Department: Operations	Document No: OP-4	Revision No: 1.1	Page 1 of 15
Title: IT-01 - IT POLICY AND PROCEDURES			
Preparation: Operations / IT		Initial Version: 11/12/2025	Next Revision: 11/12/2026

STONITE COIL CORPORATION
DATA PROTECTION POLICY AND PROCEDURES

	NAME	POST	DATE	VERSION
Reviewed by	Carol Engel	Administrative V.P., Operations	11/12/2025	1.1
Approved by	Bill Engel	President/CEO	11/12/2026	1.1

1. Introduction

Stonite Coil Corporation (“Stonite Coil”) is committed to maintaining the confidentiality of our clients’ data and records related to business interactions. Proprietary client information will be accessed and utilized solely with the client's explicit consent. We will not use confidential client information for personal or organizational benefit.

2. Purpose

The purpose of this Policy is to outline Stonite Coil's commitment to data protection and privacy. It is our intent to ensure the secure and responsible handling of all personal and sensitive information collected during the course of our consulting services. This policy serves as a guide for our employees, clients, and suppliers to understand our data protection practices and to ensure compliance with relevant data protection laws and regulations.

3. Applicability / Scope

This Data Protection Policy applies to all activities, processes, and systems within Stonite Coil that involve the collection, processing, and storage of data. This includes, but is not limited to, data collected from clients, employees, partners, and other third-parties.

This policy covers data collected both in digital and physical formats and pertains to all locations and entities associated with Stonite Coil. It extends to all employees, contractors, and any third-parties working on behalf of our firm. Additionally, this policy encompasses the use of data within our organization and its sharing, storage, and disposal.

This Data Protection Policy is subject to regular review and updates to ensure ongoing compliance with data protection regulations and to align with best practices in the industry. It is an integral part of our commitment to safeguarding personal and sensitive information.

4. Data collection and use

Data collection and use outlines how data is gathered and the purposes for which it is used, all while ensuring compliance with data protection regulations. Below is a list of each component type:

4.1. Types of Data Collected

The categories of data collected could be personal information (names, addresses, contact details), financial data (payment information), and any other relevant information. Defining the data type ensures clarity regarding the nature of data that may be collected during Stonite Coil business operations.

4.2. Purpose of Data Collection

For every data collected it is important to indicate the reasons why data is collected. It may include purposes like providing consulting services, fulfilling contractual obligations, invoicing, marketing, or other legitimate business activities. It ensures transparency about the intent behind data collection.

4.3. Legal Basis for Data Processing

This component refers to the legal justifications for processing the collected data. It might include legal obligations, contractual necessity, consent, or the legitimate interests pursued by Stonite Coil. We ensure that data processing aligns with applicable data protection laws.

4.4. Consent and Transparency

If the legal basis for data processing relies on consent, this section elaborates on how and when consent is obtained from data subjects. It underscores the importance of clear and transparent communication regarding data handling and seeks to ensure that individuals are fully informed and have willingly agreed to data processing.

Obtaining consent from data subjects should be done in a transparent and lawful manner. Below is how and when consent is typically obtained:

4.4.1. Clear and Informative Consent Requests

- Consent requests should be presented in clear and easily understandable language.
- Data subjects should be informed about what they consent to and for what purposes.
- Consent forms should be concise and not buried in lengthy terms and conditions.

4.4.2. Opt-In Mechanism

- Data subjects should actively opt-in to provide their consent, meaning they take an affirmative action like checking a box, clicking a button, or signing a consent form.
- Pre-ticked boxes that assume consent are generally not compliant.

4.4.3. Granular Consent

- When processing involves multiple purposes, data subjects should be able to consent to each purpose separately.
- This allows individuals to have more control over what they're agreeing to.

4.4.4. Unambiguous Consent

- Consent should be obtained through clear and unambiguous actions.
- Avoid using vague language or tactics that may confuse data subjects.

4.4.5. Revocable Consent

- Data subjects should be informed that they can withdraw their consent anytime.
- Clear instructions for revoking consent should be provided.

4.4.6. Consent Records

- Maintain records of consent, including when and how it was obtained, what data subjects were informed about, and what they consented to.

4.4.7. Re-consent for Changes

- If the purpose or handling of data changes, seek fresh consent from data subjects. Existing consent may not be valid for the new use.

4.4.8. Consent Renewal

- Periodically seek renewal of consent, especially for long-term data processing.

4.4.9. Specific Consent for Sensitive Data

- For the processing of sensitive data (e.g., health data), explicit and specific consent is often required.

The timing for obtaining consent can vary. In many cases, it should be acquired before data processing begins. If data is already collected and consent is not obtained, it's essential to seek consent as soon as possible and stop processing data until consent is received. It's also good practice to periodically review and renew consent, especially for ongoing data processing activities. Consent should be a continuous and well-documented process.

4.5. Data Minimization

Data minimization highlights the principle of collecting only the data that is strictly necessary for the intended purposes. It emphasizes Stonite Coil's commitment to not over-collecting or retaining data beyond its necessity. This helps reduce privacy risks and comply with data protection laws that promote minimal data processing.

5. Data Security and Storage

This section addresses how data is protected throughout its lifecycle, from collection to disposal. It outlines the procedures and practices for the secure handling of data within the organization. It includes safeguards for both physical and digital data, such as secure storage, locked cabinets, password protection, and controlled access to data.

Following are some key procedures and practices for securely handling data:

- Access Control
- Data Classification
- Regular Backups
- Secure File Sharing
- Secure Disposal of Data

- Data Masking and Anonymization
- Monitoring and Logging
- Data Transfer Security
- Employee Training
- Incident Response Plan
- Vendor and Third-party Security
- Data Retention and Disposal Policies
- Physical Security
- Regular Security Audits
- Data Access Review

Secure data handling is an ongoing process that involves a combination of technology, policies, and employee practices to protect data from unauthorized access and potential threats.

5.1. Access Control

Access control details who has permission to access and handle data. It specifies roles, responsibilities, and procedures for granting, revoking, and managing access rights. It may encompass user authentication, role-based access, and monitoring of access activities.

- Categorize data based on sensitivity and importance.
- Apply appropriate security controls to each data category.
- Limit access to highly sensitive data to only those who need it.
- Implement role-based access control (RBAC) to restrict data access to authorized personnel.
- Require strong, unique passwords for accessing systems and data.
- Use multi-factor authentication (MFA) to enhance login security.
- Periodically review and revoke access for employees who no longer require access to specific data.

5.2. Data Retention Periods

This section clarifies the timeframes for which different types of data are retained within the organization. It should align with legal requirements and business needs. It outlines when data will be deleted or archived, reducing risks associated with keeping unnecessary information.

- Establish clear data retention policies to determine how long data should be kept.
- Properly dispose of data that has exceeded its retention period.

5.3. Disposal of Data

This section addresses the secure disposal of data that is no longer needed. It details the methods for data destruction, which may include shredding physical documents, securely erasing digital data, and disposing of electronic devices. It emphasizes the importance of thorough and compliant data disposal to mitigate data breach risks.

5.3.1. Secure Disposal Methods

It is crucial to note that the effectiveness of these methods can vary, and the choice of method should be based on the type of storage device and the sensitivity of the data. In some cases, it may be necessary to combine multiple methods to ensure data is irretrievable. Additionally, it is important to keep records of the data destruction process for compliance and auditing purposes.

5.3.2 Methods used for disposing of data:

- **Physical Data:** Securely shredding or destroying physical documents that contain sensitive data.

- **Digital Data:** Digital data should be securely erased or destroyed. Here are some common industry methods:
    - **Overwriting**: Data can be overwritten with random data patterns, making the original data unreadable. Repeated overwrites increase security. Tools like "shred" or "sdelete" can be used for this purpose.
    - **Physical Destruction**: Physical destruction is a highly effective method for hard drives and solid-state drives (SSDs). This involves physically breaking or shredding the storage device.
    - **Secure Erase Features**: Some modern storage devices, particularly SSDs, have built-in secure erase features. These features allow the drive to erase all data securely.
    - **Remote Wiping**: Remote wiping is an option for mobile devices and laptops. This allows you to erase data on a device that is lost or stolen. Mobile device management (MDM) software often includes this capability.

5.3.3 Responsible Parties

Identify the roles and responsibilities of individuals or teams responsible for overseeing the disposal of data. This may include officers, IT staff, or designated personnel.

5.3.4 Data Destruction Procedures

The organization will define a step-by-step guide to the procedures for destroying data, including:

- **Verification:** Verify that the data to be disposed of is no longer needed and has met retention periods.
- **Secure Handling:** Ensure that data is handled securely throughout the disposal process.
- **Shredding and Erasure:** Explain how and when data is shredded, erased, or otherwise rendered unreadable.
- **Records:** Document the disposal process, including the data type, date, and individuals involved.
- **Verification of Destruction:** Describe how the firm confirms the successful destruction of data.

5.3.5 Disposal Schedule

The organization must specify the schedule for regular data disposal, covering the frequency at which data is assessed for disposal and the actual disposal process. Ensure that data is disposed of promptly after it is no longer needed.

5.3.6 Compliance with Legal Requirements

The organization must emphasize compliance with relevant data protection laws, regulations, and industry standards when disposing of data. Highlight the importance of documenting disposal processes for compliance purposes.

5.3.7 Training and Awareness

Discuss the importance of ongoing training and awareness programs to educate employees about the proper disposal of data. Ensure that staff understand their responsibilities in this regard.

6. Data Access and Sharing

6.1. Internal Data Access

This section ensures that data access and sharing within the organization and with third-parties are controlled, secure, and compliant with data protection regulations. It also emphasizes the importance of formal agreements and protocols to protect sensitive data.

6.1.1. Access Control

The organization will describe the procedures and protocols for controlling access to data within the organization. Include information about user authentication, role-based access, and the assignment of access rights based on job responsibilities.

6.1.2. Need-to-Know Principle

The organization will explain the concept of the "need-to-know" principle, emphasizing that employees should only have access to data required for their specific job roles.

6.1.3. Monitoring and Auditing

The organization will detail how internal data access is monitored and audited to detect unauthorized or inappropriate access. This may include regular access reviews.

6.2. Third-party Access

6.2.1. Third-party Engagement

The organization will define the circumstances under which third-parties, such as vendors, partners, or contractors, may access company data. Specify the necessity for third-party access.

6.2.2. Third-party Responsibilities

The organization will outline the data security and protection responsibilities of third-parties, including compliance with data protection regulations, confidentiality requirements, and any other relevant obligations.

6.2.3. Data Sharing Agreements

Highlight the importance of formal data-sharing agreements with third-parties. These agreements should explicitly state the terms and conditions of data access and processing.

6.3. Data Sharing Protocols

6.3.1. Data Classification

The organization will classify data based on sensitivity and the associated protocols for sharing different types of data.

6.3.2. Secure Data Transfer

The organization will describe the methods and tools used for secure data transfer, such as secure file transfer protocols, VPNs, or secure email communication.

6.4. Data Processing Agreements

6.4.1. Purpose of Data Processing Agreements

Explain the importance of data processing agreements with third-parties to ensure data security, privacy, and legal compliance.

6.4.2. Content of Agreements

Outline the key elements that should be included in data processing agreements, such as data protection obligations, confidentiality clauses, compliance with data protection laws, and data breach notification requirements.

6.4.3. Review and Monitoring

Describe the processes for reviewing and monitoring compliance with data processing agreements and the steps to be taken in case of non-compliance.

7. Third-Party Personal Information

7.1. Categories of Information

This Policy applies to third-party personal information, which covers the following categories of information:

- Personal information regarding current, former, and prospective partners, principals, and employees to operate and manage Stonite Coil human resource administration and maintain contact with individuals.

- Personal information regarding current, former, and prospective clients and their personnel, customers, or other data subjects to deliver Stonite Coil services, maintain ongoing relationships, and perform business development activities.
- Personal information regarding our suppliers, service providers, and other third-parties, and their personnel to manage and administer Stonite Coil business relationships with such third-parties.
- Personal information collected from members of the general public in order to answer inquiries or provide information requested.

Personal information obtained from or relating to clients or former clients is further subject to the terms of any specific privacy notice provided to the client, any contractual arrangements with the client, and applicable laws and professional standards.

Information to individuals and businesses regarding the information collected from them and how that information is used may be provided through this Policy, other Stonite Coil privacy notices, or other direct forms of communication with appropriate parties, such as contracts or agreements. Where necessary and appropriate, consent for personal information to be collected, used, and/or transferred may also be obtained through these same means.

Stonite Coil collects and processes personal information only to the extent that it is compatible with the purposes for which it was collected or subsequently authorized by the data subject. Stonite Coil does not retain personal information after it no longer serves the purposes for which it was collected or subsequently authorized. Stonite Coil takes reasonable steps to ensure that personal information is accurate, complete, current, and reliable for its intended use.

7.2. Transfers of personal information to third-parties

Stonite Coil may transfer personal information to other third-parties. We will only disclose an individual's personal information to third-parties under one or more of the following conditions:

- The disclosure is to a third-party providing services to Stonite Coil or to the individual in connection with the operation of our business and as consistent with the purpose for which the personal information was collected. We maintain written contracts with these third-parties and require that these third-parties provide at least the same level of privacy protection and security.
- With the individual's permission to make the disclosure.
- Where required to the extent necessary to meet a legal obligation to which Stonite Coil is subject, including a lawful request by public authorities and national security or law enforcement obligations and applicable law, rule, order, or regulation.
- Where reasonably necessary for compliance or regulatory purposes or for the establishment of legal claims.

7.3. Individual rights

Those individuals whose personal information falls under the purview of this Policy are entitled to access the personal information that Stonite Coil maintains about them. Should any of this information be inaccurate, we welcome individuals to contact us for the purpose of correction, amendment, or deletion.

Furthermore, individuals may also have the option to, under specific circumstances, limit the use and disclosure of their personal information. Your ability to manage your personal data is a priority for us.

7.4. Security

Stonite Coil is dedicated to ensuring the security of personal information within its possession, implementing measures that align with the potential risks of loss, misuse, unauthorized access, disclosure, alteration, and destruction. These security measures are thoughtfully customized to address the unique characteristics of personal information, and the risks involved in its processing while adhering to industry best practices for data security and protection.

7.5. Enforcement

Stonite Coil is committed to addressing any IT security and data privacy concerns. If you have inquiries about this Policy or would like to report an information security incident, you may contact Carol Engel, Administrative Vice President confidentially and without fear of retaliation at cengel@stonitecoil.com.

8. IT Security Goals and Objectives

Stonite Coil commits to information security and data protection across its operations and stakeholders. As such, we have established the following objectives:

8.1 Qualitative Goals

- Continue existing and new internal security policies and procedures, including documented standards for system hardening, password complexity, and data handling.
- Implement industry best practice frameworks and guidelines relevant to the organization's sector and technology landscape.
- Apply legal and regulatory requirements mandates pertaining to third-party data privacy, internal IT security, and IT governance.
- Implement performance metrics and service level agreements (SLAs) related to system availability, incident response times, and data backup success rates.
- Assess the effectiveness of implemented corrective actions.

8.2 Quantitative Goals

- Achieve 100% completion of Phishing training for all employees using company computers by 2028.
- Ensure 100% of relevant employees receive training on data confidentiality / IT Security procedures by 2027.

9. Policy Review

This policy will be reviewed on an annual basis to ensure its effectiveness and that it adheres to the latest regulations, industry standards, and best practices in IT Security and Data Protection.

10. Related Documents

- Stonite Coil Incident Response Procedure Summary
- ThreatDown Firewall - Device monitoring report with fixes

  Sonicwall TZ-370 with Advanced Protection Security Suite

  -
  - Device Monitor Status - Stonite Coil
  - Patch Management Details - Stonite Coil

    Server,back up server, cloud

    Patches are managed through Microsoft Windows Update Server Service

    All PCs and Servers are protected with ThreatDown

    This removes viruses and scans for vulnerabilities

    I receive a report and then apply the needed updates to correct any issues

  - Patch Management Activity - Stonite Coil