Corporate Policy: Green Thumb Nursery
Title: Data Storage and Security Policy

Complete this template by replacing the bracketed text with the relevant information.

Purpose: This policy aims to establish a secure and systematic approach to data management within Green Thumb Nursery. It handles all data, regardless of its form or storage medium, with the highest security and compliance standards. The policy protects the organization's data from unauthorized access, breaches, loss, or corruption, thus safeguarding our business operations, client relationships, and company reputation.

Scope: This policy applies to all personnel at Green Thumb Nursery, including full-time employees, part-time staff, contractors, and third-party service providers. It covers all types of data storage and handling practices, whether digital or physical, encompassing servers, cloud solutions, personal devices, and paper records. This policy is mandatory for anyone accessing, managing, or storing data under the organization's guidance.

Description

1. Policy

a. Data Storage

i. Data must be classified according to sensitivity defined in the Data Inventory and Classification document and stored in environments that match its classification requirements.

ii. All sensitive data must be encrypted using approved cryptographic techniques at rest and in transit.

iii. Access to data will be strictly controlled and monitored, with permissions granted based on the least privilege principle. Unauthorized access attempts must be logged and investigated.

iv. Data must be regularly backed up according to the objectives of data criticality and recovery time. These backups should be tested periodically to ensure their integrity and effectiveness.

b. Data Security

i. The company commits to implementing robust defensive measures against data breaches, including firewalls, intrusion detection systems, and regular vulnerability scans.

ii. All employees must receive training on data security principles, best practices, and their specific responsibilities regarding data security.

iii. Data security policies and procedures will be reviewed and updated annually or in response to significant changes in the business environment or technology infrastructure.

iv. Data loss or breach incidents must be reported immediately according to the company’s incident response plan, which outlines procedures for containment, investigation, and remediation.