Reluna Technology Ltd.

Backup Policy

Effective starting: September 1, 2o24

The purpose of this data backup policy is to define the guidelines for the backup and recovery of critical data for the Portfolio Asset Management System. This policy ensures that data is regularly backed up, securely stored, and available for timely recovery to prevent data loss and minimize disruption to business operations.

1. **Scope**

2.1. This policy applies to all data and systems critical to the operation of the Portfolio Asset Management System, including but not limited to databases, application data, and configuration files. The policy covers all data residing in AWS environments, including AWS Elastic Kubernetes Service (EKS) and AWS Relational Database Service (RDS).

3. **Objectives:**

3.1. To ensure the availability, integrity, and confidentiality of critical data.

3.2. To minimize data loss and downtime in the event of a disaster or system failure.

3.3. To define responsibilities for data backup and recovery operations.

4. Backup Strategy

4.1. **Database-Only Backup Approach:** All critical data for our Portfolio Asset Management System is stored exclusively within a database hosted on Amazon Relational Database Service (RDS). Therefore, our backup strategy focuses entirely on ensuring the availability, integrity, and recoverability of the database.

4.2. **AWS RDS Backup Mechanism:** We leverage the automated backup and snapshot functionality provided by AWS RDS to ensure that our database is consistently backed up and ready for restoration in case of any failure or data loss.

4.3. **Daily Automated Backups (Snapshots):** AWS RDS automatically takes daily snapshots of the entire database, capturing a point-in-time copy of the database. These snapshots are retained for a configurable period (currently set to 7 days by default but configurable as needed). Snapshots include data, settings, and configurations for fast recovery.

4.4. **Transaction Log Backups:** AWS RDS continuously backs up transaction logs to allow point-in-time recovery. This ensures that the database can be restored to any specific point in time within the backup retention window, minimizing potential data loss to a matter of minutes.

4.5. **Backup Frequency:**

4.5.1. AWS RDS takes daily automated snapshots, which are stored in secure, durable AWS storage.

4.5.2. Transaction logs are backed up continuously, allowing recovery of data up to the last committed transaction.

5. Backup Storage

5.1. Primary Storage: Backups are stored in Amazon S3 with versioning and lifecycle policies enabled to protect against accidental deletion and data corruption.

5.2. Secondary Storage: Replicated copies of backups are stored in a different AWS region for geo-redundancy to ensure availability in case of a regional failure.

6. Security of Backups

6.1. All backups are encrypted using AES-256 encryption, both in transit and at rest, to ensure the confidentiality and integrity of the data.

6.2. Access to backup data is restricted to authorized personnel only.AWS Identity and Access Management (IAM) policies are used to enforce role-based access controls (RBAC).

6.3. Multi-factor authentication (MFA) is required for accessing backup data.

7. Backup and Recovery Procedures

7.1. Automated scripts are configured to initiate backups according to the defined schedule. The status of each backup is logged and monitored.

7.2. In the event of data loss or corruption, the IT support team is responsible for initiating the recovery process.

7.3. Restore the most recent backup (full, incremental, or transaction log) depending on the nature of the incident. Prioritize restoring critical data to resume essential business functions.

7.4. Once data is restored, integrity checks and verification tests are performed to ensure data accuracy and completeness.

7.5. Document the recovery process, analyze the cause of data loss, and implement preventive measures to avoid future incidents.

8. Roles and Responsibilities

8.1. Responsibilities of IT Team:

8.1.1. Oversee the implementation and monitoring of backup operations.

8.1.2. Perform regular checks to ensure backups are successfully completed.

8.1.3. Manage access controls and security of backup data.

8.1.4. Execute data recovery operations in the event of data loss or system failure.

8.2. Responsibilities of Backup Administrator:

8.2.1. Configure and manage backup schedules.

8.2.2. Ensure that backup storage locations have sufficient capacity.

8.2.3. Test backup integrity and perform regular restoration tests to verify recovery processes.

8.3. Responsibilities of Security Officer:

8.3.1. Monitor for security threats and unauthorized access to backup data.
8.3.2. Implement security measures, such as encryption and access controls.

8.4. Responsibilities of Compliance Officer:

8.4.1. Ensure that backup policies comply with industry regulations and legal requirements.
8.4.2. Maintain records of backup operations, retention schedules, and recovery tests.

5. Testing and Maintenance

5.1. Regular Testing:

5.1.1. Conduct monthly integrity tests to ensure that backups can be restored successfully without data corruption.
5.1.2. Perform quarterly recovery drills simulating different disaster scenarios to verify the effectiveness of recovery procedures and RTO/RPO objectives.

6. Policy Review and Updates:

6.1. The backup policy is reviewed annually or whenever significant changes occur in the infrastructure, data, or regulatory requirements.

6.2. Updates to the policy are communicated to all relevant personnel.

7. Compliance and Audit

7.1. This backup policy aligns with industry standards, including ISO 27001, GDPR, and other relevant regulatory requirements.

7.2. Regular internal audits are conducted to ensure compliance with the backup policy and procedures.

7.3. Detailed documentation of backup schedules, configurations, and recovery procedures is maintained.

7.4. Logs of backup operations and recovery incidents are stored for audit purposes.