Data Classification Policy

1. Purpose
The purpose of this Data Classification Policy is to define a structured approach to categorizing and handling the Company's data based on its sensitivity, value, and regulatory requirements. Proper classification ensures that data is protected against unauthorized access and disclosure while supporting business operations and compliance obligations.

2. Scope
This policy applies to all employees, contractors, and other individuals who access, process, or store the Company's data in any format, including physical and digital assets.

3. Data Classification Levels
All Company data must be classified into one of the following categories:

- **Public:** Data intended for public disclosure with no confidentiality restrictions (e.g., marketing materials, publicly posted information).
- **Internal Use Only:** Non-sensitive business data that is not intended for public release but does not require strict confidentiality measures (e.g., internal communications, non-confidential reports).
- **Confidential:** Sensitive business or customer data that requires protection to prevent unauthorized access or exposure (e.g., financial records, employee information, proprietary business plans).
- **Restricted:** Highly sensitive or legally regulated data that requires the highest level of protection due to its potential impact on the Company if exposed (e.g., personally identifiable information (PII), payment card data, trade secrets, legal documents).

4. Roles and Responsibilities

- **Data Owners:** Responsible for classifying data and ensuring appropriate security measures are applied.
- **Employees and Contractors:** Must adhere to classification guidelines when handling data.
- **IT and Security Teams:** Implement technical controls to enforce classification policies, including access restrictions and encryption.
- **Compliance Team:** Ensures data classification practices align with regulatory requirements.

5. Data Handling Requirements
Each classification level has specific handling requirements:

- **Public:** No access restrictions; can be shared freely.
- **Internal Use Only:** Limited to authorized personnel; must not be shared externally without approval.

- **Confidential:** Must be stored in secure locations with access controls; transmission requires encryption.
- **Restricted:** Access is strictly limited to authorized individuals; storage must be encrypted, and data must not be shared externally without management approval.

6. Data Storage and Retention

- Data must be stored according to classification requirements, leveraging encryption and secure access controls where applicable.
- Retention policies must align with business needs and regulatory obligations.
- Secure disposal methods must be followed when classified data is no longer needed.

7. Compliance and Monitoring

- The Company will conduct periodic audits to ensure adherence to data classification policies.
- Employees must report any suspected misclassification or unauthorized access to the IT Security Team.
- Non-compliance may result in disciplinary action, including termination or legal consequences.

8. Policy Review and Updates

This policy will be reviewed and updated annually or as needed to accommodate changes in regulatory requirements and business practices. Employees are responsible for staying informed of any updates.