# TABLE OF CONTENTS

1. POLARIS OVERVIEW ................................................................. 3

2. SECURE THE PLATFORM/APPLICATION .................................................. 3
   2.1. Security Overview & Architecture ..................................................... 3
   2.2. Availability & Continuity ................................................................. 3

3. DATA MANAGEMENT ........................................................................... 4
   3.1. Polaris Partners ............................................................................. 4
   3.2. Protection of Customer Information and Records ................................. 4

4. SECURE SOFTWARE DEVELOPMENT LIFECYCLE (SDLC) PRACTICES. .................. 4

5. VULNERABILITY MANAGEMENT .......................................................... 5
   5.1. Vulnerability Scanning .................................................................. 5
   5.2. Third-Party Penetration Testing ...................................................... 5

6. ENCRYPTION/KEY MANAGEMENT ...................................................... 5

7. ACCESS MANAGEMENT ...................................................................... 5

8. LOGGING AND MONITORING ............................................................ 6

9. INCIDENT RESPONSE. ...................................................................... 6

10. POLICIES AND PROCEDURES .......................................................... 6

11. TRAINING AND AWARENESS ......................................................... 6

12. REFERENCE DOCUMENTS ................................................................. 7

13. REVISION HISTORY .......................................................................... 7
1. POLARIS OVERVIEW

Polaris is a Software-as-a-Service (SaaS) platform that is accessed via web browser. Polaris is used as a platform to deliver a unified system of record that brings all Rubrik Cloud Data Management (CDM) instances together for ease of management when customers have multiple CDM instances on-site. Within the Polaris platform, there are features such as GPS and Radar.

2. SECURE THE PLATFORM/APPLICATION

2.1. SECURITY OVERVIEW & ARCHITECTURE

Rubrik offers a comprehensive approach to security regardless of where data is located. To help facilitate the privacy and safety of enterprise data, Rubrik deploys a multi-layered security framework that consists of the following components:

- **Flexible key management:** Polaris uses key management based on Google’s Key Management Service (KMS) which has a Hardware Security Module (HSM) behind it. Information regarding Google’s Cloud KMS can be found at https://cloud.google.com/kms/docs/hsm.

- **User authentication:** Rubrik reduces the risk of data breaches and cyber-attacks by supporting the assignment of granular permissions for data access. The Rubrik platform integrates with Active Directory (AD) and supports granting authorization and groups from AD. With support for SAML 2.0, users can also securely access the cluster with single sign-on from their SAML 2.0 compatible IdP (Identify Provider). This enables users to access multiple applications with a single set of credentials without the interoperability issues associated with vendor-specific designs.

- **Data integrity:** Rubrik Cloud Data Management provides data immutability against cyber-attacks such as ransomware. No external or internal operation can modify the data since the underlying backups are read-only.

- **Centralized compliance reporting:** All user activity in the Rubrik platform is logged and made available to administrators through the Rubrik UI and APIs. The activity logs centralize compliance reporting for system operations such as backup and recovery.

2.2. AVAILABILITY & CONTINUITY

**UPTIME**

Rubrik is working on making available a publicly available system-status webpage. This page will include comprehensive information such as system availability details, scheduled maintenance, service incident history, and relevant security events.

**BUSINESS CONTINUITY AND DISASTER RECOVERY**

Rubrik’s business continuity and disaster recovery program is designed to address the risks when Rubrik services are unavailable. Business continuity and disaster recovery plans are reviewed annually and are periodically tested through tabletop tests, functional tests, or actual incidents.

**MONITORING**

Stats, log excerpts, and log bundles are used by our alerting system to generate internal Support and Engineering alerts to deliver proactive, context-aware support for Rubrik services. Diagnostic system data is securely transmitted to Rubrik, to determine the health of a cluster. Rubrik support teams monitor and analyze the data to proactively identify issues before they surface and monitor infrastructure health.
3. DATA MANAGEMENT

3.1. POLARIS PARTNERS
Rubrik works with multiple third parties to support our Polaris product. Information about our sub-processors can be found at https://www.rubrik.com/en/legal/rubrik-subprocessors.

3.2. PROTECTION OF CUSTOMER INFORMATION AND RECORDS
Polaris is designed such that it does not collect any customer’s data (e.g. files, records, etc.) housed on their CDM appliances or software. Polaris only collects customer metadata for product performance monitoring purposes. Customers’ data remains and resides on their own premises, data-centers or customer-owned cloud deployments. Metadata collected includes attributes such as Rubrik CDM cluster information (e.g., cluster name, location, use of encryption, etc.).

Polaris isolates individual customer metadata into logically partitioned databases to prevent potential data leakage and preserve data isolation between customers. Rubrik provisions customer accounts based on geographical location to address data residency concerns and requirements. For customers based in Europe, Polaris accounts are provisioned in Rubrik’s European Polaris region on Google Cloud Platform (GCP). See https://cloud.google.com/security/gdpr for GCP resources on GDPR.

All customer metadata at rest as well as in-transit between CDM and Polaris is encrypted using modern cryptography and using Google Managed Encryption Keys (more information can be found at https://cloud.google.com/storage/docs/encryption/default-keys). Sensitive fields in the database are encrypted using an encryption framework built on top of the Cloud Key Management Service (found at https://cloud.google.com/security-key-management) and Cloud IAM (found at https://cloud.google.com/iam/docs/overview). A key management hierarchy is in place to facilitate key rotation and revocation.

4. SECURE SOFTWARE DEVELOPMENT LIFECYCLE (SDLC) PRACTICES
Rubrik engineers follow secure code practices that span OWASP top ten security risks, common attack vectors, and Rubrik security controls. Rubrik leverages secure open-source frameworks with security controls to limit exposure to OWASP top ten security risks. These inherent controls reduce our product exposure to SQL injection (SQLi), cross-site scripting (XSS), and cross site request forgery (CSRF), among others.

Rubrik uses the following principles to guide the SDLC process:

- Quality in every step of the engineering process.
- Security by design, not as an afterthought.
- Continuous integration and release qualification.
- End-to-end test automation for velocity and repeatability.
- Phased product rollout with continuous customer feedback.
- Root Cause Analysis (RCA) process for continuous improvement.

Rubrik follows the release process outlined below when creating a new product:

1. **Definition**: In the definition phase, content and features are finalized for release. The engineering, product management, and support teams review and commit to requirements.

2. **Development**: During this stage, documentation is designed, tests are planned, and code is reviewed according to secure coding standards. For large projects, testing development and validation are ongoing.
3. **Hardening**: At this stage, features tests are automated and executed. There is an additional focus on system, scale, and stress tests, as well as scanning for security findings.

4. **General availability**: In the general availability phase, new features and functionality is made available for customer use.

5. **VULNERABILITY MANAGEMENT**

5.1. **VULNERABILITY SCANNING**

Rubrik employs security tooling to continuously and dynamically scan our products and related infrastructure against common security vulnerabilities. We maintain a dedicated in-house product security team to continuously test and drive remediation of any discovered issues based on internally defined service level agreements (SLAs). The source code repositories for our platform are also scanned for security issues.

5.2. **THIRD-PARTY PENETRATION TESTING**

In addition to our internal vulnerability management and security testing program, Rubrik employs independent third-party security experts to perform penetration tests continuously, and periodically.

6. **ENCRYPTION/KEY MANAGEMENT**

All customer metadata at rest as well as in-transit between a CDM cluster and Polaris is encrypted using modern cryptography and uses Google Managed Encryption Keys (found at [Google Managed Encryption Keys](#)). Sensitive fields in the database are encrypted using an encryption framework built on top of Cloud Key Management Service (found at [Cloud Key Management Service](#)) and Cloud IAM (found at [Cloud IAM](#)). A key management hierarchy is in place to facilitate key rotation and revocation.

7. **ACCESS MANAGEMENT**

Access to Rubrik’s production environment is restricted on an explicit need-to-know basis, utilizes least privilege, and is logged and monitored. Employees accessing the Rubrik production network are required to use multi-factor authentication.

**Authorization**: Polaris offers fine-grained privileges and allows for individual and group privileges to be manually created.

**Authentication Options**: Polaris supports Passwords, Security Assertion Markup Language (SAML), Active Directory (AD) and Single Sign-on (SSO). Two Factor Authentication (2FA) is supported via SSO in Polaris. Polaris does not support Client certificate unless the SSO has a client certificate as the second form of authentication.

**Hash Algorithm**: To store passwords and other authentication credentials, we use Auth0 which uses state-of-the art password management practices.

**Password Management**: Polaris requires passwords to have a minimum of 8 characters. Polaris does not allow customers to configure the password parameters.

**Account Lockout**: Polaris has built-in account lockouts to protect your accounts from unauthorized access.
8. LOGGING AND MONITORING
Polaris uses Cloud Audit Logging (found at Cloud Audit Logging) to audit logs at an infrastructure level and alert based on it. Rubrik uses Google Cloud Security Command Center (Google Cloud Security Command Center and its Security Health Analytics, Cloud Anomaly Detection and Event Threat Detection offerings.

Customers can monitor events based on the logging capabilities built into the Polaris service. Polaris aggregates audit logs from all connected clusters enabling customers to easily monitor changes across their Rubrik clusters.

9. INCIDENT RESPONSE
Rubrik’s Security Incident Response Team (SIRT) is responsible for responding to security incidents. They manage the receipt, investigation, and public reporting of information about security vulnerabilities and issues related to our products and networks.

Reporting an incident or obtaining security support:

If you identify a security issue or have a security concern related to Rubrik’s products or services, contact Rubrik Support at support@rubrik.com.

Process:

Rubrik SIRT follows the following process for vulnerability management.

1. **Awareness**: SIRT receives notification of security incident.

2. **Active Management**: SIRT prioritizes and identifies resources.

3. **Determination of a fix**: SIRT coordinates fix and impact assessment.

4. **Mitigation plan**: SIRT engages experts and executives to mitigate the issue, and Customer Support to plan notifications to customers. If applicable, appropriate contacts with relevant authorities shall be maintained.

5. **Communications**: SIRT/Customer Support send out notifications to affected customers.

6. **Postmortem**: SIRT writes a postmortem on the issue.

10. POLICIES AND PROCEDURES
Rubrik has developed a set of security policies covering a broad range of topics relevant to Rubrik’s operating environment. In addition to requiring users to acknowledge understanding of these policies through mandated annual training, they are made available on our intranet to all employees and contractors.

11. TRAINING AND AWARENESS
All employees and contingent workers are required to complete privacy and security awareness training upon hire, and annually thereafter. Rubrik’s security team also attends bi-monthly seminars to get trained on updates to products and related security topics. Additionally, we conduct regular phishing campaigns across the company and have an executive-sponsored campaign called #notonmywatch to actively instill good security behaviors and a strong security culture across Rubrik.
12. REFERENCE DOCUMENTS

- Rubrik Polaris User Guide
- Rubrik Polaris Radar Quick Start Guide

13. REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Created By</th>
<th>Change Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>September 01, 2020</td>
<td>2020.01</td>
<td>Information Security team</td>
<td></td>
</tr>
</tbody>
</table>

Rubrik, the Multi-Cloud Data Control™ Company, enables enterprises to maximize value from data that is increasingly fragmented across data centers and clouds. Rubrik delivers a single, policy-driven platform for data recovery, governance, compliance, and cloud mobility. For more information, visit www.rubrik.com and follow @rubrikInc on Twitter. © 2020 Rubrik. Rubrik is a registered trademark of Rubrik, Inc. Other marks may be trademarks of their respective owners.