# RUBRIK, INC DATA SECURITY SCHEDULE

This Data Security Schedule ("**Schedule**") sets forth the technical and organizational measures that Rubrik and Customer will maintain in order to protect the 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 Schedule, this Schedule 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, in order 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 enhance security measures for the Rubrik Service in line with current industry practices. 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 |
|---|---|
| **Information Security Policies** | **Information Security Policies.** 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.<br>**Rubrik's Information Security Policies document organizational requirements for:**<br>• the baseline information security elements applicable to the design and implementation of the Rubrik Service;<br>• assessing and managing risks from external threats as well as authorized insiders;<br>• multi-tenancy and cloud service Customer isolation (including virtualization);<br>• access to cloud service Customer assets by Rubrik personnel;<br>• access control procedures such as strong authentication for administrative access to cloud services;<br>• change management;<br>• virtualization security; and,<br>• access to and protection of Customer Data. |

| Domain | Control Practices |
|---|---|
| **Organization of Information Security** | **Internal Organization:** 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.<br>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.<br>• 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.<br>• Rubrik has implemented roles and processes to build information security requirements for the continued enhancement of the Rubrik Service.<br>**Mobile Devices and Remote Work:** Rubrik has established organizational security requirements, including usage restrictions, configuration/connection requirements, and usage of mobile device management. |
| **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.<br>**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.<br>• Rubrik 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.<br>• 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.<br>**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** | **Responsibility for Rubrik Assets:** Rubrik has developed procedures to maintain an inventory of information systems and data. All Rubrik assets are assigned to a responsible individual, who is responsible to protect the asset and any Customer Data that is stored or processed with the Rubrik asset.<br>• 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 describes the asset owners' requirements to enforce baseline security measures. |

| Domain | Control Practices |
|---|---|
| | • 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.<br>**Information Classification:** Rubrik has developed processes to classify data within the organization, which then corresponds to different security safeguards based on the classification.<br>**Labelling of Information:** Rubrik has developed and implemented policies and procedures for information labelling and employees are educated and trained on the data classification scheme.<br>**Media Handling:** Rubrik 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:** Rubrik has implemented and maintains appropriate access controls and 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.<br>• Rubrik will limit access to Customer 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. Rubrik applies the concept of "least privileged access" to customer environments, Rubrik's network, Rubrik's assets, and to physical access within Rubrik's facilities.<br>• Privileged access for Rubrik personnel will be audited on a periodic basis as a minimum standard to confirm that concept of "least privileged access" is implemented. In addition, Rubrik limits access of Customer Data to those personnel who have been trained in Rubrik's information security practices and are bound by an obligation of confidentiality.<br>• Rubrik maintains continuous training on new security practices, privacy standards, and organizational policies, which occur at least on an annual basis to build upon Rubrik's employees' body of knowledge.<br>**User Access Management:** The Rubrik Service offers a formal user registration and de-registration process to enable the assignment of access rights.<br>• 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.<br>• Rubrik manages Privileged Access Rights, the access given to privileged or super users such as Rubrik's system administrators, through the use of the concept of "least privileged access". Privileged Access Rights are under increased scrutiny and review.<br>• Rubrik reviews the access privileges accounts possess to continuously enforce the concept of "least privileged access". |

| Domain | Control Practices |
|---|---|
|  | **System and Application Access Control:** Rubrik leverages industry standard methods to control access to applications and Rubrik Service through Single Sign-On and Multi-Factor Authentication.<br>• Access to application system functions and information are restricted in accordance with Rubrik's Access Control Policy.<br>• Access to systems with increased security measures and access to Customer environments are defined within the Access Control Policy and are controlled by a secure access procedure.<br>• Rubrik enforces the concept of "least privileged access" on all information systems containing Rubrik's source code. |
| **Cryptography** | **Cryptographic Controls:** To the extent technically feasible, but in all situations where required by applicable law, Rubrik agrees to store and transmit Customer Data in a commercially reasonable format using industry accepted encryption technology.<br>• 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.<br>• Rubrik provides documentation to customers about how to leverage encryption capabilities within the Rubrik Service and allows Customer to apply its own where feasible.<br>**Key Management:** Rubrik 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:** Rubrik implements and maintains reasonable physical security safeguards for Rubrik facilities. For third-party data centers where Customer Data may be stored as part of the Rubrik Service, industry standard physical and technical security measures are implemented.<br>• Physical access to Rubrik's third-party data centers is restricted to authorized Rubrik 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 Rubrik management.<br>• 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.<br>• Rubrik has a physical security policy that mandates security requirements for internal and third-party security personnel.<br>**Equipment Security:** Rubrik has implemented and maintains policies and procedures for the protection of Rubrik's physical equipment to prevent against loss, damage, theft, or compromise of assets and interruption to Rubrik's operations.<br>**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. |

| Domain | Control Practices |
|---|---|
|  | Rubrik enforces a technical measure to automatically lock devices after a period of inactivity.<br>**Clear Desk and Clear Screen Policy:** Rubrik has implemented and maintains a clear desk and clear screen policy. |
| **Operations Security** | **Operational Procedures and Responsibilities:** Rubrik has implemented and maintains policies and operating procedures for user interaction with the Rubrik Service and information processing systems used internally.<br>• 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.<br>• Rubrik communicates information regarding the status of the Rubrik Service via [https://status.rubrik.com](https://status.rubrik.com).<br>**Protection from Malware:** Rubrik employs malicious code protection mechanisms on information systems and within the software development lifecycle process to detect and treat malicious code.<br>• 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.<br>**Penetration testing and Vulnerability management:** Rubrik conducts annual application penetration testing by an independent third-party organization for the Rubrik Service and/or applications within the scope of the Rubrik Service provided to customers. Customers are not permitted to perform penetration tests on the Rubrik Service and/or applications. Rubrik will also engage in social engineering penetration testing to test the security posture and awareness of Rubrik's personnel. Further, Rubrik 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 all such vulnerabilities in accordance with industry standard timelines based upon risk.<br>**Backup:** Rubrik utilizes practices, including 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.<br>**Logging and Monitoring:** Rubrik 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.<br>• Audit logs will follow 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. |

| Domain | Control Practices |
|---|---|
| | • Customers are responsible for configuring and maintaining industry-standard security controls to manage access to their infrastructure, devices, equipment, and applications that interface with the Rubrik Service. Customers are responsible for securing the Rubrik Service in their environments and for implementing the requirements prescribed in the security hardening documentation provided by Rubrik. |
| **Communications Security** | **Network Security Management:** Rubrik maintains firewalls and security monitoring capabilities that monitor traffic on Rubrik's networks in connection with the Rubrik Service.<br>• Firewalls are used to protect Rubrik'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 Rubrik standards. Rubrik periodically reviews and validates firewall rulesets. |
| **System Acquisition, Development, and Maintenance** | **Security Requirements of Information Systems:** Rubrik has implemented and maintains a security program which establishes requirements for all information systems and processes.<br>**Security in Development and Support Processes:** Rubrik adheres to security and privacy by design principles and builds those principles into the Rubrik Service such that security and privacy are considered throughout the development process.<br>• 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.<br>• Rubrik Management reviews and approves the policies covering SDLC on an annual basis. |
| **Supplier Relationships** | **Information Security in Supplier Relationships:** Rubrik has implemented and maintains policies and procedures which establish requirements for mitigating the risks associated with each supplier's access to Rubrik's assets.<br>• Rubrik requires that providers of external services comply with Rubrik's information security requirements or that the provider's requirements meet or exceed Rubrik's security baseline.<br>**Supplier Service Delivery Management:** Rubrik has implemented and maintains policies and procedures which require the regular monitoring, review, and audit of suppliers based on risk and the services provided.<br>• Rubrik selects suppliers that meet the baseline security requirements of the organization before suppliers begin providing services. |
| **Information Security Incident Management** | **Management of Information Security Incidents and Improvements:** Rubrik has implemented and maintains detection tools to prevent data |

| Domain | Control Practices |
|---|---|
|  | exfiltration through Rubrik provided laptops, workstations, and cloud environments.<br>• Rubrik monitors its on-premise and multi-cloud environments 24x7, detects security threats, investigates, and responds to security events and incidents.<br>• 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.<br>• 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.<br>• Rubrik's Incident Response Policy includes management responsibilities to establish a prompt, effective, and orderly response to information security incidents.<br>**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.<br>• The incident response program is regularly tested, including through tabletop exercises involving all departments of Rubrik having responsibilities relating to breach responses.<br>• 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 any confirmed breach of Customer Data. Rubrik will cooperate with Customer's reasonable requests for information regarding any such data breach, and Rubrik will provide regular updates, upon request, on the incident and the investigative action and corrective action taken. |
| **Information Security Aspects of Business Continuity Management** | **Information Security Continuity:** 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:<br>• Utility interruptions;<br>• Labor shortages;<br>• Equipment failures;<br>• Interruption from externally provided products, processes and services;<br>• Recurring natural disasters;<br>• Infrastructure disruptions;<br>• Cyber-attacks on Rubrik or Rubrik's suppliers' systems |

| Domain | Control Practices |
|---|---|
|  | 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.<br>• Rubrik's Business Continuity 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.<br>• In addition, Rubrik leverages systems and services with high availability and redundancy. |
| **Compliance** | **Compliance with Legal and Contractual Requirements:** Rubrik has implemented and maintains policies and procedures to manage compliance with applicable legislative, regulatory, and contractual requirements.<br>• Rubrik's personnel work to identify, document, and maintain compliance-based requirements for all information systems and processing activities within the organization.<br>• 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.<br>• Rubrik 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.<br>**Information Security Reviews:** Rubrik assesses the security of the computers and computing environments used in processing Customer Data (including Customer Personal Data) within the Rubrik Service.<br>Rubrik conducts certain assessments which meet the following requirements:<br>• assessments will be performed at least annually;<br>• assessment will be performed according to industry standards, such as, ISO 27001, ISO 27017, ISO 27018, SOC 2; and,<br>• assessments will be performed by independent third party security professionals at Rubrik's selection and expense.<br>**Technical Compliance Review:** Rubrik has implemented and maintains policies and procedures to assess the security controls Rubrik has implemented to establish reasonable security measures that safeguard Rubrik's operations and Customer Data. |