DATA SECURITY SCHEDULE

This Data Security Schedule (“**Schedule**”) sets forth the technical and organizational measures that Supplier will maintain in order to protect the security of Rubrik Data during the term of the applicable agreement in place between Rubrik and Supplier (the “**Agreement**”). In the event of an inconsistency between the terms of the Agreement and the terms of this Schedule, this Schedule will govern. All capitalized terms used but not defined herein have the meanings ascribed to them in the Agreement.

Security Measures

Supplier has implemented and maintains reasonable technical, physical, and organizational security measures in accordance with industry standard practices commensurate for companies in similarly situated industries as Supplier, including those security measures included within the services or products Supplier provides to Rubrik under the Agreement (collectively, the "**Services**”), in order to protect Rubrik Data against any unauthorized disclosure, access, alteration, or unlawful destruction. Supplier maintains and enforces a written information security and data protection program, including policies and procedures that are aligned with industry standards.

Additionally, Supplier maintains a risk management program for purposes of identifying and mitigating security and data concerns proactively, and as such, risks are continuously monitored, measured, and mitigated in accordance with industry practices. Further, Supplier will routinely enhance security measures for the Services in line with current industry standard security practices.

Domain	Control Practices
Information Security Policies	**Information Security Policies.** Supplier maintains Information Security Policies which establish the framework for the management of information security within Supplier and apply to the entire Information Security Management System (“**ISMS**”). The ISMS encompasses the overall management processes that address planning, implementing, maintaining, reviewing, and improving Supplier’s information security procedures and processes. Policies are reviewed at least annually or during significant organizational changes. **Supplier’s Information Security Policies document organizational requirements for:** ● the baseline information security elements applicable to the design and implementation of the Services; ● assessing and managing risks from external threats as well as authorized insiders; ● multi-tenancy and cloud service customer isolation (including virtualization); ● access to cloud service customer assets by Supplier personnel; ● access control procedures such as strong authentication for administrative access to cloud services; ● change management; ● virtualization security; and, ● access to and protection of customer data.
	Internal Organization:

Domain	Control Practices
Organization of Information Security	Supplier implements and maintains organizational Information Security Policies for all employees, consultants, service Suppliers, Suppliers, and other external agencies which have access to Supplier systems or information. Supplier has appointed one or more security officers who are responsible for coordinating and monitoring Supplier's security posture in accordance with Supplier's Information Security Policies and with applicable laws and regulations. In addition, Supplier has developed an enterprise-wide information security program that includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance. ● Supplier separates support roles and responsibilities to prevent conflicting duties and areas of responsibility. Supplier applies responsibility segregation to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets. ● Supplier has implemented roles and processes to build information security requirements for the continued enhancement of the Services. **Mobile Devices and Remote Work:** Supplier has established organizational security requirements, including usage restrictions, configuration/connection requirements, and usage of mobile device management.
Human Resources Security	**Prior to Employment:** Supplier has implemented security measures at the beginning of the Supplier employment lifecycle with employee background screening, documented security standards within the employee handbook, terms and conditions of employment that obligate employees to adhere to security standards and defining responsibilities to enforce security measures based on role. **During Employment:** Supplier has developed and maintains an information security awareness, education, and training program to continuously increase data privacy and security knowledge of its workforce. ● Supplier has established and makes readily available to individuals requiring access to certain information systems, the processes, and procedures with regard to the information system usage. ● Supplier has developed and communicates the disciplinary processes and actions Supplier will implement for those employees who violate information security policies or commit an information security breach. **Termination and Change of Employment:** Employees who leave Supplier are interviewed and reminded of their obligations of confidentiality upon exit. All role and responsibility changes are communicated to Supplier personnel. All access to Supplier systems and information shall be promptly terminated for any Supplier personnel leaving, but in no event more than twenty-four (24) hours after their exit.
Asset Management	**Responsibility for Supplier Assets:** Supplier has developed procedures to maintain an inventory of information systems and data. All Supplier assets are assigned to a responsible individual, who is responsible to protect the asset and any Rubrik Data that is stored or processed with the Supplier asset.

Domain	Control Practices
	Supplier has developed policies specifically for describing the acceptable use of Supplier assets. These policies detail the rules for how assets and information processing activities within those assets must be carried out and describe the asset owners' requirements to enforce baseline security measures. Upon termination of an individual's employment, Supplier obtains all physical assets and information assigned to or held by the individual. If the individual was the responsible party of a digital asset, ownership and security responsibilities will be reassigned. **Information Classification:** Supplier has developed processes to classify data within the organization, which then corresponds to different security safeguards based on the classification. **Labeling of Information:** Supplier has developed and implemented policies and procedures for information labeling and employees are educated and trained on the data classification scheme, including as it pertains to any Rubrik Data. **Restrictions on Data:** Supplier imposes restrictions on printing or copying any customer data, including Rubrik Data, to only those uses that are necessary for the performance of the Services. **Media Handling:** Supplier maintains policies and procedures which establish the requirements of the implementation of media protection and media protection controls including the management of removable media, the disposal of media, and the physical transfer of media.
Access Control	**Business Requirement of Access Control:** Supplier has implemented and maintains appropriate access controls and segregation of duties in the assignment of all critical job functions related to its processing of Rubrik Data and the Services. ● Supplier will limit access to Rubrik Data to personnel using the concept of "least privileged access," and as a result, individuals are granted access to only those systems that are required to perform their defined responsibilities. Supplier applies the concept of "least privileged access" to customer environments, Supplier's network, Supplier's assets, and to physical access within Supplier's facilities. ● Privileged access for Supplier personnel will be audited on a periodic basis as a minimum standard to confirm that the concept of "least privileged access" is implemented. In addition, Supplier limits access of Rubrik Data to those personnel who have been trained in Supplier's information security practices and are bound by an obligation of confidentiality. ● Supplier maintains continuous training on new security practices, privacy standards, and organizational policies, which occur at least on an annual basis to build upon Supplier's employees' body of knowledge. **User Access Management:** ● Supplier manages Privileged Access Rights, the access given to privileged or super users such as Supplier's system administrators, through the use of the concept of "least privileged access". Privileged Access Rights are under increased scrutiny and review. ● Supplier reviews the access privileges accounts possess to continuously

Domain	Control Practices
	enforce the concept of “least privileged access”. **System and Application Access Control:** Supplier leverages current industry standard methods to control access to applications and if applicable, to the Services through Single Sign-On and Multi-Factor Authentication. ● Access to application system functions and information are restricted in accordance with Supplier’s Access Control Policy. ● Access to systems with increased security measures and access to Supplier environments are defined within the Access Control Policy and are controlled by a secure access procedure. ● Supplier enforces the concept of “least privileged access” on all information systems containing Supplier’s source code.
Cryptography	**Cryptographic Controls:** To the extent technically feasible, but in all situations where required by applicable law, Supplier agrees to store and transmit Rubrik Data in a commercially reasonable format using current industry accepted encryption technology. ● The Services offer current industry standard encryption methods to protect Rubrik Data stored on-premises or in a cloud environment and to protect Rubrik Data while in transit. ● To the extent applicable to the Services, Supplier provides documentation to customers about how to leverage encryption capabilities within the Services and allows Supplier to apply its own where feasible. **Key Management:** Supplier has implemented and maintains policies and procedures on the use, protection, and lifecycle of cryptographic keys and key management.
Physical and Environmental Security	**Secure Areas:** Supplier implements and maintains reasonable physical security safeguards for Supplier facilities. For third-party data centers where Rubrik Data may be stored as part of the Services, industry standard physical and technical security measures are implemented. ● Physical access to Supplier’s third-party data centers is restricted to authorized Supplier personnel and is provisioned based on roles and responsibilities. A review of access to third-party data centers is performed on a periodic basis by Supplier management. ● Supplier maintains access control mechanisms such as badging requirements for its onsite personnel and visitors and uses badges and video surveillance cameras to monitor and restrict individual physical access to sensitive areas. ● Supplier has a physical security policy that mandates security requirements for internal and third-party security personnel. **Equipment Security:** Supplier has implemented and maintains policies and procedures for the protection of Supplier’s physical equipment to prevent against loss, damage, theft, or compromise of assets and interruption to Supplier’s operations.

Domain	Control Practices
	Unattended User Equipment: Supplier has implemented and maintains a policy requiring Supplier employees to lock Supplier-managed laptops and workstations (devices) when the employee steps away from the device. Supplier enforces a technical measure to automatically lock devices after a period of inactivity.
Operations Security	**Clear Desk and Clear Screen Policy:** Supplier has implemented and maintains a clear desk and clear screen policy. **Operational Procedures and Responsibilities:** Supplier has implemented and maintains policies and operating procedures for user interaction with the Services and information processing systems used internally. ● Supplier has documented and makes available for all applicable internal users, documented operating procedures, change management procedures, capacity planning procedures, and procedures for the separation of development and operational environments. **Protection from Malware:** Supplier employs malicious code protection mechanisms on information systems and within the software development lifecycle process to detect and treat malicious code. ● Supplier conducts scans of information systems and hosted applications for vulnerabilities. When new vulnerabilities are discovered that may affect Supplier systems, additional scans may be performed to test remediation of discovered issues. **Penetration testing and Vulnerability management:** Supplier conducts annual application penetration testing by an independent third-party organization for the Services and/or applications within the scope of the Services. Supplier's customers are not permitted to perform penetration tests on the Services and/or applications. Supplier will also engage in social engineering penetration testing to test the security posture and awareness of Supplier's personnel. Further, Supplier will complete internal and external vulnerability scans of its systems and will periodically update and patch operating systems, applications, firewalls, and all other in-scope systems and applications and remediate or mitigate critical and high vulnerabilities within 7 and 15 calendar days. **Backup:** To the extent applicable, Supplier utilizes practices, including redundancy, fail-over, and industry standard backup practices to provide the Services with minimal unplanned interruptions and to protect against the loss of Rubrik Data. **Logging and Monitoring:** Supplier maintains processes to confirm that authorization for access to Rubrik Data has been approved by the appropriate Supplier management personnel. Access to all systems processing Rubrik Data is logged. Audit logs will follow industry standard practices allowing Supplier to identify and monitor system access. If access to Rubrik Data is no longer necessary, Supplier will remove such personnel's access promptly.
Communications Security	**Network Security Management:** Supplier maintains firewalls and security monitoring capabilities that monitor traffic on Supplier's networks in connection with the Services. Firewalls are used to protect Supplier's networks from the internet and separate the internal network from the internet and customers connections. Firewall settings have been configured to deny traffic by default and allow only authorized traffic in accordance with Supplier standards. Supplier

Domain	Control Practices
	periodically reviews and validates firewall rulesets.
System Acquisition, Development, and Maintenance	**Security Requirements of Information Systems:** Supplier has implemented and maintains a security program which establishes requirements for all information systems and processes. **Security in Development and Support Processes:** Supplier adheres to security and privacy by design principles and builds those principles into the Services such that security and privacy are considered throughout the development process. ● Supplier's development practices include assessing security vulnerabilities following industry standard guidance, such as OWASP Top 10, SANS Top 20, and CIS Control Benchmarks. Supplier's formal Software Development Life Cycle ("**SDLC**") policy governs the development, acquisition, configuration, implementation, and maintenance of system components. Supplier Management reviews and approves the policies covering SDLC on an annual basis.
Supplier Relationships	**Information Security in Supplier Relationships:** Supplier has implemented and maintains policies and procedures which establish requirements for mitigating the risks associated with each supplier's access to Supplier's assets. ● Supplier requires that suppliers of external services comply with Supplier's information security requirements or that the suppliers' requirements meet or exceed Supplier's security baseline. **Supplier Management:** Supplier has implemented and maintains policies and procedures which require the regular monitoring, review, and audit of suppliers based on risk and the services provided. Supplier selects suppliers that meet the baseline security requirements of the organization before suppliers begin providing services to Supplier.
Information Security Incident Management	**Management of Information Security Incidents and Improvements:** ● Supplier has implemented and maintains detection tools to prevent data exfiltration through laptops, workstations, and cloud environments. ● Supplier monitors its on-premise and multi-cloud environments 24x7, detects security threats, investigates, and responds to security events and incidents. ● Supplier has established and maintains automated alerts to inform security personnel of irregular activity to mitigate the risk of insider threats. Alerts are processed to determine the outcome of any identified irregularities. ● Supplier has implemented and maintains an Incident Response Policy which includes directions to be followed in the event of any action deemed a security incident. This policy includes the roles and responsibilities of personnel assigned to the security incident, the leadership responsibilities, command and control methods, and guidance on developing and implementing corrective action plans. ● Supplier's Incident Response Policy includes management responsibilities to establish a prompt, effective, and orderly response to

Domain	Control Practices
	information security incidents. **Data Breach Management:** Supplier has implemented and maintains a written security incident response program, including event reporting and escalation procedures, that are used by Supplier's personnel to report and manage security incidents, including any data breaches. ● The incident response program is regularly tested, including through tabletop exercises involving all departments of Supplier having responsibilities relating to breach responses. To the extent permitted and in accordance with applicable Data Protection Laws, Supplier will promptly, but in no later than forty-eight (48) hours, notify Rubrik of any confirmed breach of Rubrik Data. Supplier will cooperate with Rubrik's reasonable requests for information regarding any such data breach, and Supplier will provide regular updates, upon request, on the incident and the investigative action and corrective action taken.
Audit	Supplier agrees to have audits performed by independent external auditors to verify its technical and organizational measures. Such audits will be conducted: (a) by a qualified independent third party; (b) at least annually; (c) in accordance with SOC 2 or ISO 27001 standards or substantially equivalent standards; and (d) will result in an audit report ("Report"). Upon Rubrik's written request, and subject to the confidentiality obligations set forth in the Agreement, Supplier agrees to make available the Report and its applicable certifications in order to demonstrate the technical and organizational measures implemented by Supplier. Supplier will also provide information on Supplier's compliance program and submit to a reasonable data security and privacy compliance audit by Rubrik, or at Rubrik's request, by an independent third party, or customers of Rubrik, to verify compliance with the security and privacy standards set forth in this DPA, or applicable law, and any other applicable contractual obligations. Supplier must permit Rubrik, or its agent or authorized third-party or regulator ("Authorized 3P - Defined term") to request and/or perform at the expense of Rubrik, up to one (1) security assessment per year by filling out a security questionnaire and comprising a review of policies, processes, and procedures. Such assessment will be communicated at least one (1) month in advance and conducted at a time mutually agreed upon between the Supplier and Rubrik. Supplier shall remediate mutually agreed gaps identified by the audit or security review process within a mutually agreed time period, otherwise Rubrik may terminate the Agreement. Rubrik may share the results of the audit with the "Authorized 3P".
Business Continuity Management	In the event of any unforeseen or unpreventable events and emergencies, such as: ● Utility interruptions; ● Labor shortages; ● Equipment failures; ● Interruption from externally provided products, processes and services; ● Recurring natural disasters; ● Infrastructure disruptions; ● Cyber-attacks on Supplier or Supplier's suppliers' systems, Supplier has implemented and maintains processes and procedures to minimize the disruption of important and time critical operations, even during an emergency.

Domain	Control Practices
	Supplier’s Business Continuity program guides personnel to establish and implement a consistent management and response method in order for Supplier to perform mission-critical functions and services under threats and adverse conditions. In addition, Supplier leverages systems and services with high availability and redundancy. Supplier will perform business impact assessments on a periodic basis to identify critical business functions. Suppliers will also perform annual tests and exercises of business contingency plans (such as, Business Continuity Plans/ Disaster Recovery plans) that satisfies industry standards for defined RTO/RPO. Evidence of testing will be provided to Rubrik upon request. Supplier will notify Rubrik of any crisis, threat, warning or cyber event against the Supplier that is reasonably likely to have an adverse impact on the Services provided to Rubrik or its customers.
Compliance	**Compliance with Legal and Contractual Requirements:** Supplier has implemented and maintains policies and procedures to manage compliance with applicable legislative, regulatory, and contractual requirements. ● Supplier’s personnel work to identify, document, and maintain compliance-based requirements for all information systems and processing activities within the organization. ● Procedures for protecting records from loss, destruction, falsification, unauthorized access, and unauthorized release have been implemented and are maintained in accordance with applicable legislative, regulatory, contractual, and business requirements. ● Supplier has implemented and maintains policies and procedures establishing the requirements for utilizing appropriate industry standard cryptographic controls to comply with customer agreements, legislation, and regulations. **Technical Compliance Review:** Supplier has implemented and maintains policies and procedures to assess the security controls Supplier has implemented to establish reasonable security measures that safeguard Supplier’s operations and Rubrik Data.