Data Protection & Privacy Policy

1. OVERVIEW

Nexus Global Solutions is committed to protecting the privacy and security of all personal, client, and corporate data. This policy sets out the framework for handling sensitive information in compliance with relevant data privacy laws and regulations.

2. DATA HANDLING GUIDELINES

All employees are responsible for safeguarding company data. The following rules must be strictly adhered to:

- **Need to Know:** Data should only be accessed by employees who require it to perform their official duties.
- **Secure Storage:** Electronic data must be stored on encrypted company servers. No sensitive information may be stored on personal devices or external hard drives without prior IT approval.
- **Data Sharing:** Sensitive information should not be shared via unsecured channels (e.g., personal email, public messaging apps).

3. PASSWORD MANAGEMENT AND SECURITY

Strong passwords are the first line of defense against unauthorized access. Employees must use passwords that are at least 12 characters long and include a mix of letters, numbers, and symbols. Passwords must be updated every 90 days and must never be written down or shared with colleagues.

Notice: Multi-Factor Authentication (MFA) is mandatory for all company accounts. Disabling MFA is a direct violation of this policy.

4. DEVICE MANAGEMENT

All company-issued devices are centrally managed by the IT department. Employees must lock their screens whenever they leave their desks (Windows: Win + L, Mac: Cmd + Ctrl + Q). In the event a device is lost or stolen, it must be reported to IT immediately to initiate a remote wipe.

5. INCIDENT REPORTING

Any suspected data breach, phishing attempt, or unauthorized access must be reported to the IT Security Team immediately at security@nexusglobal.dummy. Delaying a report can cause irreparable harm to the company and our clients.