AMBITION SERVICES PRIVATE LIMITED

Name of the Policy	**Data Security & Backup Policy**
Policy Owner	**IT/Admin Department**
Policy Custodian	**Legal & Compliance Department**
Date of approval by the Board	**19th October, 2024**

Table of Contents

Data Security & Backup Policy

1. Introduction

This policy outlines the procedures and responsibilities to ensure the protection, confidentiality, and integrity of Ambition Services Private Limited ("the Company" or "Ambition") data and procedures for managing data backups using OneDrive across all employee systems.

2. Purpose

The purpose of this policy is to safeguard Ambition's information against unauthorized access, breaches, or loss and ensure that all company data is securely backed up and can be restored in case of accidental deletion, hardware failure, cyberattacks, or other unforeseen events.

3. Scope of this Policy

This policy applies to all systems, networks, and devices within the company's IT infrastructure. It includes but is not limited to desktops, laptops, mobile devices, cloud storage, and data sharing platforms and this policy applies to all employees, contractors, and third parties using company-owned or personal devices to access company data. The policy covers all Ambition data stored on employee systems and associated cloud services like OneDrive.

4. Data Protection Measures

4.1 Antivirus Software

- All company systems must have Quick Heal antivirus installed, configured, and regularly updated to provide protection against malware, ransomware, viruses, and other cyber threats.

4.2 Restricted External Devices

- The use of USB drives, external hard drives, and any other portable storage devices for data transfer is strictly prohibited unless expressly authorized by IT/Admin.
- USB ports and other external device connections will be disabled to prevent unauthorized data extraction.

4.3 Data Sharing Restrictions

- Sharing Ambition data through personal email accounts such as Gmail, Yahoo, or messaging apps like WhatsApp is prohibited.
- Employees must use the company's official email system for all work-related communications.
- Employees may not upload Ambition data to unauthorized cloud services or file-sharing platforms
- The use of OneDrive, the company's designated backup system, is mandatory for storing and sharing company data securely.

- Any other unauthorized platforms that could lead to data leakage are blocked.

4.4 Admin Control

- The control and management of these restrictions, including the activation and deactivation of data sharing policies, reside with an authorized admin. The login and password for admin access are confidential and controlled exclusively by the admin with approval from both the CEO and COO.

5. Access Control

Only authorized personnel will be granted access to sensitive data. Access rights will be regularly reviewed and updated as necessary to ensure appropriate levels of control.

6. Data Backup & Recovery

6.1 Data Backup

- Backup System: OneDrive for Business will be used as the primary backup solution.
- Devices Covered: All desktop computers, laptops, and mobile devices used for work purposes.
- Data Coverage: The policy covers files, documents, emails, and any other business-critical data stored locally on employee devices.

6.2 Backup Frequency

- Real-Time Backup: Files stored in designated OneDrive folders will be automatically synced and backed up in real time.
- Daily Backup Verification: At the end of each workday, a system check will ensure all files have been successfully backed up.
- Weekly Review: IT/Admin staff will conduct weekly audits to confirm the integrity and accessibility of the backed-up data.

6.3 Data Retention

- Standard Retention Period: All files will be retained for a minimum of 1 year from the date of creation or modification.
- Archival Policy: Files no longer actively in use but still required for legal or historical reasons will be moved to an archive folder within OneDrive and retained for the period required as per law.
- Deletion Policy: Files will be permanently deleted from OneDrive after the retention period unless otherwise required by business needs or legal requirements.

6.4 Restoration Process

- Employee Requests: Employees can restore files themselves from OneDrive for up to 30 days from accidental deletion.

- IT/Admin Support: If further assistance is needed, employees must submit a support request to IT/Admin, and restoration will be completed within 24 hours.

7. Employee Responsibilities

- Employees must adhere to all Ambition policies regarding data security.
- Unauthorized attempts to circumvent or disable any of the security controls are strictly prohibited and will result in disciplinary actions.
- All data transfers should be performed using company-approved methods and platforms.
- Ensure Sync: Employees must ensure that business-critical files are stored in designated OneDrive folders that are included in the backup.
- Reporting Issues: Any issues with OneDrive sync or data recovery must be immediately reported to IT/Admin.
- Compliance: Employees must comply with the company's data retention and deletion policies.

8. IT/Admin Responsibilities

- Monitoring: The IT/Admin department is responsible for monitoring the backup process, ensuring data integrity, and addressing any issues with syncing or restoration. All data transfers and communications are monitored for compliance with this policy. Any unauthorized activity will be flagged and investigated.
- Support: IT/Admin must provide assistance to employees for data recovery requests and respond to incidents related to data loss.
- Documentation: Maintain up-to-date documentation on backup schedules, retention periods, and the recovery process.

9. Disciplinary Actions

Violations of this policy may result in disciplinary actions, up to and including termination of employment. Legal action may also be taken if the violation results in a data breach or other serious consequences.

10. Policy Review

This policy will be reviewed annually or as needed to accommodate changes in technology, business processes, or security requirements.