US Solutions Pvt Ltd. - Backup and Disaster Recovery Policy

Document Control:

- **Version:** 1.0
- **Date Issued:** 2024-03-08
- **Author:** IT & Infosec Department - Julianna Reyes
- **Approved By:** Harold Vance, Infrastructure Resilience Manager
- **Effective Date:** 2024-04-08
- **Review Frequency:** Annually

1. Introduction

US Solutions Pvt Ltd. recognizes that data loss and system disruptions can significantly impact business operations. This Backup and Disaster Recovery Policy outlines the procedures for backing up critical data and recovering systems in the event of a disaster or other disruptive event. All employees, contractors, and authorized users ("Users") are required to adhere to this policy.

2. Purpose

The purpose of this policy is to:

- Establish a comprehensive backup and disaster recovery plan.
- Minimize data loss and system downtime.
- Ensure business continuity in the event of a disaster.
- Facilitate compliance with applicable laws, regulations, and industry standards.
- Define the responsibilities of personnel involved in backup and recovery operations.

3. Scope

This policy applies to all critical systems, applications, and data owned, managed, or accessed by US Solutions Pvt Ltd., including:

- Servers and databases.
- Workstations and laptops.
- Cloud-based services.
- Network devices.
- Critical applications.
- All data deemed critical to business operations.

4. Backup Requirements

- **Backup Frequency:** Critical data must be backed up regularly, based on its criticality and recovery time objective (RTO).
  - Daily backups for highly critical data.
  - Weekly backups for moderately critical data.
  - Monthly backups for less critical data.

- **Backup Media:** Backups must be stored on reliable media, such as disk, tape, or cloud-based storage.
- **Backup Retention:** Backups must be retained for a defined period, based on legal, regulatory, and business requirements.
- **Backup Testing:** Backups must be tested regularly to ensure their integrity and recoverability.
- **Offsite Backups:** Offsite backups must be maintained to protect against physical disasters.
- **Encryption:** Backups containing sensitive data must be encrypted.
- **Backup Verification:** Automated or Manual verification of backups must be done, to ensure backups completed successfully.

5. Disaster Recovery Requirements

- **Recovery Time Objective (RTO):** The RTO for critical systems must be defined and documented.
- **Recovery Point Objective (RPO):** The RPO for critical data must be defined and documented.
- **Disaster Recovery Plan (DRP):** A comprehensive DRP must be developed and maintained.
- **DRP Testing:** The DRP must be tested regularly to ensure its effectiveness.
- **Alternate Site:** An alternate site must be identified for recovering critical systems and data.
- **Communication Plan:** A communication plan must be developed for notifying stakeholders during a disaster.
- **System Prioritization:** A system prioritization list must be created and maintained, for determining which systems are recovered first.

6. Responsibilities

- **IT Department:**
  - Implement and maintain backup and disaster recovery systems.
  - Develop and test the DRP.
  - Manage backup media and offsite backups.
  - Perform data recovery operations.
  - Ensure compliance with this policy.
- **Data Owners:**
  - Identify critical data and systems.
  - Define RTO and RPO requirements.
  - Approve backup and recovery procedures.
- **All Users:**
  - Report any data loss or system disruptions.
  - Comply with backup and recovery procedures.
  - Avoid actions that may compromise data integrity.

7. Disaster Recovery Plan (DRP) Components

The DRP must include the following components:

- **Emergency Response Procedures:** Procedures for responding to immediate threats.
- **System Recovery Procedures:** Procedures for recovering critical systems and applications.
- **Data Recovery Procedures:** Procedures for restoring data from backups.
- **Communication Plan:** Procedures for communicating with stakeholders.
- **Alternate Site Procedures:** Procedures for relocating operations to an alternate site.
- **Plan Maintenance:** Procedures for updating and testing the DRP.

8. Legal and Regulatory Compliance

- Backup and disaster recovery practices must comply with all applicable laws, regulations, and industry standards (e.g., GDPR, CCPA, HIPAA).
- Data retention policies must be consistent with legal and regulatory requirements.

9. Training and Awareness

- Authorized personnel will receive training on backup and disaster recovery procedures.
- Regular security awareness training will be provided to all Users regarding data protection.

10. Policy Review and Updates

- This policy will be reviewed and updated annually or as needed to reflect changes in technology, threats, and regulations.
- Any updates to this policy will be communicated to all Users.

11. Monitoring and Enforcement

- The IT department will conduct regular audits to ensure compliance with this policy.
- Violations of this policy may result in disciplinary action, up to and including termination of employment or contract.

12. Acknowledgement

- By accessing Company systems, applications, and data, Users acknowledge that they have read, understood, and agree to comply with this Backup and Disaster Recovery Policy.

This Backup and Disaster Recovery Policy is designed to ensure the resilience of US Solutions Pvt Ltd.'s operations in the event of a disaster or other disruptive event. By adhering to these guidelines, Users contribute to the overall security and continuity of the Company.