Employee Handbook For IT Services

Developed by Elven Enterprises for Frodo Tech

Elven Enterprises (EvE) has the distinction and privilege of being partners with Frodo Tech. Elven Enterprises leads the way in the implementation of efficient and state-of-the-art networking and information technology services. As a partner of Frodo Tech, Elven Enterprises has put together this handbook in order to provide guidelines and instructions for navigating the technology you will be using day-to-day.

Agreements & Service Documents:

*Acceptable Use Agreement

Standard Operating Procedures:

1. Onboarding New Employees
2. Cybersecurity
3. Network Monitoring
4. Back Up & Data Restoration
5. Employee Termination
6. Secure/Personal Information Disposal
7. Network Change Management

**Must be signed by the employee before viewing any SOP's or documents on this Employee Handbook page.*

Acceptable Use Agreement

Developed by Elven Enterprises for FrodoTech

This Acceptable Use Agreement covers the entirety of communications throughout the FrodoTech network, security of said network and use of all FrodoTech information and IT resources. It also includes the use of email, internet, voice and mobile IT equipment associated with work at FrodoTech. This agreement applies to all FrodoTech employees, temps and contractors (who use company IT equipment).

This agreement applies to all information, in whatever form (digital or otherwise), relating to FrodoTech business activities regionally and nationally, and to all information handled by FrodoTech relating to outside organizations with whom it deals.

Computer Access Control – Employee Responsibility

Access to the FrodoTech IT network is controlled by Elven Enterprises. All User IDs and passwords are to be uniquely assigned by Elven Enterprises but employees are accountable for all actions on the FrodoTech IT systems.

Employees must NOT:

- ☐ Allow anyone else to use their user ID and password on any FrodoTech IT system.
- ☐ Leave their accounts logged in at an unattended computer.
- ☐ Use someone else's user ID and password to access FrodoTech IT systems.
- ☐ Leave their password unprotected.
- ☐ Execute any unauthorized changes to FrodoTech IT systems or information.
- ☐ Attempt to access data that they are not authorized to use or access.
- ☐ Exceed the limits of their authorisation or specific business need to interrogate the system or data.
- ☐ Connect any non-FrodoTech authorized device to the FrodoTech network or IT systems.
- ☐ Store FrodoTech data on any non-authorised FrodoTech equipment.
- ☐ Give or transfer FrodoTech data or software to any person or organization.

Internet and email Conditions of Use
Use of FrodoTech internet and email is intended for business use. Personal use is permitted in areas that do not affect the individual's productivity or performance and is not a security risk to FrodoTech in any way.

All employees are accountable for their actions on the internet and email systems.

Individuals must not:

- ☐ Use the internet or email for harassment or abuse of other employees or any other human beings for that matter..
- ☐ Use profanity, obscenities, overtly racial, insensitive or other derogatory remarks in communications.
- ☐ Access, download, send or receive any data (including images), which FrodoTech considers offensive in any way, including sexually explicit, discriminatory or defamatory.
- ☐ Use the internet or email to make personal gains, run "Side Hustle's" or conduct personal business.
- ☐ Post any information on the Internet that relates to FrodoTech, alter any information about it, or express any opinion about FrodoTech, unless they are specifically authorized to do this.
- ☐ Send unprotected sensitive or confidential information to external receivers.
- ☐ Forward FrodoTech mail to personal FrodoTech email accounts (gmail account for example).
- ☐ Make commitments through the internet or email on behalf of FrodoTech unless authorized to do so.
- ☐ Download copyrighted material such as music media (MP3 or MP4) files, film and video files without appropriate approval.
- ☐ Download any non-relevant software from the internet without prior approval of the IT Department.
- ☐ Connect FrodoTech devices to the internet using non-approved devices.

Clear Desk and Clear Screen Policy
In order to reduce the risk of losing information or unauthorized access, FrodoTech enforces a clear desk and screen policy as follows:

- ☐ Personal and/or confidential business data must be protected using the security features provided by Stone Wrought Technology.
- ☐ Computers must be logged off/locked or protected with a screen locking device or controlled by a password when unattended.

- ☐ Care must be taken to not leave physical, confidential material on printers or photocopiers.
- ☐ All business-related printed material must be disposed of using shredders or secure bins marked for regular destruction by a service.

Working Off-site
It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- ☐ The FordoTech Virtual Private Network (VPN) shall be used exclusively when accessing the HQ network or traveling.
- ☐ Commuting for business and working away from the office must be in line with FrodoTech remote working policy.
- ☐ Laptops must be locked in non-visible areas when left in vehicles (trunk or glove box for example.
- ☐ Laptops must be carried as carry on luggage when traveling.
- ☐ Information should be protected against loss or compromise when working remotely (for example at home or in public places). Laptop encryption must be used.
- ☐ Public Wifi must never be utilized while using devices to access the internet; hotspots or private connections only.

Mobile Storage Devices

Mobile devices such as flash drives, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only FrodoTech authorized mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

Software

Employees must only use software that is authorized by FrodoTech on FrodoTech computers. Authorized software must be used in accordance with the software supplier's licensing agreements. All software on FrodoTech computers must be approved and installed by the FrodoTech IT department.

Viruses

Elven Enterprises has implemented automated virus detection and antivirus software which update periodically within the FrodoTech IT structure. All PCs have antivirus software installed to detect and remove any virus automatically.

Employees must not:

- ☐ Remove or disable anti-virus software.

- ☐ Attempt to remove virus-infected files or clean up an infection, other than by the use of approved FrodoTech anti-virus software and procedures.

  Telephony (Voice) Equipment Conditions of Use

  Use of FrodoTech voice equipment is intended for business use. Individuals must not use FrodoTech voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances. All non-urgent personal communications should be made at an individual's own expense using alternative means of communications.

Employees must not:

- ☐ Use FrodoTech voice for conducting private business.
- ☐ Make "prank" calls or threatening calls to internal or external destinations.
- ☐ Accept reverse charge calls from domestic or International operators, unless it is for business use.

Actions upon Termination of Contract

All FrodoTech equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to FrodoTech at termination of contract.

All FrodoTech data or intellectual property developed or gained during the period of employment remains the property of FrodoTech and must not be retained beyond termination or reused for any other purpose.

I have read and understand the terms and conditions of this Acceptable Use Agreement.

Employee name (Print):

_____

Employee Signature:

_____

DATE:_____

Date	Employee	Change
04/15/2024	Steve Cherewaty	“Updated Acceptable Use Agreement”

Preferred Systems, Services and Software

Developed by Elven Enterprises for FrodoTech

Purpose:

The purpose of this list is to document and inventory the preferred systems, services and software Elven Enterprises uses to build, support and maintain FrodoTech's network.

Services:
Amazon Web Services

Software:
Veeam Backup
Pfsense virtual router
Windows Server 2019

Revision History:

Date	Employee	Change
4/17/24	Steve Cherewaty	Created Document: "Preferred Systems, Services and Software"

New Employee Onboarding

(Developed by Elven Enterprises in cooperation with FrodoTech Human Resources)

Purpose:

This SOP is to assist new employees in setting up their computer, email system and the tools they will use in the normal operations of FrodoTech. This, and other SOP's created by Elven Enterprises serve as guidelines for new hires to ensure an efficient, painless and smooth onboarding process. For questions regarding new employee onboarding please call 1-800-353-5433 (1-800-ELF-LIFE) for more information or support.

Scope:

This SOP is specifically for new employees who are unfamiliar with the separation of the FrodoTech satellite office and the Corporate HQ and also have not been configured for a workstation, user account or email.

Responsibilities:

The following organizations are responsible for the successful implementation of this SOP:

1. FrodoTech Human Resources department: Responsible for gathering necessary employee information, assigning a workstation, requesting permissions and using the network architecture.
2. Elven Enterprises: Responsible for engineering the network architecture, access and management therein.

Prerequisites:

Before setting up the necessary hardware and software as well as connecting to the company network, these prerequisites must be met:

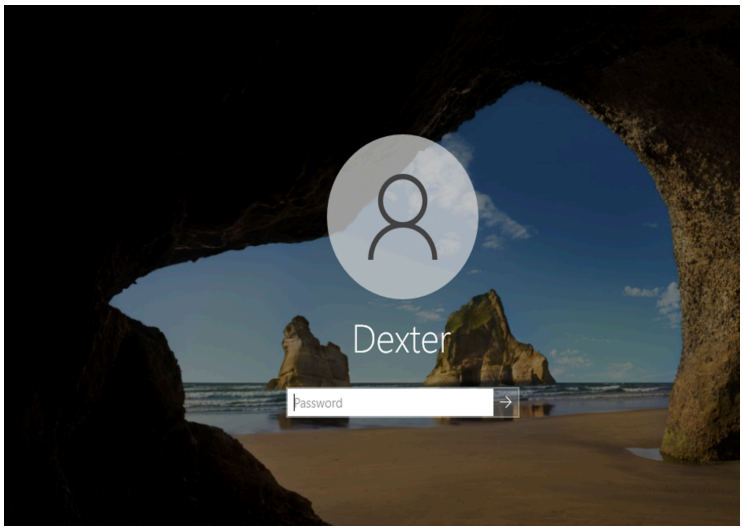
1. FrodoTech **Human Resources** must assign the new employee a computer workstation.
2. The workstation must meet Elven Enterprises minimum hardware requirements as well as have updated versions of software. See Elven Enterprises requirements HERE
3. All necessary IT agreements have been verified and signed by the new employee. If you have not signed the employee Acceptable Use Agreement you may do so HERE.

Procedure:

Elven Enterprises endeavors to make this process as simple as possible for new employees being onboarded. However, there are some steps the new employee must take to ensure the proper setup and installation of the necessary work tools.

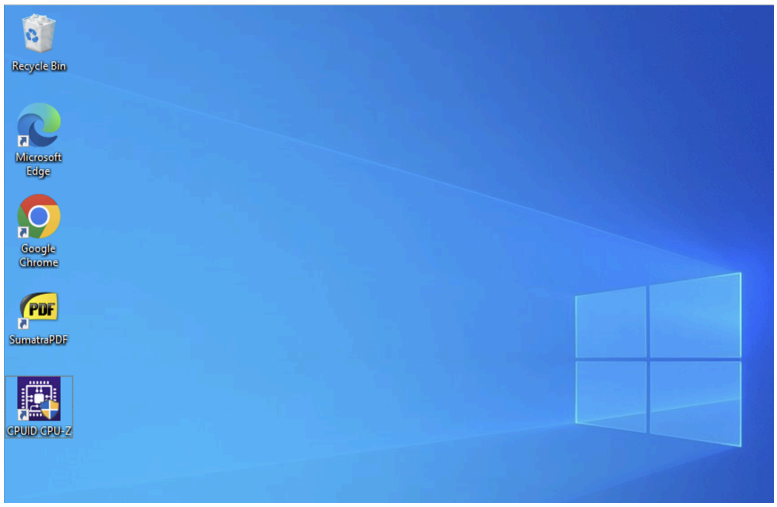
Computer Setup:

1. A Username has been set up for you and a temporary password has been issued.
2. Power-on your computer and wait until the screen looks like this (Dexter is just an example):



3. You will enter the temporary password the hiring manager gave to you. **You will be immediately prompted to change your password**. *Please make your password easily memorable and if you write it on a piece of paper, please secure it, memorize it and/or throw it away in a secure shredding bin.*

4. This is what your computer screen will look like once you're logged in



5. These are the programs Elven Enterprises will have installed for you

Email Account Setup:

1. Your company email has been set up for you by Elven Enterprises; it is an outlook account that comes with MS Office 365.
2. Your signature will be created for you but you're more than welcome to change it once you verify it's working.
3. Send a test email to your personal email and confirm it is operational.

VPN Tunnel:

1. Your company VPN has been set up for you by Elven Enterprises
2. If issues with the VPN or connecting to the company VPC arise

Shared Drive Setup:

1. You will have access to a local shared drive. This is an on-site machine that safeguards valuable documents which can be retrieved after a crash or disaster.
2. All company documents to be shared with other departments and employees must be saved to the saved drive.

Auto-backups:

1. OneDrive is the application chosen by Elven Enterprises to execute regular "cloud-based" backups.

References:

This document references and/or depends on processes from the following sections:

1. "Preferred Hardware and Software"
2. "Acceptable Use Agreement"

Definitions:

What words are used throughout this document and procedure which have specific meanings that must be respected.

1. Cloud
2. Software: programs or applications that run on a computer, such as Microsoft Office or Adobe Photoshop.
3. IT policies and procedures: guidelines and rules set by the company for the use of information technology resources and systems.

Revision History:

Date	Employee	Change
04/14/24	Steve Cherewaty	“SOP: New Employee Computer and Email Configuration”

Cybersecurity

Purpose

The purpose of this Cybersecurity SOP is to establish a comprehensive framework for protecting sensitive information, safeguarding customer data, and ensuring the confidentiality, integrity, and availability of all digital assets within FrodoTech. For questions regarding Elven Enterprises cybersecurity policy please call 1-800-353-5433 (1-800-ELF-LIFE) for more information or support.

Scope

This SOP applies to all employees and systems within Frodotech. It covers essential cybersecurity measures including employee training, access control, data protection, network security, physical security, incident response, vendor management, remote access security, regular security audits, and reporting security incidents.

Responsibilities

- FrodoTech Staff: Responsible for adhering to the cybersecurity training, following strict access control policies, and promptly reporting any security incidents.
- Elven Enterprises: Tasked with implementing and maintaining cybersecurity measures, conducting regular audits, and managing incident responses for FrodoTech.
- FrodoTech Management: Accountable for approving and supporting cybersecurity initiatives, ensuring policy compliance, and fostering a culture of security awareness among all staff.

Prerequisites

- Access to updated cybersecurity training materials.
- Secure and regularly updated computer systems.
- Antivirus and anti-malware software installed and active on all devices.
- Well-documented incident response plan.

Procedures

1. Employee Training and Awareness

- Conduct regular cybersecurity awareness training sessions coordinated by Elven Enterprises.
- Emphasize the importance of strong password policies and secure authentication practices.
- Train staff to identify phishing and social engineering attacks.

2. Access Control

- Ensure access is granted based on a strict need-to-know basis.
- Regularly review and revise access rights to prevent unauthorized access.
- Implement and maintain two-factor authentication systems through Elven Enterprises.

3. Data Protection

- Encrypt sensitive data both in transit and at rest, utilizing tools and protocols provided by Elven Enterprises.
- Perform regular backups of critical data, ensuring data recovery capabilities are robust and tested.
- Implement data retention and secure data disposal policies.

4. Network Security

- Keep antivirus software and network defense tools up-to-date, with updates and support provided by Elven Enterprises.
- Secure the Wi-Fi network with a robust passphrase and WPA3 encryption, regularly reviewed by Elven Enterprises.
- Regularly update and patch all software applications to mitigate vulnerabilities.

5. Physical Security

- Restrict physical access to critical servers and computing equipment.
- Secure all mobile devices to prevent unauthorized access and theft.
- Install and maintain surveillance cameras in strategic areas, with technical support from Elven Enterprises.

6. Incident Response Plan

- Develop, maintain, and regularly test a comprehensive incident response plan in collaboration with Elven Enterprises.
- Assign clear roles and responsibilities for incident response, ensuring rapid and effective action.
- Continuously improve the response plan based on drill outcomes and real incident learnings.

7. Vendor Management

- Thoroughly assess and vet all third-party vendors for compliance with Frodotech's security standards, supported by Elven Enterprises' expertise.
- Regularly review and update vendor contracts to ensure ongoing compliance and security.
- Monitor vendor performance and security practices continually.

8. Remote Access Security

- Implement secure remote access solutions with infrastructure and oversight provided by Elven Enterprises.
- Enforce the use of VPNs for all remote connections.
- Regularly review and adjust remote access policies to ensure they remain secure.

9. Regular Security Audits

- Schedule and conduct regular cybersecurity audits through Elven Enterprises.
- Promptly remediate any vulnerabilities identified during audits.
- Continuously monitor and enhance cybersecurity measures based on audit findings.

10. Reporting Security Incidents

- Establish a clear and straightforward process for all staff to report security incidents.
- Investigate and address all reported incidents promptly with assistance from Elven Enterprises.
- Document each incident thoroughly and use the findings to strengthen future security measures.

Date	Employee	Change
04/16/24	Bradley Baack	“SOP: Cybersecurity”

Network Monitoring

Purpose:

Network monitoring provides visibility into each layer of OSI, helping network administrators easily identify and troubleshoot network issues. Elven Enterprises will monitor traffic ensuring security of data exchange and guarding against suspicious activity. Employees of FrodoTech have already signed the Acceptable Use Agreement regarding what websites and services should and should not be accessed via company machines. The following is a high-level summary of Elven Enterprises Network Monitoring activities:

Common Network Devices to Monitor

- **Routers:** Routers help connect networks via the internet.
- **Switches:** Switches help connect devices such as servers, computers, printers, and more. Monitoring switches is critical to ensure network health and performance. It's also essential to monitor traffic and hardware through the switch.
- **Firewalls:** The role of a firewall is to protect the network by controlling incoming and outgoing traffic.
- **Servers:** Server monitoring helps provide information about the network, data usage, and more.

Scope:

This SOP outlines the infrastructure to regulate, supervise and control the network. IT will monitor network traffic, server performance, and protect confidential data. Elven Enterprises will help optimize network performance, decrease downtime and improve data security through this type of data surveillance.

Responsibilities:

1. FordoTech Staff: Responsible for adhering to cybersecurity training, following access control policies, and reporting security incidents promptly.
2. Elven Enterprises: Responsible for implementing and maintaining cybersecurity measures, conducting regular audits, and managing incident responses.
3. Management: Responsible for approving and supporting cybersecurity initiatives, ensuring compliance with policies, and fostering a culture of security awareness.

Prerequisites:

1. Access to cybersecurity training materials.
2. Secure and updated computer systems.
3. Secure Wi-Fi network with WPA3 encryption.
4. Antivirus and anti-malware software installed on all devices.
5. Incident response plan documentation.

Procedure:

Elven Enterprises will be using Wireshark through Kali-Linux for network monitoring. The IT team will take care of this process in the background. Specific details of Elven Enterprises procedures can be described further but require higher authorization.

Definitions:

Network monitoring is the process of constantly monitoring a computer network for problems such as slow traffic, suspicious activity and/or component failure.

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
4/15/24	Julian Pena	“SOP: Network Monitoring”

Back Up & Data Restoration

Purpose:

The purpose of this document is to outline the SOP for implementing an effective backup and data restoration solution within the realm of our IT services. For questions regarding Elven Enterprises backup and data restoration policy please call 1-800-353-5433 (1-800-ELF-LIFE) for more information or support.

Scope:

This SOP encompasses all aspects of data backup and restoration ensuring the availability of crucial information incase of potential data loss or system failures.

Responsibilities:

Elven Enterprises is responsible for the successful implementation of this SOP for the following:

- Design backup policies
- Monitor backup system for failure
- Troubleshoot and manage

User:

- Comply with data backup policies
- Report incidents of data loss as soon as possible

Prerequisites:

Before starting the setup process, the following prerequisites must be met:

1. Hardware and software components required for backup and restoration are available and properly configured
2. Document all record backups, storage locations, and restoration procedures
3. Install Veeam on each endpoint (individual computers)
4. AWS S3 (Simple Storage Service) Corporate account which serves as a repository for conglomerated company data.

Procedure:

Backups of endpoints are scheduled every 24 hours and will happen regardless of FrodoTech employees' disposition. Veeam (a backup application) is installed on every user's endpoint. In almost all cases, this is a process FrodoTech employees will NOT need to manage. However, should the installed application or specific scheduling interfere with an employee's work operations please call 1-800-353-5433 (1-800-ELF-LIFE) for one-off solutions.

Backups:

1. Identifying all data within the organization that requires backup
2. Automate Backups inside of endpoint Veeam applications
3. Monitor backup processes, troubleshoot when necessary

Restoration:

1. Identify the affected files, applications, and databases
2. Identify the appropriate backup selection
3. Begin the restoration process according to the documented plan.

References:

Sources this document pulls from or references, or simply extended reading/documentation on this subject.

1. Veeam - https://www.youtube.com/watch?v=ptcRJ0nl4Bw
2. Amazon S3 - https://www.youtube.com/watch?v=77lMCiiMilo

Definitions:

What words are used throughout this document and procedure which have specific meanings that must be respected.

1. Hardware: physical components of a computer
2. Software: programs or applications that run on a computer

Date	Employee	Change
04/16/24	Brad Baack	"SOP: Backup and Data Restoration"

Employee Termination

Purpose:

The purpose of this SOP is to establish clear guidelines for the termination of an employee's employment. By outlining specific steps to be followed, the SOP ensures that the termination process is carried out efficiently, with respect for the employee, and in alignment with company policies and procedures. For questions regarding Elven Enterprises employee termination policy please call 1-800-353-5433 (1-800-ELF-LIFE) for more information or support.

Scope:

This SOP applies to all employees, supervisors, managers, and HR personnel involved in the termination process within FrodoTech.
Responsibilities:
The following individuals are responsible for the successful implementation of this SOP:

1. Human Resources:
    - Start and oversee the termination process.
    - Handle exit interviews and paperwork.
    - Keep record of the termination.
2. Managers/Supervisors:
    - Advice HR when someone needs to be let go.
    - Help with paperwork and discussions if needed.
    - Help with employee transition out.
3. IT:
    - Block access to company systems.
    - Collect company devices and keep data secure.
4. Employees Leaving:
    - Follow termination process
    - Return company stuff

Prerequisites:

The information, resources, permissions, etc. required to execute this procedure.

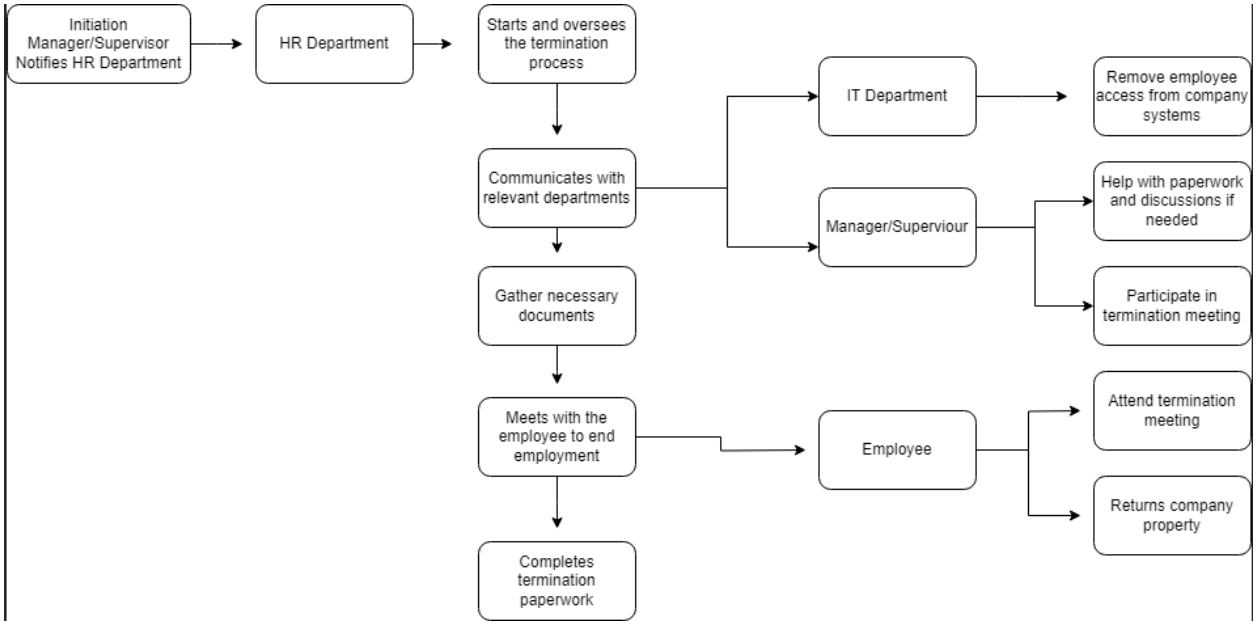
1. Updated Documentation: Ensure all necessary documents are prepared and accessible.
2. Clear Communication: Establish communication between departments involved in the termination process.
3. Training: Provide training on conducting termination meetings and handling paperwork.
4. Confidentiality Measures: Implement procedures to maintain the confidentiality of termination-related information.

Procedure:

1. Initiation:
    - HR or the supervisor initiates the termination process by notifying HR.
2. Document Review:
    - HR reviews and gathers all necessary documents related to the termination.
3. Communication:
    - HR communicates with relevant departments involved in the termination process to ensure coordination and compliance.
4. Training:
    - Provide training to those involved in conducting termination meetings and handling paperwork.
5. Termination Meeting:
    - HR schedules and conducts the termination meeting with the employee.
6. Paperwork:
    - Complete all necessary paperwork, including termination letters and final payments.
7. IT and Facilities:
    - The IT department disables the employee's access to company systems, and facilities management retrieves company property.
8. Confidentiality:
    - Implement procedures to maintain the confidentiality of termination-related information.
9. Documentation:
    - Document all steps taken during the termination process for record-keeping and compliance purposes.

Definitions:

1. Employee Termination: The process of ending an employee's employment within an organization, which may occur voluntarily or involuntarily.
2. HR: Human Resources department responsible for managing employee-related matters with an organization.
3. IT: Information Technology department responsible for managing and maintaining computer systems, networks, and digital infrastructure.



Revision History:

Date	Employee	Change
04/15/2024	Omar Ardid	“SOP: Employee Termination”

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”

Network Change Management

This SOP outlines the procedures for managing changes to the network infrastructure to minimize disruption and ensure network stability. For questions regarding Elven Enterprises Network Change Management policy please call 1-800-353-5433 (1-800-ELF-LIFE) for more information or support.

Purpose

- Standardize the approach to network changes.
- Minimize risks associated with network modifications.
- Ensure proper documentation and communication of network changes.

Scope

This SOP applies to all planned changes to the network infrastructure, including:

- Hardware additions, removals, or upgrades
- Software installations, updates, or configuration changes
- Security policy modifications
- Network topology changes

Responsibilities

- **Change Requester:** Initiates the change request process by submitting a detailed description of the desired change.
- **Change Advisory Board (CAB):** Reviews change requests, assesses risks, and approves or rejects them.
- **Network Engineer:** Implements approved changes, conducts testing, and documents the process.
- **Stakeholders:** Are informed of planned changes and potential impacts.
-

Prerequisites

- Robust network

- Competent management

Procedures

Change Request Process

1. Submitting a Change Request:

- The Change Requester submits a formal request outlining:
    - The nature of the change
    - Justification for the change
    - Expected impact on the network
- The request is categorized based on complexity and risk.

2. Change Review and Approval:

- The CAB reviews the request, assesses potential risks, and determines the approval process.
    - Low-risk changes may receive expedited approval.
    - High-risk changes may require further analysis and testing.
- The CAB approves, rejects, or requests modifications to the change request.

Change Implementation

Once approved, the Network Engineer implements the change according to the approved plan. This may involve:

- Scheduling downtime (if necessary)
- Configuring devices
- Implementing security updates
- Documenting the entire process

Testing and Rollback

- Thorough testing is conducted to verify the success of the change and identify any unintended consequences.
- A rollback plan is established to revert to the previous configuration if necessary.

Communication and Documentation

- All stakeholders are informed of the planned change, potential impact, and expected timeline.

- The change request, approval process, implementation details, and testing results are documented for future reference.

Post-Implementation Review

- The CAB conducts a review to assess the effectiveness of the change and identify any lessons learned.

Continuous Improvement

- The SOP is reviewed and updated periodically to reflect best practices and address evolving network needs.

Date	Employee	Change
04/19/24	Steve Cherewaty	“SOP: Network Change Management”