DATAROBOT INFORMATION SECURITY POLICY

This Information Security Policy ("**Policy**") describes the technical and organizational security measures implemented by DataRobot to secure the Solution and Customer Data where Customer purchases the SaaS version of the Solution. DataRobot may update or change its controls from time to time but will never materially decrease the level of security as set out in this Policy.

1. Definitions

Unless otherwise defined herein, all capitalized terms have the meaning given to them in the DataRobot Master Subscription Agreement ("**Agreement**").

"Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data.

"Personal Data" means any Customer Data relating to an identified or identifiable natural person or household.

"Supervisory Authority" means any regulator or regulatory body or supervisory authority in any country.

2. General Security Practices

DataRobot has implemented and shall maintain appropriate technical and organizational measures designed to protect Customer Data against accidental loss, destruction, alteration, unauthorized disclosure or access, or unlawful destruction, including the policies, procedures and internal controls as set forth in this Policy.

3. Information Security Organization

3.1 **Information Security Program.** DataRobot shall maintain a comprehensive written information security program ("**Program**") that encompasses administrative, technical and physical controls designed to protect the confidentiality, security, integrity, and availability of Customer Data and with the aim of protecting against Data Breaches. DataRobot shall ensure the Program is consistent with global industry standards and appropriately tailored to the types of data processed by DataRobot.

3.2 **Information Security Personnel.** DataRobot's Program shall be led by its Chief Information Security Officer or other designated information security professional ("**CISO**"), who is responsible for its direction, governance and oversight. To administer the Program, the CISO shall direct a team of highly qualified personnel with training and certifications specialized in information security.

3.3 **Information Security Review.** DataRobot's Program and approach to managing information security shall be reviewed regularly and whenever significant changes occur, by appropriate internal and external assessors.

3.4 **Information Security Governance.** DataRobot shall leverage a cross-functional leadership team to shape security programs and drive executive alignment in all security initiatives. Relevant DataRobot personnel shall meet regularly to foster communication between operational teams and ensure security is considered in all projects.

3.5 **Policies and Procedures.** DataRobot shall maintain policies and procedures related to information security, confidentiality and integrity. These shall be reviewed and updated at least annually and made available to employees via the DataRobot intranet. Employees must review and acknowledge these policies at onboarding and on an annual basis.

4. Human Resources Security

4.1 **General.** DataRobot shall ensure all personnel are subject to written confidentiality obligations and the DataRobot Code of Conduct and Business Ethics, and shall inform personnel of the consequences of violation. Personnel who violate these shall be subject to disciplinary action up to and including termination.

4.2 **Training and Awareness.** DataRobot shall ensure that mandatory information security and data privacy training is provided to employees at onboarding and on a regular basis throughout employment to aid in the prevention of unauthorized or unintended disclosure of Customer Data. Training shall be regularly reinforced by security awareness communications, events and phishing campaigns.

4.3 **Background Checks.** DataRobot shall conduct background checks on personnel in compliance with applicable law, which may include employment history, foreign employment, criminal background, credit check (when applicable), education verification, sex offender register, OFAC/Global Sanctions, SSN Tracing.

4.4 **Third Party Security.** DataRobot shall implement a vendor management program to assess and monitor risk associated with service providers that process Customer Data. Service providers shall be evaluated prior to onboarding and periodically throughout their engagement, and are contractually obligated to security and confidentiality requirements.

5. Business Continuity Management

5.1 **Business Continuity Management Program.** DataRobot shall maintain a Business Continuity Management Program ("**BCM Program**") designed to manage significant disruptions to operations and infrastructure, including cybersecurity incident response. The BCM Program shall include the following elements:

(a) defined global and regional governance bodies and executive ownership;

(b) BCM professionals responsible for creating, managing and monitoring preparedness;

(c) defined crisis management organizations and escalation protocols;

(d) established crisis communications strategies for all stakeholders;

(e) identification of critical activities and planned recovery time objectives;

(f) thorough risk and impact assessments of locations and processes, including critical suppliers;

(g) testing on at least an annual basis of all related systems and components, including staff recovery, and tracked remediation for any issues identified during testing; and

(h) continued maintenance and review of arrangements to respond to changing business requirements and risks.

5.2 **Data Recovery.** Where and as applicable, DataRobot shall design redundant storage and procedures for recovering data in its possession or control in a manner sufficient to reconstruct Customer Data in its original state on the last recorded backup.

6. Physical Controls

6.1 **Physical Access to Facilities.** DataRobot shall limit access to all office locations to authorized individuals. All office building entryways shall be monitored by building security personnel and/or CCTV and shall be access controlled at all times.

(a) All personnel shall be issued entry and identification badges which must be carried at all times. Badges shall be deactivated upon employment termination.

(b) All office visitors shall be logged and accompanied throughout the office.

6.2 **Physical Access to Equipment.** All DataRobot server rooms shall implement badge entry access controls to limit access to authorized personnel only.

6.3 **Protection from Disruptions.** DataRobot shall implement appropriate measures designed to protect against loss of data due to power supply failure or line interference.

7. Audits

7.1 **General.** DataRobot shall cooperate with reasonable requests by Customer for legally required audits of DataRobot's security and privacy practices. The time, duration, place, scope and manner of the audit must be mutually agreed by the parties.

7.2 **Audit Procedure.** On written request from Customer, DataRobot shall answer Customers' written questions about DataRobot's security and privacy practices and shall provide Customer with information necessary to demonstrate DataRobot's compliance with the terms of this Information Security Policy and the DataRobot Data Processing Policy . Customer may make one request per calendar year except if a Data Breach has occurred.

7.3 **Certifications.** DataRobot shall make available to Customer, upon written request and without undue delay, copies of any third-party audit reports or evidence of certifications it maintains (such as SSAE 16 –SOC2, attestations or ISO 27001:2013 certifications, or their equivalent under any successor standards) that apply to the Solution. DataRobot shall maintain SSAE 16 – SOC2 and ISO 27001:2013 certifications, or equivalent successor standards, for the duration of the Agreement.

7.4 **Regulatory Compliance.** Taking into account the nature of the request and to the extent reasonably feasible from a technical perspective, DataRobot shall provide Customer with any information necessary to enable Customer to comply with any applicable law or any request from a Supervisory Authority.

7.5 **Cooperation with Supervisory Authorities.** If a Supervisory Authority wishes to carry out an audit of DataRobot or its activities under the Agreement, Customer shall provide DataRobot with no less than 10 business days' notice, unless the Supervisory Authority has given less notice to Customer. DataRobot shall cooperate with the Supervisory Authority as they require.

8. Customer Data

8.1 Where Customer Data includes Personal Data, the parties will comply with their obligations in the Data Processing Policy found at https://www.datarobot.com/legal/Data_Processing. Where DataRobot has provided to Customer a SaaS-version of the Solution with the express right to include Protected Health Information ("**PHI**") in the Customer Data, with respect to such PHI the parties will comply with their obligations in the Business Associate Agreement found at https://www.datarobot.com/legal/BAA, unless the parties have executed a separate Business Associate Agreement in which case such executed Business Associate Agreement shall apply.

8.2 **Cloud Data Storage.** DataRobot's multi-tenant SaaS offering ("**MTS**") is hosted on AWS servers located in the United States, Ireland, and Japan. Unless specified otherwise by Customer, customers based in the United States will be provisioned on the United States AWS instance, customers based in the European Economic Area, Switzerland and the UK will be provisioned on the Ireland AWS instance, and customers based in Japan will be provisioned on the Japan AWS instance. Customers located in other countries will be provisioned on either Ireland, the US, or the Japan AWS instance. To review AWS's security documentation, please visit https://aws.amazon.com/compliance/data-center/controls/. DataRobot's single-tenant SaaS offering ("**STS**") can be hosted by various service providers (e.g., AWS, GCP, Azure) in various locations. Customer shall choose its hosting provider and data storage location based on available offerings at the time of product purchase and may review the applicable hosting provider's security documentation at such time.

8.3 **Data Backups.** For MTS, AWS Elastic Block Store (EBS) volumes are backed up using EBS Snapshots. Backups shall be automated, encrypted, and performed multiple times daily. For STS, please review applicable hosting providers data-backup policies at the time of purchase.

8.4 **Logging and Monitoring.** DataRobot shall maintain logs of administrator and operator activity and data recovery events.

8.5 **Data Encryption.** DataRobot shall encrypt all Customer Data residing in or transiting to or from the Solution. Customer Data in transit is encrypted using HTTPS (TLS 1.2/AES-256 or better). Data at rest in cloud environments is encrypted with SSE-S3 object level data encryption (AES-256) available from the cloud supplier.

8.6 **Return of Data**. Customer may export its data from the Solution at any time during the Subscription Term in accordance with the instructions in the Documentation.

8.7 **Data Disposal.** Within 30 days of termination of Subscription Term, DataRobot will delete all Customer Data that is not required to be retained by law. Any Customer Data that is retained will be managed in accordance with the terms of this Policy and the Data Processing Policy (where applicable) and deleted according to our retention policy.

9. Access Controls

9.1 **Access Management**. DataRobot shall employ access control mechanisms to prevent unauthorized access to Customer Data and systems that have access to Customer Data. DataRobot shall restrict access to Customer Data only to personnel whose access is necessary to provide the Solution.

(a) DataRobot shall maintain a record of personnel authorized to access Customer Data and review user access rights at regular intervals.

(b) DataRobot shall have controls designed to avoid personnel assuming access rights beyond those that they have been assigned to limit unauthorized access to Customer Data.

(c) At Customer's reasonable request, DataRobot shall promptly suspend or terminate access rights to Customer Data for DataRobot personnel reasonably suspected of breaching any of the provisions of this Policy. DataRobot shall remove access rights of all personnel upon termination of their employment.

9.2 **Secure Access Protocols.** DataRobot shall use secure access protocols and solutions such as LDAP, firewalls, and VPN to enforce logical access in the internal network environment.

9.3 **Application Password Management.** For users attempting to access the Solution, DataRobot shall require complex user passwords with length, character complexity, and non-repeatability requirements. DataRobot shall ensure that deactivated or expired login credentials are not granted to other individuals. User passwords shall be encrypted and salted using PBKDF2 (SHA512+128bit salt).

9.4 **Application Authentication Controls.** DataRobot shall monitor repeated failed attempts to gain access to the Solution and shall lock out user accounts after five failed authentication attempts. DataRobot shall ensure that two factor authentication is available for user accounts, and provide for unique user API tokens. DataRobot shall allow for Single Sign On (SSO) authentication with any standard SAML 2.0 identity provider.

9.5 **Role Based Access.** DataRobot shall provide granular user application privilege controls. User administrative accounts shall have the ability to assign user and group roles with varying levels of access privileges based on the user's or group's use of the Solution.

10. Data Breaches

DataRobot shall maintain procedures to ensure a timely and efficient response to a Data Breach.

DataRobot shall:

(a) notify Customer without undue delay but no later than 48 hours after becoming aware of a Data Breach;

(b) provide assistance and available information to Customer as reasonably requested to enable Customer to investigate, mitigate the effects of and remediate the Data Breach and comply with any breach notification obligations that apply to Customer under applicable law;

(c) take steps to identify the cause of any Data Breach and put in place measures and take steps that DataRobot deems necessary to mitigate the effects of and remediate the Data Breach;

(d) retain appropriate information and records about any Data Breach for a reasonable period of time;

(e) cooperate with Customer, law enforcement and any appliable Supervisory Authorities as reasonably required in relation to a Data Breach;

(f) not reference or identify Customer when making any notification to a third party about a Data Breach unless required to do so by applicable law.

11. Communications Security

11.1 **Networks.** DataRobot shall use the following controls designed to secure its networks that access or process Customer Data:

(a) Network traffic shall pass through firewalls, which are monitored at all times. DataRobot shall implement intrusion detection and/or prevention systems.

(b) Network devices used for administration shall utilize industry standard cryptographic controls when processing Customer Data.

(c) Anti-spoofing filters and controls shall be enabled on routers. Network, application and server authentication passwords shall have complexity requirements. DataRobot shall have a policy prohibiting the sharing of user IDs, passwords or other login credentials.

(d) Firewalls shall be deployed to protect the perimeter of DataRobot's networks.

11.2 **Virtual Private Networks.** DataRobot shall employ the following controls when remote connectivity to DataRobot's network is required for processing Customer Data:

(a) Connections shall be encrypted using industry standard cryptography (i.e. a minimum of 256 bit encryption);

(b) Connections shall only be established using VPN servers;

(c) Multifactor authentication shall be required for access.

12. Secure Development

12.1 **Development Requirements.** DataRobot shall have policies for secure development, system engineering, change control, and support. DataRobot shall conduct appropriate tests for system security as part of acceptance testing processes. DataRobot shall supervise and monitor the activity of outsourced system development.

12.2 **Change Management.** DataRobot shall follow industry best practices for the tracking of application projects and source code changes. Task tracking software shall be used to provide an audit trail of all software changes and pull requests. All code shall be subject to extensive testing, stakeholder signoffs, and code review prior to release.

12.3 **Application Code Security Analysis.** DataRobot shall adhere to the OWASP Top 10 for secure coding practices. Static, dynamic and software composition analysis scans shall be performed on each major application release. If the scans reveal any material deficiencies or weaknesses, DataRobot shall promptly take such steps as may be required, in DataRobot's reasonable discretion, to remediate, taking into consideration their criticality based on their nature, severity and likelihood.

12.4 **Application Environment Security Analysis.** For each major application release, DataRobot shall perform static and dynamic analysis scans and container environment scans. If the scans reveal any material deficiencies or weaknesses, DataRobot shall promptly take such steps as may be required, in DataRobot's reasonable discretion, to remediate, taking into consideration their criticality based on their nature, severity and likelihood.

12.5 **Supply Chain Management.** DataRobot shall manage and regularly scan its software supply chain libraries for vulnerabilities and license compliance. DataRobot shall promptly remediate any material vulnerabilities or instances of noncompliance that are identified.

13. Security Testing and Monitoring

13.1 **Testing and Monitoring Requirements.** DataRobot shall maintain policies and procedures for the ongoing testing and monitoring of DataRobot environments by internal and/or external parties, using industry standard tools and methodologies.

13.2 **Threat Management.** DataRobot shall maintain a threat management program to monitor both malicious and non-malicious threats**.** Identified issues shall be reviewed and investigated.

13.3 **Penetration Testing.** On at least an annual basis, DataRobot shall engage a trusted third-party security vendor to perform penetration tests to detect corporate infrastructure and network vulnerabilities. Any and all identified vulnerabilities or weaknesses shall undergo a risk assessment process and shall be mitigated as appropriate.

13.4 **Remediation.** If the testing and monitoring described in this Section 13 reveal any material deficiencies or weaknesses, DataRobot shall promptly take such steps as may be required, in DataRobot's reasonable discretion, to remediate, taking into consideration their criticality based on their nature, severity and likelihood.