Confidentiality & Non-Disclosure Procedure

Objective:

To protect the company's proprietary, financial, and strategic information from unauthorized disclosure or misuse, ensuring that all employees understand and uphold their duty of confidentiality during and after employment.

Scope:

This procedure applies to all employees, contractors, consultants, interns, and third parties who have access to the company y's confidential or sensitive information.

Responsibility:

- **All Employees:** Must handle company information responsibly and always maintain confidentiality.
- **Supervisors/Managers:** Ensure team members are aware of and comply with confidentiality requirements.
- **Human Resources (HR):** Ensures each employee signs a non-disclosure agreement (NDA) and provides ongoing awareness training.
- **IT Department:** Ensures secure data management and access control to sensitive systems and information.

Definition of Confidential Information:

Confidential information includes, but is not limited to:

- Business strategies, financial data, pricing, contracts, and trade secrets.
- Client and supplier information, contact lists, and agreements.
- Technical data, designs, product plans, and intellectual property.
- Employee data, payroll details, and internal HR records.
- Any non-public information shared during employment or business activities.

Confidentiality Agreement (NDA):

- All new employees must sign a Non-Disclosure Agreement (NDA) before or on their first day of work.
- The agreement outlines the employee's obligation to protect company information and not disclose it to unauthorized persons or entities.
- Contractors, consultants, and vendors must also sign a separate NDA before starting any project involving sensitive data.

Handling of Confidential Information:

Employees are required to:

- Access confidential data only when necessary for legitimate business purposes.
- Avoid sharing confidential information verbally, in writing, or electronically with anyone who is not authorized.
- Store sensitive documents securely (locked drawers, password-protected files).
- Avoid using personal devices or email accounts for company business unless explicitly approved.
- Label documents and emails as "Confidential" where applicable.
- Report any accidental or potential data breaches immediately to HR or IT.
- Lock their computers while leaving their desk even for a short period.
- Ensure any physical confidential documents are stored securely in locked drawers before leaving their desks.
- Be mindful of who can overhear confidential matters while discussing in meetings or public spaces

Electronic Data & IT Security

- Employees must use **company-approved systems** for storing or transmitting confidential information.
- Passwords must be kept secure and changed periodically.
- IT regularly monitors access permissions and removes access upon termination or transfer.
- The use of USB drives or external storage for confidential information is strictly prohibited unless it is approved by IT.

Post-Employment Obligations

- The duty of confidentiality **continues indefinitely** after the end of employment.
- Departing employees must return all company documents, devices, and confidential materials before their last working day.
- HR reminds employees during the **exit process** of their continuing confidentiality and non-disclosure responsibilities.