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”