RUBRIK, INC.
DATA SECURITY SCHEDULE

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

Security Measures

Rubrik has implemented and maintains reasonable technical, physical, and organizational security measures in accordance with industry practices, including those security measures included within the Rubrik Service, to protect Customer Data against any unauthorized disclosure, access, alteration, or unlawful destruction. Rubrik maintains and enforces a written information security and data protection program, including policies and procedures that are aligned with industry standards.

Additionally, Rubrik 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, Rubrik will routinely update security measures for the Rubrik Service in line with current industry practices, provided, however, that such updates will be designed to enhance and not materially diminish the security measures set forth herein. The Rubrik Service offers certain features and functions with security and privacy options that customers may select and use to protect Customer Data.

Domain	Control Practices
Policies & Organization of Information Security	Rubrik maintains information security policies which establish the framework for the management of information security within Rubrik 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 Rubrik's information security procedures and processes. Policies are reviewed at least annually or during significant organizational changes. Rubrik implements and maintains organizational Information Security Policies for all employees, consultants, service providers, vendors, and other external agencies which have access to Rubrik systems or information. Rubrik develops and disseminates an enterprise-wide information security program that includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance. ● Rubrik separates support roles and responsibilities to prevent conflicting duties and areas of responsibility. Rubrik applies responsibility segregation to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets. ● Rubrik has implemented roles and processes to build information security requirements for the continued enhancement of the Rubrik Service. ● Rubrik has a Chief Information Security Officer, or equivalent executive, that is designated as responsible for coordinating, managing, and monitoring the information security function, policies, and procedures.
Certifications and Audits	Rubrik maintains security controls to meet certification and attestation for the objectives stated in ISO, and SOC data protection series, and NIST or equivalent standards for its security program. At least once per calendar year, an assessment against such standards and audit methodologies by an independent third-party auditor will be obtained for the Rubrik Service. Rubrik's certifications and attestations can be found here: https://www.rubrik.com/compliance-program Upon written request and at no additional cost to Customer, Rubrik will provide Customer, and/or its appropriately qualified third-party representative(s) (collectively, the "**Auditor**"), access to

Domain	Control Practices
	reasonably requested documentation evidencing Rubrik's compliance with its security obligations in the form of, as applicable, (i) ISO 27001, 27017, 27018, SOC 2 Type II audit report and other similar audit reports; (ii) most recently completed industry standard security questionnaires, such as a SIG or CAIQ; and (iii) architecture and data flow diagrams (in collaboration with the Customer) for the Rubrik Service (the foregoing i) to iii) constitute an "**Audit**"). To the extent that Customer has not reasonably been able to satisfy its internal requirements by following the procedure outlined in this clause, Rubrik will provide Customer with such further assistance by evidencing documentation, and providing additional information as may reasonably be required (in accordance with the assistance obligations described herein) to substantially satisfy such requirements.
Human Resources Security	**Prior to Employment:** Rubrik has implemented security measures at the beginning of the Rubrik 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:** Rubrik has developed and maintains an information security awareness, education, and training program to continuously increase data privacy and security knowledge of its workforce. ● Rubrik has established and makes readily available to individuals requiring access to certain information systems, the processes and procedures regarding the information system usage. ● Rubrik has developed and communicates the disciplinary processes and actions Rubrik will implement for those employees who violate information security policies or commit an information security breach. **Termination and Change of Employment:** Employees who leave Rubrik are interviewed and reminded of their obligations of confidentiality upon exit. All role and responsibility changes are communicated to Rubrik personnel.
Asset Management	Rubrik has developed procedures to maintain an inventory of information systems and data: ● Rubrik has developed policies specifically for describing the acceptable use of Rubrik 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, Rubrik 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. **Data Classification:** Rubrik has implemented processes to classify data within the organization based on sensitivity. Rubrik's security safeguards are considerate of and commensurate with the respective data classification level. **Data Labeling:** Rubrik has implemented policies and procedures for data labeling. Employees are educated and trained on the data labeling and classification scheme. **Media Handling:** Rubrik maintains policies and procedures establishing the requirements for media handling and media protection controls, including: the management of removable media, the disposal of media, and the physical transfer of media. Before final disposition of such media or for deletion of data, including the deletion of Customer Data at Customer's request, Rubrik follows industry standards such as NIST 800-88 (or substantially equivalent).

Domain	Control Practices
Access Control	Rubrik has implemented the principle of least privilege to govern and restrict access to Customer Data and to Rubrik's network and assets, which includes: (i) user access management; (ii) system and application access control; (iii) Rubrik-managed device control; (iv) regular review and audits; and (v)segregation of duties in the assignment of all critical job functions related to its Processing of Customer Data and the Rubrik Service provided to the Customer. **Rubrik User Access Management** ● Rubrik limits personnel access to its systems and Customer Data based on defined roles and responsibilities. Personnel are only granted access to systems as necessary for performing their specific duties. ● Duties are divided among different individuals or systems to prevent any single entity from having control over all aspects of a critical task, reducing the risk of unauthorized use, sabotage, fraud or error. **Customer User Access Management:** The Rubrik Service offers a formal user registration and de-registration process to enable the assignment of access rights. ● Customers have the ability to authorize users' access to the Rubrik Service based on roles, group membership, or other attributes. Customers are able to control access to specific attributes or elements of the Rubrik Service with fine-grained privileges. **System and Application Access Control:** Rubrik leverages industry standard methods to control access to applications and the Rubrik Service through Single Sign-On and Multi-Factor Authentication. ● Access to application system functions and information are restricted in accordance with Rubrik's Access Control Policy. ● Access to systems with increased security measures (e.g., systems containing Rubrik's source code and Customer Data), and access to Customer environments are defined within the Access Control Policy and are controlled by secure access procedures. ● Rubrik manages access given to privileged or super users, such as Rubrik's system administrators, with an increased level of scrutiny and review. **Rubrik-Managed Device Control and Remote Work:** Rubrik has tools that provide industry standard anti-virus, endpoint detection and response, and advanced threat hunting and has established organizational security and access control requirements for all managed devices, including usage restrictions, configuration/connection requirements, and usage of mobile device management. **Regular Reviews:** Rubrik audits the privileged access permissions of its personnel on a periodic basis to evaluate the necessity for access and continuously reinforce the concept of "least privileged access". In addition, Rubrik limits access to Customer Data to those privileged personnel who have been trained in Rubrik's information security practices and are bound by an obligation of confidentiality.
Cryptography	To the extent technically feasible, and in all situations where required by applicable law, Rubrik stores and transmits Customer Data using industry accepted strong encryption technology. ● The Rubrik Service offers industry standard encryption methods to protect Customer Data stored on-premises or in a cloud environment and to protect Customer Data while in transit. ● Rubrik provides documentation to customers about how to leverage encryption capabilities, as well as other controls, features or functionalities, to protect Customer Data within the Rubrik Service. Where Customer Data is stored in Rubrik's Azure instance

Domain	Control Practices
	(for example, Rubrik for M365), Rubrik provides the ability for the customers to leverage Bring Your Own Key (BYOK). **Key Management:** Rubrik has implemented and maintains policies and procedures on the use, protection, and life cycle of cryptographic keys and key management.
Physical Security	Rubrik implements and maintains reasonable physical security safeguards for Rubrik facilities. To the extent Rubrik leverages third-party data centers to store Customer Data as part of the Rubrik Service, they are validated to have implemented industry standard physical and technical security measures as part of Rubrik's third party risk management program. ● Physical access to Rubrik facilities is restricted to authorized Rubrik personnel and is provisioned based on roles and responsibilities. A review of access to Rubrik facilities is performed on a periodic basis by Rubrik management. ● Rubrik 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. ● Rubrik has a physical security policy that mandates security requirements for internal and third-party security personnel. **Equipment Security:** Rubrik has implemented and maintains policies and procedures for the protection of Rubrik managed physical equipment to prevent loss, damage, theft, or compromise of assets and interruption to Rubrik's operations. **Unattended User Equipment**: Rubrik has implemented and maintains a policy requiring Rubrik employees to lock Rubrik managed laptops and workstations (devices) when the employee steps away from the device. Rubrik enforces a technical measure to automatically lock devices after a period of inactivity. **Clear Desk and Clear Screen Policy:** Rubrik has implemented and maintains a clear desk and clear screen policy.
Operations Security & Penetration Testing	Rubrik has implemented and maintains policies and operating procedures for user interaction with the Rubrik Service and information processing systems used internally. ● Rubrik 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. **Malware Protection:** Rubrik employs malicious code protection mechanisms on information systems and within the software development lifecycle process to detect and treat malicious code. ● Rubrik conducts scans of information systems and hosted applications for vulnerabilities. When new vulnerabilities are discovered that may affect Rubrik systems, additional scans may be performed to test remediation of discovered issues. **Penetration Testing:** While Customers are not permitted to perform penetration tests on the Rubrik Service and/or applications, Rubrik conducts annual application penetration testing using an independent third-party organization for the Rubrik Service and/or applications within the scope of the Rubrik Service provided to Customers. Executive summary reports from the penetration testing are made available to customers upon request, subject to confidentiality obligations. Rubrik also engages in social engineering penetration testing to test the security posture and awareness of Rubrik's personnel.

Domain	Control Practices
	Backup and Resiliency: Rubrik utilizes data redundancy, fail-over, and industry standard backup practices to provide the Rubrik Service with minimal unplanned interruptions and to protect against the loss of Customer Data.
Vulnerability management	Rubrik applies a risk-based, continuous remediation approach to vulnerability management and adheres to strictly enforced service levels for certain known vulnerabilities that present risk. Among other industry standards, Rubrik uses OWASP Top 10 and SANS Top 20 to identify and remediate critical and high severity vulnerabilities prior to releasing software into production. **Detection:** Rubrik conducts periodic internal, external, and third-party scans and testing of its source code, systems, applications, and the Rubrik Service to identify vulnerabilities. In cloud workloads, Rubrik uses data leakage monitoring and cloud security posture management tooling to monitor for security issues. Additionally, Rubrik operates both bug bounty and vulnerability disclosure programs to expand its capability for detecting vulnerabilities. **Triage and Evaluation:** Newly discovered or reported vulnerabilities are checked for applicability to the Rubrik Services, and if applicable, issues are further assessed to confirm the contextual security risk and severity applicable to each instance of the vulnerability. Rubrik uses CVSS scoring in line with industry practices to establish severity and may adjust a severity rating and/or remediation timeline in light of an instance's compensating controls and mitigating factors, if any. **Remediation:** Based on risk and severity, hot fixes, patches, and/or updates, are tested and then deployed on operating systems, applications, firewalls, and in-scope components to remediate or mitigate known vulnerabilities. Issues are mapped to firm remediation deadlines based on their contextually confirmed severity and criticality. Where there is a dependency on a supply chain vendor, Rubrik monitors closely for the release of a fix so that remediation can be achieved without undue delay. **Post Remediation:** Impacted components are rescanned or validated after remediation to confirm that the issue is fixed, and timeliness of resolution is checked as a key measure of performance against service levels. For vulnerabilities with broader impact and applicability as part of a security event, Rubrik personnel conduct a debrief to establish lessons learned and ensure that response and resolution procedures are updated where needed.
Logging and Monitoring	Rubrik implements and maintains processes designed to confirm that authorization for access to Customer Data has been approved by the appropriate Rubrik management personnel. Access to all systems processing Customer Data is logged. ● Audit logs: industry standard practices allowing Rubrik to identify and monitor system access. If access to Customer Data is no longer necessary, Rubrik will remove such personnel's access promptly. ● Infrastructure logs: monitoring tools or services, such as host-based intrusion detection tools, are utilized to log certain activities and changes within the cloud environments. These logs are further monitored and are securely stored for at least one year. ● Rubrik provides features and capability to export logs from the Rubrik Services to the Customer's Security Information and Event Management (SIEM) systems through webhook integrations.
Network Security	Rubrik maintains network security devices and security monitoring capabilities for controlling and monitoring traffic on Rubrik's networks in connection with the Rubrik Service. ● Firewalls and other network-based devices are used to segment and segregate Rubrik's networks to protect Customer Data. Firewall settings are configured to deny traffic by default and allow only authorized traffic in accordance with Rubrik standards. Rubrik

Domain	Control Practices
	periodically reviews and validates firewall rulesets. Access to production systems and environments is managed through Single Sign-On (SSO) and secured with Two-Factor Authentication (2FA) and facilitated via a Virtual Private Network (VPN) and includes secure gateway, and continuous verification of user identity and device.
Software Development Life Cycle	Rubrik has implemented and maintains a security program that establishes security requirements for all information systems and processes**.** Rubrik adheres to security and privacy by design principles and integrates those principles into the Rubrik Service such that security and privacy are considered throughout the development process. ● Rubrik's development practices include assessing security vulnerabilities following industry standard guidance, such as OWASP Top 10, SANS Top 20, and CIS Control Benchmarks. Rubrik's formal Software Development Life Cycle ("**SDLC**") policy governs the development, acquisition, configuration, implementation, and maintenance of system components. ● At a minimum, Rubrik's management team(s) reviews and approves the policies covering SDLC on an annual basis.
Third-Party Risk Management	**Information Security in Vendor Relationships:** Rubrik has implemented and maintains policies and procedures that establish requirements for assessing and mitigating the risks associated with each vendor's access to Rubrik's assets in connection with the Rubrik Service. ● Rubrik requires providers of third-party services to meet or exceed Rubrik's information security requirements. **Risk Management:** Rubrik has implemented and maintains policies and procedures that require regular monitoring, re-assessment, and audits of vendors based on risk and the nature of the services provided. ● Rubrik conducts an initial vendor review, including a risk assessment of each vendor's security controls, to evaluate and select vendors that meet its information security requirements. Any selected vendor must meet Rubrik's information security requirements prior to the commencement of any third-party services. In addition to an initial assessment, Rubrik undertakes an annual assessment of its vendors, consisting of a comprehensive review of their security controls.
Information Security Incident Management	Rubrik has implemented and maintains detection tools to prevent data exfiltration through Rubrik provided laptops, workstations, and cloud environments. ● Rubrik monitors its on-premises and multi-cloud environments 24x7, detects security threats, investigates, and responds to security events and incidents. ● Rubrik 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. ● Rubrik 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. ● Rubrik's Incident Response Policy includes management responsibilities to establish a prompt, effective, and orderly response to information security incidents.

Domain	Control Practices
	Data Breach Management: Rubrik has implemented and maintains a written security incident response program, including event reporting and escalation procedures, that are used by Rubrik'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 Rubrik having responsibilities relating to breach responses. ● To the extent permitted and in accordance with applicable Data Protection Laws, Rubrik will promptly, but in no later than seventy-two (72) hours, notify the Customer of a confirmed breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data ("**Security Breach**"). Rubrik will, to the extent available, provide Customer with a description of (i) the nature of the Security Breach; (ii) likely consequences of the Security Breach; and (iii) corrective action plans, mitigation measures, and timelines involved in addressing the Security Breach. Rubrik will cooperate with Customer's reasonable requests for additional information and regular updates regarding any such Security Breach. **Breach notifications:** In order to be notified in the event of a Security Breach**,** Customer will provide contact details of the responsible party to be notified in the event of a Security Breach. The contact details may include but are not limited to that of the Customer's Chief Information Security Officer (CISO), Chief Technology Officer (CTO), Chief Operating Officer (COO), Chief Information Officer (CIO), Incident Management team, Compliance team and the Risk Management team.
Business Resiliency and Continuity Management	**Business Resiliency Program:** While Rubrik continually strives to anticipate and prevent problems from occurring, Rubrik recognizes that the potential exists for 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; ● Infectious diseases (e.g., COVID-19); ● Infrastructure disruptions; ● Cyber-attacks on Rubrik or Rubrik's suppliers' systems In the event of an unforeseen or unpreventable event, Rubrik has implemented and maintains processes and procedures to minimize the disruption of important and time critical operations, even during an emergency. ● Rubrik's Business Resiliency program guides personnel to establish and implement a consistent management and response method in order for Rubrik to perform mission-critical functions and services under threats and adverse conditions. ● In addition, Rubrik leverages systems and services with high availability and redundancy. **Disaster Recovery:** Rubrik maintains a Disaster Recovery Plan (DRP) to address disaster recovery that is consistent with industry standards, for applicable Rubrik Services. The DRP is tested at least once every year and remediation action plans are documented and prioritized to promptly address and resolve any deficiencies or concerns.

Domain	Control Practices
Legal and Contractual Compliance Requirements	Rubrik has implemented and maintains policies and procedures to manage compliance with applicable legislative, regulatory, and contractual requirements. ● Rubrik'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.
Shared Responsibility	Rubrik and its Customers operate under a shared responsibility model, where each has obligations and responsibilities as it relates to security and the Rubrik Service. The obligations described within this DSS are only applicable to the Rubrik Service and do not apply to: (i) information shared with Rubrik that is not Customer Data; or (ii) any data processed by Customer or its users in violation of this DSS or the Agreement. Before providing any data to Rubrik in connection with the Rubrik Service, Customers are responsible for: (i) reviewing Rubrik's security program and making an independent determination as to whether it meets Customer's requirements, taking into account the type and sensitivity of the provided Customer Data; and (ii) implementing access control functionalities within the instance to protect Customer Data. After providing any data to Rubrik in connection with the Rubrik Service, Customers are responsible for the ongoing implementation, configuration, and other day-to-day operations of Customer's instance of the Rubrik Service. Rubrik provides a variety of security capabilities that enable Customers to configure the security of the Rubrik Service based on their requirements. Such capabilities include, but are not limited to, the ability to: (i) authenticate users before accessing the Rubrik Service; (ii) manage access Credentials; (iii) access the Rubrik Service audit logs; (iv) configure and maintain industry-standard security controls to manage access to their infrastructure, devices, equipment, and applications that interface with the Rubrik Service (v) secure the Rubrik Service in their environments per the requirements prescribed in the security hardening documentation provided by Rubrik.