**Data Classification Policy**

**1. Introduction**

The purpose of this Data Classification Policy is to ensure that information within the small construction company is appropriately categorized based on its sensitivity, value, and risk if disclosed or accessed by unauthorized individuals. This policy establishes a framework for handling data according to its classification level, ensuring compliance with relevant regulations and the NIST Cybersecurity Framework.

This policy applies to all employees, contractors, and third-party vendors who handle, process, or manage company data.

**2. Data Classification Levels**

All data within the company must be classified into one of the following categories:

* **Confidential:**
  + Definition: Information that could cause significant financial, reputational, or operational damage if disclosed.
  + Examples: Employee personal information (PII), financial records, project blueprints, client contracts, proprietary data.
  + Protection Requirements: Must be encrypted at rest (AES-256) and in transit (TLS 1.3). Access restricted to authorized personnel only.
* **Internal Use Only:**
  + Definition: Information meant for internal use that, if disclosed, could negatively impact business operations but does not cause significant damage.
  + Examples: Internal communications, operational procedures, internal project updates.
  + Protection Requirements: Requires encryption during transmission and appropriate access controls.
* **Public:**
  + Definition: Information approved for public release with no associated risk of disclosure.
  + Examples: Marketing materials, press releases, public reports.
  + Protection Requirements: No encryption required but should be monitored to prevent unauthorized modifications.

**3. Roles and Responsibilities**

* **Data Owners:** Responsible for determining the appropriate classification level of data under their management.
* **IT Security Team:** Implements technical controls based on classification levels, including encryption and access controls.
* **Employees and Contractors:** Must handle data in accordance with its classification level and report any security breaches.

**4. Data Handling Procedures**

**4.1 Data Collection and Storage**

* All sensitive data must be stored in secure, access-controlled environments.
* Data classified as Confidential must be encrypted both at rest and in transit.

**4.2 Data Access and Transmission**

* Access should be granted based on the principle of least privilege (Role-Based Access Control).
* Secure methods such as TLS 1.3 should be used for transmitting any sensitive data.

**4.3 Data Retention and Disposal**

* Data must be retained based on regulatory requirements and business needs.
* Secure disposal of Confidential and Internal Use data must be ensured using approved deletion tools or physical destruction.

**5. Data Reclassification**

Data should be reviewed periodically to ensure that classifications remain accurate. Changes in sensitivity, business value, or regulatory requirements may necessitate reclassification.

**6. Monitoring and Compliance**

* Regular audits must be conducted to verify compliance with the data classification policy.
* Unauthorized access or misuse of data must be reported immediately and addressed according to the company’s incident response procedures.

**7. Policy Review and Updates**

This policy will be reviewed annually or following significant changes in business operations, regulatory environments, or cybersecurity threats.

**8. Enforcement**

Violations of this policy may result in disciplinary actions, including termination of employment or legal action. Third-party vendors who violate this policy may face termination of contracts.