Backup and Business Continuity Plan (BCP)

1. Objective

To ensure uninterrupted business operations and data protection in the event of unforeseen disruptions such as hardware failures, cyberattacks, natural disasters, or human error.

---

2. Scope

This plan applies to:

- All IT systems, applications, and databases.
- All employees, contractors, and stakeholders.
- All locations where business operations are carried out.

---

3. Backup Policy

3.1 Types of Backups

- **Full Backup** – Weekly full system backup.
- **Incremental Backup** – Daily incremental backup.
- **Database Backup** – Twice daily automated backups.
- **Cloud Backup** – Real-time replication of critical data to secure cloud storage.

3.2 Storage Locations

- **Primary Storage**: On-premises servers.
- **Secondary Storage**: Cloud storage (AWS, Azure, or Google Cloud).
- **Tertiary Storage**: External hard drives or off-site physical storage (monthly).

3.3 Retention Policy

- Daily backups retained for **7 days**.
- Weekly backups retained for **1 month**.
- Monthly backups retained for **1 year**.
- Yearly backup archive retained for **3 years** (for compliance).

3.4 Backup Testing

- Quarterly test restores to ensure data integrity.
- Annual disaster recovery drill.

---

4. Business Continuity Plan (BCP)

4.1 Risk Scenarios Covered

- Server/Network outage.
- Cyber-attack or ransomware.
- Power failure.
- Natural disasters (fire, flood, earthquake).
- Pandemic or workforce disruption.

4.2 Recovery Objectives

- **Recovery Time Objective (RTO):** Maximum 4 hours for critical applications, 24 hours for non-critical systems.
- **Recovery Point Objective (RPO):** Maximum 15 minutes for critical databases, 24 hours for non-critical data.

4.3 Continuity Strategies

- **IT Infrastructure:**
  - Cloud hosting for mission-critical applications.
  - Redundant power supply and internet connections.
- **Workforce:**
  - Remote work readiness (VPN, secured access).
  - Emergency contact tree for employees.
- **Operations:**
  - Manual workarounds for essential business functions.
  - Alternative vendor/supplier arrangements.

---

5. Roles and Responsibilities

- **BCP Committee:** Oversees plan implementation and updates.
- **IT Team:** Ensures data backups, restores, and infrastructure continuity.
- **HR & Admin:** Manages employee communication and safety.
- **Management:** Approves decisions and allocates resources during disruptions.

---

6. Communication Plan

- Emergency hotline and WhatsApp group for employees.
- Email and SMS alerts for clients regarding disruptions.
- Weekly status updates until issue resolution.

---

7. Plan Maintenance & Review

- Review plan **yearly**.
- Update after major system changes or incidents.