Data Backup And Disaster Recovery Plan

1.0 Policy Objective & Scope

The objective of this Data Backup and Disaster Recovery Plan is to ensure the availability, integrity, and confidentiality of all critical corporate data in the event of a system failure, cyberattack, natural disaster, or other disruptive incident. This policy applies to all employees, contractors, and third-party vendors who handle, store, or process company data, including but not limited to HR records, financial data, customer information, and operational databases.

The scope covers all on-premises servers, cloud-based applications, employee workstations, and mobile devices used for business purposes. This plan is designed to minimize downtime, prevent data loss, and ensure compliance with Canadian privacy legislation, including PIPEDA and provincial privacy laws.

2.0 Roles & Responsibilities

- **IT Administrator:** Responsible for configuring, monitoring, and testing backup systems; executing the disaster recovery plan; and restoring data as needed.
- **HR Manager:** Ensures that employee data is included in backup cycles and that access to sensitive HR records is restored promptly after a disaster.
- **Department Heads:** Identify critical data and systems within their departments and communicate recovery priorities to the IT team.
- Chief Information Officer (CIO) / Director of IT: Approves the backup schedule, reviews recovery test results, and authorizes the activation of the disaster recovery plan.
- **All Employees:** Report any data loss or system anomalies immediately to the IT department and follow prescribed procedures during a disaster event.

3.0 Core Rules & Guidelines

- All critical data must be backed up at least once every 24 hours, with incremental backups taken every 4 hours during business operations.
- Backups must be stored in at least two separate physical or cloud locations, one of which must be off-site or in a different geographic region.
- All backup data must be encrypted at rest (AES-256) and in transit (TLS 1.2 or higher) to protect against unauthorized access.
- **Retention periods:** Daily backups retained for 30 days, weekly backups for 12 weeks, monthly backups for 12 months, and annual backups for 7 years to comply with legal and regulatory requirements.
- Disaster recovery drills must be conducted quarterly to validate the integrity of backups and the effectiveness of the recovery process.
- Access to backup systems and recovery tools is restricted to authorized IT personnel only, with multi-factor authentication enforced.

4.0 Step-by-Step Procedure / Workflow

1. Identify and classify all critical data assets (e.g., HR records, financial databases, customer lists, production schedules) and assign a recovery priority level (Critical, High, Medium, Low).

2. Configure automated backup schedules in the backup management software (e.g., Veeam, Acronis, or cloud-native tools) to perform full backups daily and incremental backups every 4 hours.

3. Encrypt all backup data using AES-256 encryption and ensure that encryption keys are stored securely in a separate location from the backup data.

4. Transfer encrypted backups to two destinations: a local on-premises storage array and a secure off-site cloud provider (e.g., AWS S3, Azure Blob Storage) located in a different Canadian province.

5. Monitor backup completion status daily via automated alerts; any failed backups must be investigated and resolved within 2 hours.

6. Conduct a quarterly disaster recovery drill by simulating a total system failure: restore a sample set of critical data from the off-site backup to a test environment and verify data integrity.

7. Document the results of each drill, including recovery time objective (RTO) and recovery point objective (RPO) metrics, and report findings to the CIO.

8. In the event of an actual disaster, the IT Administrator immediately activates the disaster recovery plan, notifies the CIO, and begins restoring critical systems in priority order.

9. After restoration, verify that all data is intact and functional by running integrity checks and cross-referencing with pre-disaster reports.

10. Communicate the restoration status to all affected departments and provide a post-incident report within 48 hours detailing the cause, impact, and corrective actions taken.

5.0 Documentation & Compliance

1. Maintain a centralized backup log in the SwitchDesk admin portal that records the date, time, size, and status of every backup operation.

2. Store all disaster recovery drill reports, including RTO/RPO metrics and any issues encountered, in a secure, encrypted folder accessible only to IT and executive leadership.

3. Ensure that all backup and recovery documentation is retained for a minimum of 7 years to comply with PIPEDA and provincial record-keeping requirements.

4. Conduct an annual audit of the backup and disaster recovery plan by an external IT security firm to identify gaps and recommend improvements.

5. Update the plan immediately following any significant change in IT infrastructure, data classification, or regulatory requirements.