Company Data & Disaster Management Policy

1. Introduction

This Disaster Management Policy outlines our company's approach to safeguarding critical business information, including employee records, payroll data, and other sensitive employee information. It details our processes for data protection, security measures, and protocols for data recovery in the event of a breach or system compromise.

2. Data Protection Procedures

- **Employee Records and Payroll Data Backup:**
  All employee-related data, including records and payroll information, is backed up regularly. A scheduled backup process runs weekly to ensure the latest data is securely stored. This includes sensitive files such as employment contracts, personal identification details, and financial information.
- **Data Upload to Secure Locations:**
  To minimize risks, backup data is uploaded to multiple secure locations:
  1. **Cloud Storage:** Data is encrypted before being uploaded to a secure secondary cloud storage provider.
  2. **Physical Storage:** External hard drives are used for additional redundancy.
- **Yearly Backup Archiving:**
  An annual backup copy is archived and stored with a different cloud vendor to ensure long-term data preservation. These backups are organized year-wise for easy retrieval.

3. Data Security Measures

- **Two-Step Verification (2SV):**
  Access to sensitive employee data is protected using Two-Step Verification (2SV). This adds an extra layer of security beyond passwords, requiring:
  - A verification code sent to the user’s registered email.
  - A one-time password (OTP) sent to the user’s registered phone number.
- **One-Time Password (OTP) Authentication:**
  OTPs are dynamically generated and valid for a limited time. This ensures secure access even if login credentials are compromised.
- **User Authentication:**
  Only authorized personnel with company-issued email accounts and verified phone numbers can access sensitive data. Permissions are reviewed quarterly to maintain security compliance.

- **Data Recovery Protocol:**

1. Retrieve the most recent backup from the primary secure location.
2. If the primary backup is compromised, access the secondary cloud vendor’s archived copy.
3. Systematically restore data to ensure integrity and minimize downtime.

4. Consequences of Data Breach

- **Internal Consequences:**
    - Potential disciplinary actions against employees found negligent in following security protocols.
    - Increased security audits and mandatory retraining sessions.
- **External Consequences:**
    - Possible legal and regulatory implications.
    - Damage to the company's reputation and potential financial penalties.

6. Roles and Responsibilities

- **IT Administrator:** Oversees data protection processes, security configurations, and data recovery procedures.
- **Data Protection Officer:** Ensures compliance with data security policies and conducts regular audits.
- **Authorized Users:** Follow security protocols and report any suspicious activities promptly.

7. Review and Updates

This policy is reviewed annually or after any major incident to ensure its effectiveness. Updates are communicated to all relevant stakeholders.