Secure/Personal Information Disposal

Purpose:

The purpose of this Secure/Personal Information Disposal Standard Operating Procedure (SOP) is to establish guidelines and procedures for the secure disposal of personal and sensitive information within FrodoTech. This SOP aims to prevent unauthorized access to confidential data, maintain compliance with data regulations, and foster a culture of security and compliance. For questions regarding the disposal of secure information please call 1-800-353-5433 (1-800-ELF-LIFE) for more information or support..

Scope:

This SOP applies to all employees who handle or manage personal and sensitive information, including customer data and employee records. It encompasses the proper disposal of physical and digital documents containing sensitive information.

Responsibilities:

1. FrodoTech Staff: Responsible for identifying, segregating, and disposing of documents containing personal or sensitive information for secure disposal in accordance with this SOP. They are also responsible for participating in training and awareness programs related to secure information disposal.
2. Elven Enterprises: Responsible for overseeing the secure disposal of digital information and ensuring compliance with the SOP. They are also responsible for implementing technological solutions to enhance information security.
3. Management: Responsible for approving and supporting the implementation of secure disposal measures, conducting risk assessments, and promoting a culture of continuous improvement and collaboration across departments.

Prerequisites:

1. Secure disposal containers for physical documents.
2. Shredders for on-site document shredding.
3. Secure methods for deleting digital files and ensuring they cannot be recovered.

Procedure:

Identification of Sensitive Information:
- Train employees to spot documents with personal or sensitive info.
- Clearly mark these documents for secure disposal.

Collection and Segregation:
- Use secure containers for sensitive physical documents.
- Keep them separate from regular waste.

Disposal:
- Shred physical documents using onsite shredders.
- Delete digital files securely.

Verification:
- Regularly check if disposal procedures are followed.

Training and Awareness:
- Conduct regular training on secure disposal practices.

Incident Response:
- Establish procedures for reporting and addressing disposal incidents.

Risk Assessment:
- Regularly assess disposal risks and prioritize mitigation.

Continuous Improvement:
- Gather feedback and update procedures as needed.

Auditing and Compliance:
- Conduct audits to ensure compliance with regulations.

Environmental Considerations:
- Follow eco-friendly disposal practices.

Cross-Functional Collaboration:
- Foster collaboration between departments.

Documentation:
- Keep records of disposal activities and training.

Disposal Containers:
- Ensure secure placement and regular emptying.

Third-Party Services:
- Ensure compliance of external disposal service

Definitions:

- Secure Disposal Containers: Specifically designated receptacles for the collection of physical documents containing personal or sensitive information, ensuring their secure disposal.
- On-Site Shredders: Machines used to shred physical documents on the premises, converting them into irrecoverable fragments.
- Secure Deletion Methods: Advanced and secure techniques employed for the permanent erasure of digital files, ensuring they cannot be recovered.
- Verification Steps: Procedures implemented to confirm the successful disposal of both physical and digital sensitive information, providing an additional layer of security.
- Third-Party Disposal Services: External services contracted for the secure disposal of sensitive information, ensuring compliance with data protection regulations.

Revision History:

This SOP will be reviewed annually and updated as needed to reflect changes in technology, regulations, and the supermarket's operating environment

Date	Employee	Change
04/15/2024	Omar Ardid	"SOP: Secure/Personal Information Disposal"