stated in the Underlying Agreement shall apply to the breach of the DPA.

13.3 Any supplementary agreements or amendments to this DPA must be made in writing and signed by both Parties.

13.4 Should individual provisions of this DPA become void, invalid or non-viable, this shall not affect the validity of the remaining conditions of this DPA.

14. Definitions

"Customer Personal Data" means Personal Data:

a) supplied to Processor by, or on behalf of Controller; and/or

b) obtained by, or created by, Processor on behalf of Controller in the course of delivery of Services.

"Data Protection Laws" shall mean the GDPR and any applicable EU Member State national laws implementing or supplementing the GDPR, the UK Data Protection Laws and the Swiss Data Protection Laws.

"DP Losses" means all liabilities, including:

a) costs (including legal costs);
b) claims, demands, actions, settlements, charges, procedures, expenses, losses and damages (whether material or non-material, and including for emotional distress);

c) to the extent permitted by applicable law:

i) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a data protection authority or any other relevant Regulatory Authority;

ii) compensation to a Data Subject ordered by a data protection authority to be paid by Processor;

iii) the costs of compliance with investigations by a data protection authority or any other relevant Regulatory Authority.

“EEA” means European Economic Area.

"GDPR" shall mean 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.

“ICO” means the UK Information Commissioner’s Office.

“Restricted Country” means a country, territory or jurisdiction which is not considered by the EU Commission (or in respect of Customer Personal Data transfers caught by the requirements of UK Data Protection Laws or Swiss Data Protection Laws, the relevant UK and/or Swiss governmental or regulatory body as applicable) to offer an adequate level of protection in respect of the processing of Personal Data pursuant to Article 45(1) of the GDPR/UK GDPR (or equivalent provisions in the Swiss Data Protection Laws);

“Restricted Transfer” means a transfer of Customer Personal Data from an entity whose processing of Customer Personal Data under the DPA is caught by the requirements of the Data Protection Laws, to an entity that processes the relevant Customer Personal Data in a Restricted Country;

"Standard Contractual Clauses" means the standard contractual clauses for the transfer of Personal Data from a Data Controller in the European Economic Area to Processors established in third countries in the form set out in the Annex of the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (Module 2 Controller to Processor), as supplemented by Section 9 of this DPA.

“Swiss Data Protection Laws” means all laws relating to data protection, the Processing of Personal Data, privacy and/or electronic communications in force from time to time in Switzerland including the Swiss Data Protection Act 1992 and the Swiss Data Protection Act 2020 (as in force and applicable).

“UK” means United Kingdom.

“UK Data Protection Laws” means all laws relating to data protection, the Processing of Personal Data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.

“UK GDPR” means the UK GDPR as defined by section 3(10) of the UK Data Protection Act 2018.

"Underlying Agreement" shall mean the SingleStore Customer agreement (whether Cloud Service Agreement (formerly Managed Service Agreement) or On Premises License Agreement (formerly Self-Managed License Agreement)) available at https://www.SingleStore.com/legal/, or an equivalent master Service agreement executed between the Parties, including any order documents or statements of work for Service entered into between SingleStore and Customer.
"Controller", "Data Subject", "Personal Data Breach", "Processor", "Process", "Processing" and "Supervisory Authority" shall have the meaning given to them in the GDPR/UK GDPR. For processing subject to the UK GDPR, Supervisory Authority shall mean ICO.
Appendix A: Customer Personal Data

This Appendix includes certain details of the Processing of the Customer Personal Data as required by Article 28(3) GDPR/UK GDPR or equivalent provisions in the Swiss Data Protection Laws.

1. Subject matter and duration of the Processing of the Customer Personal Data

The subject matter of the Processing is set out in the Underlying Agreement. The duration of the Processing will be for the duration of the Underlying Agreement.

2. The nature, purpose and frequency of the Processing of the Customer Personal Data

Processor shall Process the Customer Personal Data for the purposes of providing the Services as set out in the Underlying Agreement. Where there is a Restricted Transfer, the frequency of the transfer will be on a continuous basis.

3. The types of the Customer Personal Data to be Processed

The types of Customer Personal Data are described in the Underlying Agreement and include any Personal Data provided by or on behalf of Controller to Processor in connection with the Services.

4. The categories of Data Subject to whom the Customer Personal Data relates

The categories of Data Subject to whom the Customer Personal Data relates are described in the Underlying Agreement.

5. The period for which the Customer Personal Data will be retained

The period for which the Customer Personal Data will be retained is set out in Clause 11 of this DPA.
Appendix B: SingleStore, Inc. Technical and Organizational Measures

a. Personal Data Storage

SingleStore is a global company providing services through all major cloud solution providers (CSP). SingleStore Cloud Service customers are able to choose from a selection of global processing and storage locations to meet their geographic and strategic needs.

b. Encryption and Key Management

SingleStore products support encryption at rest and in transit to ensure the security of Customer Personal Data. Customers using SingleStore on their own infrastructure are responsible for ensuring that adequate encryption is in place. For SingleStore Cloud Service encryption at rest is provided through CSP native technologies supporting AES-256 encryption and for encryption at rest TLS 1.2 is fully supported, however this requires customer configuration.

c. Support and Maintenance

SingleStore deploys changes to SingleStore Cloud Service during scheduled maintenance windows, which are agreed upon at the point of customer onboarding. For any additional maintenance required SingleStore will contact customers directly via email to notify and agree on said maintenance.

d. Incident Response and Notification

“Incident” means a security event that compromises the confidentiality, integrity or availability of an information asset. "Breach" means an Incident that results in the confirmed disclosure, not just potential exposure, of Customer Personal Data to an unauthorized party.

SingleStore has an incident response plan, including a breach notification process, to assess, escalate, and respond to identified physical and cyber security incidents that impact the organization, Customers, or result in DP Losses. Discovered intrusions and vulnerabilities are resolved in accordance with established procedures. The incident response plan is reviewed and updated annually and more frequently as needed. If there is a Breach involving Customer Personal Data, SingleStore will (A) notify you without undue delay and in any event within 72 hours of becoming aware of the Breach, (B) reasonably cooperate with you with respect to such Breach, and (C) take appropriate corrective action to mitigate any risks or damages involved with the Breach to protect Customer Personal Data from further compromise. SingleStore will take any other actions that may be required by applicable law as a result of the Breach.

e. Information Security Program

Scope and Contents: SingleStore maintains a written security program that (A) complies with applicable global industry recognized information security frameworks, (B) includes administrative, technical and physical safeguards reasonably designed to protect the confidentiality, integrity and availability of Customer Personal Data and (C) is appropriate to the nature, size and complexity of SingleStore’s business operations. SingleStore has built its information security program on the requirements of ISO 27001 and SOC 2.

Security Program Changes: SingleStore policies, standards, and operating procedures related to confidentiality, integrity and availability are made available to personnel via the corporate intranet. Security policies and procedures are reviewed, updated (as needed), and approved at least annually to maintain their
continuing relevance and accuracy. Personnel are required to review and acknowledge these policies and procedures during on-boarding and annually thereafter.

**Security Officer:** SingleStore’s GRC Program Manager and Information Security Steering Committee develop, maintain, review, and approve SingleStore’s security standards and policies.

**Security Training & Awareness:** All SingleStore personnel are required to complete security awareness training at least on an annual basis. SingleStore conducts periodic security awareness education and communications in relation to phishing and other security concerns.

**f. Risk Management**

A security risk assessment and management process is in place to identify and remediate potential threats to SingleStore. Risk ratings are assigned to all identified risks, and remediation is managed by security personnel. Executive management is kept apprised of the risk posture of the organization. Full business risk assessments are completed at least annually.

**g. Access Control**

SingleStore assigns application and data rights based on user security groups and roles within its access management system. Security access requests are approved by the designated individual prior to provisioning. Security groups and roles are created based on the principle of least privilege. SingleStore classifies informational assets in accordance with its data classification guideline.

**h. User Access Management**

SingleStore promptly disables application, platform and network access for terminated users upon notification of termination. Administrator access to confidential and restricted systems, including corporate and cloud networks, is reviewed on an annual basis for appropriateness. Any inappropriate access is removed promptly. SingleStore uses separate administrative accounts to perform privileged functions, and accounts are restricted to authorized individuals.

**i. Password Management and Authentication**

SingleStore uses an industry recognized access management system for users to authenticate to corporate resources. This also enforces minimum password length and complexity as well as requiring multi-factor authentication on all connections.

**j. Remote Access**

Remote access to the corporate network is secured through a virtual private network (VPN) solution with two-factor authentication. Remote access to all corporate applications requires authentication through the access management system and with multi-factor authentication.

**k. Asset Configuration and Security**

Endpoint antivirus technology is installed and activated on all SingleStore workstations to monitor for virus and malware infections. Endpoint devices are scanned in real-time. Monitoring is in place to indicate when an anti-virus agent does not check in for prolonged periods of time. Issues are investigated and remediated as appropriate. SingleStore uses full-disk encryption on all endpoints. Endpoint devices are monitored and
encrypted using industry recognized tools. IT administrators are alerted of discrepancies in security policies and settings identified from the tools. SingleStore maintains and regularly updates an inventory of corporate and cloud infrastructure assets, and systematically reconciles the asset list annually.

I. Security Testing

SingleStore has established a Threat and Vulnerability Management (TVM) program to monitor for vulnerabilities on an on-going basis. Quarterly internal vulnerability scans are conducted using industry-recognized vulnerability scanning tools. Identified vulnerabilities are evaluated and documented within an associated ticket and remediated to address the associated risk(s). External penetration tests are conducted by an independent third party on an annual basis to detect application security vulnerabilities. Critical and High findings from these tests are evaluated, documented, and remediated.

m. Logging and Monitoring

SingleStore continuously monitors application, infrastructure, network, data storage space and system performance. SingleStore utilizes a security monitoring tools that proactively alert based on suspicious or abnormal activities. Logs contain details on the date, time, source, and type of events. Information and works events worthy of real-time review are reviewed.

n. Change Management

SingleStore change management policies and procedures are established for requesting, testing, and approving application, infrastructure, and product related changes. All changes receive a risk score based on risk and impact criteria. Lower risk release changes generate automated change tickets and have various levels of approval based on risk score. High risk-rated changes require manual change tickets to be created and are reviewed by approvers based on change type. Planned changes to the corporate and/or cloud production environments are reviewed regularly. Change documentation and approvals are maintained in a ticketing system (SOC: CM-1). Product development changes undergo various levels of review and testing based on change type, including security and code reviews, regression, and user acceptance testing prior to approval for deployment (SOC: CM-2). Following the successful completion of testing, changes are reviewed and approved by appropriate managers prior to implementation to production (SOC: CM-3). Dedicated environments separate from production exist for development and testing activities. (SOC: CM-9).

o. Secure Development

SingleStore has established a Software Development Life Cycle (SDLC) methodology that governs the acquisition, development, implementation, configuration, maintenance, modification, and management of infrastructure and software components. The SDLC methodology is consistent with SingleStore’s security, availability, processing integrity and confidentiality policies. Prior to the final release of a new version to the production cloud environment, code is reviewed and tested. Secure coding guidelines are established based on leading industry standards, updated as needed, and are available to personnel via the intranet. Developers receive secure coding training.

p. Network Security

Network perimeter defense solutions, including firewalls, are in place to monitor, detect, and prevent malicious network activity. Security operations personnel monitor items detected and take appropriate action. Firewall rule changes that meet the criteria for the corporate change management criteria follow the
change management process and require approval by the appropriate approvers. SingleStore’s corporate and Cloud networks are logically segmented and firewalls monitor traffic to restrict access to authorized users, systems, and services.

q. Third Party Security

SingleStore assesses and manages the risks associated with existing and new vendors. SingleStore employs a risk-based scoring model for each vendor. SingleStore communicates security and confidentiality requirements and operational responsibilities to third parties through contractual agreements as necessary (e.g., Master Underlying Agreement, Non-Disclosure Agreement, Information Security Addendum, Data Processing Addendum). All vendors with access to data classified as confidential in SingleStore’s document classification scheme are reviewed at least annually using a third party vendor risk assessment tool.

r. Physical Security

Physical access to SingleStore offices is granted based on job responsibilities and work location. Access to offices can only be approved by appropriate personnel. Physical access is removed when access is no longer required and as a component of the employee termination process. Visitor logs are maintained for personnel visiting the offices, and visitors are required to be escorted by SingleStore personnel. Badge readers control all access within SingleStore offices. Unauthorized badge access attempts are denied and logged. Tailgating is prohibited by policy.

s. Internal Audit

Internal audits are aligned to SingleStore’s information security program and compliance requirements. SingleStore conducts internal control assessments to validate that controls are operating effectively. Issues identified from assessments are documented, tracked and remediated as appropriate. Internal controls related to security, availability, processing integrity and confidentiality are audited by an external independent auditor at least annually and in accordance with applicable regulatory and industry standards.

t. Business Continuity

SingleStore has a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP) in place to manage significant disruptions to operations and infrastructure. These plans are reviewed and updated periodically and approved on an annual basis by SingleStore’s GRC Program Manager and Information Security Steering Committee. Business continuity exercises are conducted to evaluate the tools, processes and subject matter expertise of SingleStore in response to a specific incident. Summaries of the results of the exercises are documented and issues identified are tracked and followed up on for remediation.

u. Human Resources Security

SingleStore requires personnel to sign a confidentiality agreement as a condition of employment. SingleStore has a new employee hiring procedure in place to guide the hiring process, and background verification checks are completed for potential SingleStore personnel in accordance with relevant laws and regulations. SingleStore maintains a disciplinary process to take action against personnel that do not comply with company policies, including but not limited to, those put in place to meet its security.