Andree Salvo
Southern New Hampshire University
CYB 410
Instructor: Johnathan Hammitt

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

Purpose: The goal of this policy is to outline specific guidelines for the handling and safeguarding of data at Green Thumb Nursery. The policy's aim is to ensure that the organization's data is efficiently being managed, protected from unauthorized access, and kept only for the duration necessary to fulfill the organization's operational and legal requirements.

Scope: The scope for this policy is relevant to all employees, contractors, and partners of Green Thumb Nursery who handle Green Thumb's Nursery data. It should also cover all forms of digital and physical storage systems, such as web servers, wireless access points, workstations, and internet routers, that are utilized for data storage and protection.

Andree Salvo
Southern New Hampshire University
CYB 410
Instructor: Johnathan Hammitt

Description

1. Policy

a. **Data Storage**

i. The data from Green Thumb Nursery must be stored exclusively on secure storage systems that have been approved by IT management. The use of personal devices or unauthorized cloud services for storage is strictly forbidden.

ii. Data should only be categorized and stored based on its level of sensitivity, such as public, internal, or confidential. Sensitive or confidential information must be encrypted both when stored and during transmission. The duration for retaining data will adhere to regulatory guidelines and business requirements, with annual reviews conducted. IT administrators should be tasked with ensuring that storage solutions are scalable and comply with retention policies.

b. **Data Security**

i. Sensitive data is only accessed by authorized individuals; it is important to implement access controls like role-based permissions and multifactor authentication.

ii. To ensure security, we must implement encryption, firewalls, systems for detecting and preventing intrusions, and regularly update hardware/systems with patches. Employees should follow secure password protocols, avoid sharing accounts, and promptly report any suspected data breaches. Regular audits and vulnerability assessments must be performed to confirm the effectiveness of data protection strategies.