Data Recovery Policy and Procedure

1. Purpose

The purpose of this policy is to ensure that the organization can recover close to exact copies of data in the event of a major incident, disaster, or emergency. This policy aims to minimize data loss and downtime, ensuring business continuity.

2. Scope

This policy applies to all organizational data and systems critical to business operations. It covers the processes for data backup, restoration, and the use of specific recovery solutions such as Cove BCDR (Business Continuity and Disaster Recovery) and SentinelOne rollback using shadow copies.

3. Policy Statement

The organization commits to maintaining a robust data recovery process that enables the quick and secure restoration of data and systems in the event of a disaster or major incident.

4. Responsibilities

- **IT Security Team**: Oversees the implementation and maintenance of data recovery solutions and processes.
- **System Administrators**: Responsible for conducting regular backups and ensuring that recovery processes are in place and tested.
- **Data Owners**: Accountable for classifying the data and determining the recovery priorities for their respective areas.

5. Procedures

5.1 Scope of Data Recovery

- Identify and document which systems and data are critical to business operations and must be included in the data recovery process.

- Maintain an inventory of these assets, including their locations, backup schedules, and recovery point objectives (RPOs).

5.2 Prioritization of System Recovery

- Establish and document the recovery time objectives (RTOs) for each critical system, ensuring that the most crucial systems are prioritized for recovery.
- Develop a recovery sequence that aligns with business continuity requirements and minimizes operational downtime.

5.3 Security of Backup Data

- Implement secure backup solutions, such as Cove BCDR, to ensure that data is encrypted during transmission and at rest.
- Utilize SentinelOne's rollback capability to create secure, point-in-time shadow copies of data, allowing for recovery in case of ransomware attacks or other data corruption incidents.
- Store backups in multiple locations, including off-site and in the cloud, to protect against localized disasters.

5.4 Review and Update the Data Recovery Process

- Regularly test the data recovery process to ensure that it meets the established RTOs and RPOs and that data can be restored accurately and securely.
- Review and update the data recovery policy and procedures annually or when significant changes in the IT infrastructure or business operations occur.
- Ensure that updates reflect advancements in technology, changes in organizational structure, and evolving security threats.

6. Compliance

Non-compliance with this policy may result in disciplinary action and could lead to increased risk of data loss during a disaster. Compliance will be monitored through regular audits and reviews of recovery process tests.

7. Review and Revision

- This policy and its associated procedures should be reviewed and updated at least annually or following significant changes to the business or IT environment.

- Changes to the policy should be approved by senior management and communicated to all relevant stakeholders.

By adopting and following this data recovery policy and procedure, the organization ensures that it can quickly and securely restore critical data and systems, thus maintaining operational continuity and reducing the impact of disasters and major incidents.