**Data Encryption Policy**

**1. Introduction**

This Data Encryption Policy establishes the guidelines for securing sensitive information within the small construction company. The objective is to protect the company’s data from unauthorized access, ensuring compliance with NIST standards, particularly the NIST SP 800-53 and Cybersecurity Framework (CSF). This policy applies to all employees, contractors, and third-party vendors handling company data.

**2. Encryption Guidelines**

**2.1 Data at Rest Encryption (AES-256)**

* All sensitive data stored on company devices, cloud services, and backup media must be encrypted using the Advanced Encryption Standard (AES) with a 256-bit key length.
* Encryption must be applied to:
  + Employee records
  + Project data (e.g., blueprints, client contracts)
  + Financial information
  + Proprietary company documents
* Encrypted backups must be regularly tested for data integrity and accessibility.

**2.2 Data in Transit Encryption (TLS 1.3)**

* All sensitive data transmitted across networks must be encrypted using Transport Layer Security (TLS) version 1.3 or higher.
* Applications and communication tools (e.g., email, VoIP) must enforce TLS encryption.
* VPNs must be configured to use strong encryption protocols (e.g., AES-256 for tunnel encryption).

**3. Data Leak Prevention (DLP) Measures**

* Implement DLP tools to monitor and control the movement of sensitive data across endpoints, emails, and cloud services.
* Monitor file transfers and data access logs for suspicious activities.
* Apply endpoint protection solutions that prevent unauthorized data transfers and detect potential breaches.
* Educate employees on handling sensitive data, including secure file sharing practices.

**4. Encryption Key Management Procedures**

* **Key Generation:** Keys must be generated using approved cryptographic algorithms.
* **Key Storage:** Encryption keys must be stored securely using Hardware Security Modules (HSMs) or equivalent secure storage systems.
* **Key Rotation:** Encryption keys must be rotated periodically, with a recommended rotation frequency of every 12 months or immediately following a suspected security breach.
* **Access Control:** Access to encryption keys must be restricted to authorized personnel only, using Role-Based Access Control (RBAC).
* **Key Backup:** Regular backups of encryption keys must be securely maintained and encrypted.

**5. Document Encryption Process Using VeraCrypt**

**5.1 Prerequisites**

* Download and install VeraCrypt from the official website [link](https://www.veracrypt.fr/en/Downloads.html).

**5.2 Step-by-Step Encryption Guide**

1. Launch VeraCrypt.
2. Click on “Create Volume” and select “Create an encrypted file container.”

A screenshot of a computer

AI-generated content may be incorrect.

1. Choose the encryption algorithm as AES with a 256-bit key.
2. Specify the volume size based on the document's size.

A screenshot of a computer

AI-generated content may be incorrect.

1. Set a strong password that complies with company password policies.

A screenshot of a computer

AI-generated content may be incorrect.

1. Format the volume using NTFS (for larger files) or FAT (for compatibility).

A screenshot of a computer

AI-generated content may be incorrect.

1. Mount the encrypted container and move the sensitive document into it.
2. Dismount the container once the document has been secured.

**5.3 Documentation and Monitoring**

* Maintain logs of encrypted files and encryption events.
* Regularly verify the integrity of encrypted files.

**6. Policy Review and Updates**

This policy will be reviewed annually or following significant security incidents or technological updates. All employees must acknowledge this policy and undergo periodic training on secure data handling practices.

**7. Compliance**

Failure to comply with this policy may result in disciplinary action, including termination of employment or contractual agreements. Legal consequences may also apply in case of violations involving sensitive data breaches.