Employee Device Data Backup Policy Framework

Purpose

The purpose of this policy is to establish a framework for regular data backup of devices used by employees in order to ensure business continuity, data integrity, and compliance with organizational requirements.

Scope

This policy applies to all employees, contractors, and temporary staff who use company or personal devices to access, store, or process company data.

Policy Statement

- All critical business data on employee devices must be backed up on a regular schedule as defined by IT.
- Backups must be stored on approved and secure storage systems.
- Personal data unrelated to business functions should be excluded from company backup systems.
- Data restoration procedures must be tested periodically.
- Only authorized personnel are allowed to access backup data.

Roles and Responsibilities

Role	Responsibility
Employees	Ensure company data on their devices is backed up in accordance with policy.
IT Department	Provide backup solutions, monitor backup processes, and support data restoration.
Managers	Ensure team compliance with backup requirements.

Backup Procedures

1. Configure automatic backups for all devices where feasible.
2. Manual backup must be performed at least weekly if automation is not available.
3. Store backups in secure, authorized locations per IT direction.
4. Encrypt backup data in transit and at rest.
5. Regularly verify the integrity and recoverability of backups.

Data Retention

- Backups will be retained for a minimum of 90 days unless regulations require longer retention.
- Expired backups must be securely deleted.

Compliance

Failure to comply with this policy can result in disciplinary action, up to and including termination, and may result in legal action if regulatory requirements are breached.

Review and Updates

This framework is subject to annual review and will be updated as necessary to address emerging risks and compliance requirements.