Woodgrove Corporate Data Handling Policy

Introduction

This Corporate Data Handling Policy (the "Policy") outlines the standards, procedures, and restrictions for all employees, contractors, and affiliated parties regarding the handling, storage, and transmission of corporate data within Woodgrove (the "Company"). The purpose of this Policy is to safeguard the integrity, confidentiality, and availability of corporate data and to ensure compliance with applicable laws, regulations, and contractual obligations.

Scope

This Policy applies to all forms of data, including electronic and paper records, that are owned, held, or processed by or on behalf of the Company. It covers all types of data storage and communication devices, including but not limited to corporate-issued computers, mobile devices, and cloud services.

Core Provisions

1. Prohibition of USB Devices

To mitigate the risk of unauthorized data transfer, introduction of malware, and loss or theft of data, the use of USB devices (e.g., flash drives, external hard drives) in any corporate device is strictly prohibited. Exceptions may only be granted by the IT Department under strict controls and for specific, approved business needs.

2. Restriction on Data Transfer

Corporate data must remain within the confines of the organization and may not be transferred, shared, or disclosed to external parties without explicit authorization in accordance with the Company's Data Sharing and Transfer Policy. This includes, but is not limited to, data sharing via email, cloud services, or physical media.

3. Approved Corporate Software for Data Storage

All corporate data must be stored on software and platforms that have been officially approved by the Company's IT Department. Employees must ensure that data is stored securely and in accordance with the IT Department's guidelines on data classification and storage. Unauthorized storage of corporate data on personal devices or unapproved third-party services is strictly prohibited.

4. Data Labeling and Sensitivity Classification

Sensitive data, including personal identifiable information (PII), financial information, and intellectual property, must be clearly labeled and treated in accordance with its sensitivity level. The Company adopts a data classification scheme that categorizes data into various sensitivity levels (e.g., Public, Internal, Confidential, and Highly Confidential). Employees are required to familiarize themselves with this classification scheme and handle data accordingly.

Compliance

Training and Awareness

All employees will receive training on this Policy and related data handling procedures. Ongoing awareness programs will be conducted to reinforce the importance of data security.

Monitoring and Enforcement

The IT Department will monitor compliance with this Policy through regular audits and reviews. Violations of this Policy may result in disciplinary action, up to and including termination of employment.

Policy Review and Updates

This Policy will be reviewed annually or as needed to reflect changes in legal, regulatory, or business requirements. Employees will be notified of any updates.

Conclusion

Adherence to this Corporate Data Handling Policy is mandatory for all employees and affiliates of the Company. By following these guidelines, we can protect our data assets, ensure compliance with legal and regulatory requirements, and maintain the trust of our clients, partners, and stakeholders.