Incident Response Plan: Cloud Backup Failure

1. Purpose

This document outlines the incident response plan for failures related to cloud backup systems. Its purpose is to provide a clear and structured process to identify, contain, eradicate, and recover from backup incidents, minimizing potential data loss and operational disruption.

2. Scope

This plan applies to all organizational data and systems that rely on cloud backup solutions for disaster recovery and data restoration.

3. Roles & Responsibilities

Role	Responsibility
Incident Response Lead	Coordinate response, communication, and escalation.
IT Support Team	Technical troubleshooting, verification, and remediation.
Communication Officer	Internal and external stakeholder notification.
System Owner	Decision-making on recovery and restoration actions.

4. Incident Identification

- Backup job failure alerts (from monitoring tools or cloud provider notifications)
- Regular audit/verification reports indicating backup issues
- User reports of inaccessible backup data
- Unexpected backup file corruption or missing backups

5. Incident Response Steps

1. **Detection & Reporting**
    - Receive and log backup failure alerts.
    - Verify incident details and scope through monitoring tools and logs.
2. **Assessment & Classification**
    - Determine affected systems, data, and time period.
    - Classify severity (single job, multiple jobs, systemic failure).
3. **Containment**
    - Prevent additional failures (pause backup jobs if necessary).
    - Isolate affected systems from further changes until resolved.
4. **Eradication**
    - Identify root cause (e.g., misconfiguration, provider outage, infrastructure issue).
    - Rectify misconfiguration or engage cloud provider support.
5. **Recovery**

- Validate restoration capability from existing backup copies.
- Resume backup jobs after resolving the issue.
- Monitor for further issues.

6. **Communication**
   - Inform relevant stakeholders based on communication protocols.

7. **Post-Incident Review**
   - Document actions taken, lessons learned, and preventive measures.
   - Update policies, procedures, and training as necessary.

6. Communication Plan

- Initial incident notification to IT management and backup system owners.
- Escalation to executive leadership and compliance if data loss is suspected.
- Status updates to stakeholders throughout the incident lifecycle.
- Post-incident summary/disclosure (as required by policy or regulation).

7. Testing & Training

- Annual tabletop exercises and backup restoration drills.
- Regular staff awareness and technical training on incident response procedures.

8. Document Control

Version	Date	Author	Description
1.0	2024-06-06	Incident Response Team	Initial incident response plan draft