Methownet Cyber Security Plan

Version: 2025
Prepared by: April Wertz
Reviewed by: Jeff Hardy, Dustin Soodak
Company: Methownet, LLC
Date: March 24, 2025

Introduction

This document outlines Methownet's cybersecurity practices, responsibilities, and controls in alignment with the **NIST Cybersecurity Framework (CSF)**. It serves as a foundation for maintaining a secure operational environment and guiding future improvements.

---

1. Governance and Team Structure

Cybersecurity Oversight

- **System Administrator / Cybersecurity Lead:** Jeff Hardy
- **Network Analyst / Server Admin:** Dustin Soodak
- **Network Support:** April Wertz
- **First Contact for Incident Reporting:** April Wertz

Cybersecurity Incident Chain of Command

1. April Wertz (Initial Notification)
2. Dustin Soodak (Escalates to Jeff)
3. Jeff and Dustin (Coordinate via text or phone depending on severity)

---

2. Access Control

- Dustin manages user access and system restrictions.
- Remote access to internal databases is restricted by IP and user credentials.
- Customer access systems and software installations are similarly restricted.
- VPN access is limited to Jeff Hardy, Dustin Soodak, Levi Murphy, and April Wertz.
- Two-Factor Authentication (2FA) is not yet implemented but recognized as a future improvement area.

---

3. System Maintenance and Backups

- **Server Backups:** Managed by Dustin using cron jobs.
- **VMware Snapshots/Backups:** Maintained by Jeff Hardy and Clint.
- Backups are verified and stored internally.

---

4. Monitoring and Logging

Daily log monitoring is conducted by April Wertz using custom scripts that retrieve key entries from the following systems:

- Mail Server
- Phone Server
- Main Firewall
- Office Switch
- Juniper Distribution and Access Switches

Logs are rotated weekly based on system storage availability.

---

5. Physical Security

- Building access is limited to keyholders only.
- Server access is restricted to authorized personnel.

---

6. System Integrity

- Systems are locked down using IP address filtering and credential authentication.
- Software updates and patches are handled internally with a focus on service stability.
- The primary firewall is a MikroTik RouterBOARD.

---

7. Email and DNS Security

- April Wertz is responsible for managing email and DNS configurations, as well as monitoring threats.
- Email filtering and logging systems are in place to detect malicious activity.

---

8. Vendor and Remote Access

- All remote database access is tightly controlled by Dustin Soodak.
- System access for remote users is secured through VPN.

---

9. Continuous Improvement Goals

- Implement Two-Factor Authentication (2FA) on all critical systems.
- Improve documentation and logging of system changes.
- Schedule and conduct regular security awareness training.
- Develop, formalize, and test a disaster recovery and contingency plan.
