Potter Fire Systems
Cybersecurity Manual

POTTER
The Symbol of Protection

Potter Electric Signal Company, LLC
St. Louis, MO
Customer Service: (866) 240-1870 • Technical Support: (866) 956-1211 • Fax: (314) 595-6999
For listing information visit our web site www.pottersignal.com

Manual #5403818 • Rev A • 12/25

Table of Contents

1. Introduction

The NFPA-72 (2025) edition introduces specific cybersecurity expectations for fire alarm systems, including secure configuration, controlled access, software/firmware integrity, and documentation supplied by the manufacturer.

This manual is provided to support those requirements. It describes the cybersecurity features of Potter fire products, the responsibilities of installers and system owners, and the practices necessary to maintain a secure life-safety system throughout its lifecycle. When implemented as described, these measures help ensure code compliance and enhance system resilience against cyber threats.

2. Scope of the Products Covered

This Cybersecurity Manual applies to Potter fire alarm control equipment, networked components, communication interfaces, and software platforms that implement configuration, user access, networking, or remote connectivity. Specifically, this document covers:

- **Fire Alarm Control Panels & Annunciator**: IPA-4000 (including E and V variants), IPA-100, IPA-60, AFC-1000 (including E and V variants), AFC-100, AFC-50, PFC-6006, PFC-4064, and PFC-5008, GTSA-7
- **Supervisory and Graphical Interfaces**: PotterNet, PotterNet-UL, PotterNet-UL-TS, PotterNet-Lite, PotterNet-FOW, PotterNet-FOW-UL
- **Communication and Integration Devices**: IntelliCom-5GV, IntelliCom-5GA, IntelliCom-5GMC, Modbus-Link, BACnet-Link, NCE-1000, NCF-1000, FCB-1000.
- **Cloud Services**: IntelliView, IntelliView mobile apps.
- **Local User Interfaces and Plink Devices**: PSK-1000, SCUI-1000, and similar annunciators and keypads. These devices rely on the authentication, permissions, and event logging implemented by the host fire alarm control panel.
- **Auxiliary Power Supplies and Audio Equipment**: PSN-106, PSN-64, PSB-10, FFT-1000, SCA and DCA series amplifiers and related modules. These devices do not implement independent user authentication or IP networking; their cybersecurity posture is governed by the connected control equipment and by physical security of the installation.
- **Addressable Field Devices**: PAD-300 and other addressable SLC devices. Additional Potter products that implement networking, user authentication, remote connectivity, or system configuration functions should be considered within the scope of this manual and follow the principles described herein.
- **System Support Tools**: PotterLink, Potter Fire Panel Programmer, PotterLink, Web sites

3. Fire Alarm Control Panels

Fire alarm control panels form the core of the life-safety system and are responsible for event processing, device supervision, annunciation, and system logic. Because these panels store configuration data, user accounts, passwords, and network settings, they represent a primary cybersecurity boundary for the entire system. This section provides the required cybersecurity guidance for Potter fire alarm control panels in accordance with NFPA-72 (2025).

3.1 System Access & Authentication

- Fire alarm control panels require authenticated access for configuration, programming, and management.
- User permissions should be assigned based on role (e.g., Installer, Service, Operator).
- Default passwords must be changed at installation.
- Passwords should be complex and be protected against unauthorized disclosure.
- Access to configuration interfaces (keypad, P-COMM port or other) must be limited to authorized personnel.

Installer Responsibilities

- Change all default credentials during commissioning.
- Restrict access to programming tools, keys, and passwords.
- Document and hand over credentials securely to the system owner.

Installer Responsibilities

- Maintain control of user accounts and restrict access to trained personnel.
- Remove or disable accounts of individuals who no longer require access.

3.2 Network Security

FACPs must operate on a dedicated fire network or a properly segmented VLAN/VPN that is isolated from general-purpose IT networks. No device on an enterprise network should have direct Layer-2 or Layer-3 access to a fire panel unless explicitly approved by the system owner and protected by firewall rules.

FACPs support Ethernet/IP for:

- PotterNet communication
- Peer-to-peer fire network
- Intellicom reporting
- Integration gateways
- Email
- Time synchronization
- Central station reporting

Because these interfaces are used for routing life-safety messages, they must be deployed on protected networks.

Minumum Network Requirements:

- Static IP addresses are recommended for each panel and supervisory station.
- No inbound internet access.
- All panel IP traffic must be behind a firewall, router, or segmented network.
- Only required ports may be opened.
- VPN or VLAN recommended for multi-building or campus networks.

Communication Security

FACPs must operate on a dedicated fire network or a properly segmented VLAN/VPN that is isolated from general-purpose IT networks. No device on an enterprise network should have direct Layer-2 or Layer-3 access to a fire panel unless explicitly approved by the system owner and protected by firewall rules.

3.3 Secure Configuration Practices

- Only required network services and features should be enabled on the control panel.
- Panels should be installed in a normally locked, protected electrical room or enclosure.
- Unused communication ports should remain closed or disabled.
- Panels must be programmed following Potter’s secure configuration recommendations and installation manuals.

3.4 Communication Security

Fire alarm control panels communicate with network cards (NCE-1000, NCF-1000), annunciators, remote devices, and integration modules.

- Panel-to-network-card communication is designed for closed, supervised life-safety networks.
- When connected to IP networks, the panel must be isolated behind a firewall or secure network segment.
- Only outbound or panel-to-panel ports required should be permitted.
- No inbound ports from public networks should be opened.

Best Practices

- Use a dedicated VLAN or physically separate network where possible.
- Prevent direct exposure of panel traffic to the public internet.
- Follow industry accepted firewall and routing recommendations for safe deployment.

3.5 Firmware Integrity & Updates

- System owners and installers are responsible for ensuring that panels and network devices remain on current, supported firmware versions. Potter publishes firmware through formal ECO (Engineering Change Order) processes; only ECO-released firmware should be installed on field equipment.
- Fire alarm control panel firmware must be kept current to ensure ongoing security, reliability, and compatibility with connected modules.
- Firmware should only be loaded using approved Potter tools and official distribution sources.
- Installers must verify the authenticity of firmware prior to applying updates.
- Unauthorized or modified firmware must never be installed.

Notes for AHJs and Owners

- Firmware updates are controlled and validated through Potter’s ECO release process.Prevent direct exposure of panel traffic to the public internet.
- Panels log events related to configuration changes and firmware updates where supported.

3.6 Physical Security

- Panels, cabinets, and auxiliary enclosures must remain locked to prevent unauthorized access.
- Keys and access methods should be controlled by facility management.
- Physical tampering is detected through standard fire alarm supervisory mechanisms (where applicable) and must be investigated immediately.

3.7 Logging and Event Tracking

- Fire alarm control panels log operational events, troubles, supervisory conditions, and configuration changes.
- Where applicable, panels record:
  - Programming changes
  - User logins
  - Network card faults
  - Firmware update events

These logs provide part of the cybersecurity audit trail required by NFPA-72 (2025).

3.8 Boundary with Other Systems

- The control panel is considered part of the protected life-safety system and should not share networks with general-purpose IT systems unless properly segmented.
- Integration to external systems (e.g., Modbus-Link, BACnet-Link, IntelliCom, PotterNet servers, third party BMS/SCADA) must be done through secured, documented interfaces.
- The system owner is responsible for maintaining the cybersecurity of networks external to the fire alarm control panel.

3.9 Local User Interfaces and P-Link Devices

P-Link devices (PSK-1000, SCUI-1000, RA-6500 and similar devices, annunciators and keypads) rely on the authentication, permissions, and event logging implemented by the host fire alarm control panel.

4. Cloud Services

IntelliView is a secure cloud-based service used to monitor, view, and manage information. IntelliView integrates with IntelliCom, IntelliView Link or PotterNet (transmitters) using authenticated and encrypted communication channels.

Security Functions

- All communications between transmitters and IntelliView use encrypted transport (TLS or equivalent).
- IntelliView requires authenticated user access with role-based controls.
- User accounts and passwords are managed through the IntelliView portal.
- Session security and password policies are enforced by the cloud platform.

Installer Responsibilities

- Ensure that transmitters are installed behind a secure, managed network (e.g., firewall/NAT).
- Configure only the required outbound ports and protocols for cloud communication.
- Ensure default passwords and credentials on the transmitters are changed.

Owner Responsibilities

- Maintain secure access to IntelliView (account management, strong passwords).
- Grant access only to authorized users.
- Remove users who no longer require access.

Manufacturer Responsibilities

- Maintain cloud infrastructure security, patching, monitoring, and access control.
- Provide firmware updates to the transmitters to ensure secure communication.
- Monitor system integrity and notify customers of security-relevant updates or advisories.

5. Auxiliary Power and Audio Equipment

These devices do not implement independent user authentication or IP networking. Their cybersecurity posture is governed by the control panel and system design. Physical access control still matters (locked enclosures, secure rooms, etc.).

6. Addressable Field Devices

PAD-300 and other addressable SLC devices are supervised by the control panel and do not provide general-purpose networking or user accounts. Cybersecurity protections for these devices are achieved through secure panel configuration, SLC wiring practices, and physical protection of system components.

7. Supervisory and Graphical Interfaces

PotterNet is a supervised fire alarm graphical workstation that communicates with Potter fire alarm control panels and provides centralized monitoring, annunciation, and system configuration. In accordance with NFPA-72 (2025), PotterNet incorporates security controls designed to protect configuration data, limit unauthorized access, and ensure secure communication with connected life-safety equipment.

PotterNet supports NFPA-72 (2025) cybersecurity requirements through the following measures:

Secure Communication

- Communication between PotterNet and Potter fire alarm control panels is performed over encrypted connections using TLS 1.2.
- Panel communication occurs only on designated TCP ports, which must be restricted by the installer through firewalls or network access control lists.
- PotterNet requires static IP addresses, supporting stable, secured supervisory links.
- To minimize risk, PotterNet servers should be placed on a dedicated supervisory network segment that is isolated from general corporate IT traffic. IT administrators should restrict access to the PotterNet host machine using ACLs (Access Control Lists), VLAN boundaries, or firewall rules.

Port Requirements

- PotterNet requires that specific ports on the external and internal firewalls be open. This section summarizes the ports and protocols that will be used. This information should be provided to the appropriate IT personnel in order to be sure all equipment is configured properly.

Initiating Software or Product	*Receiving Software or Product*	*Port*	*Protocol*	*Definition*
PotterNet Studio	FACP	69	UDP	Panel importer to copy the configuration from a newly added FACP. Trivial File Transfer Protocol (TFTP)
PotterNet	PotterNet	32001	TCP	PotterNet TCP connection
PotterNet	PotterNet Server	32002	TCP	PotterNet database synchronization
PotterNet	FACP	32000	TCP	This is the default port used by the fire panels. Potter recommends using this port. If the port on the FACP is changed, then it needs to be addressed in the firewall settings.
PotterNet	PotterLink (12.232.138.145)	443	TCP/HTTPS	PotterNet connection to Potter Licensing Server

If the system includes BACnet connectivity using the PotterNet BACnet Server then the following ports must be open:

Initiating Software or Product	*Receiving Software or Product*	*Port*	*Protocol*	*Definition*
PotterNet Studio	BACnet Device	47808	UDP	BACnet device discovery default port Existing BACnet system dependent
PotterNet	BACnet Device	32003	TCP	PotterNet TCP connection
PotterNet	BACnet Device	47808	UDP	Default port for BACnet communications Existing BACnet system dependent

Access Control & Authentication

- PotterNet requires authenticated access and uses industry-standard password hashing and salting (PBKDF2) for credential protection.
- User roles, permissions, and operational capabilities (acknowledge, reset, silence, configuration, reporting) are controlled through a role-based permission system.
- Default administrator credentials must be changed during commissioning.

System Hardening & Operating Environment

PotterNet imposes strict PC hardening requirements, including:

- A dedicated Windows 10 or 11 Professional or UL-listed PC
- Antivirus protection
- Control of Windows Update behavior
- Restriction against installing non-approved applications
- Data in transit or stored on PotterNet is encrypted using AES 256.

Anti-Virus Software Compatibility

Computer security is critical to the long term operation of your system. It is important to protect your system against ransomware, Trojans, viruses, and other types of malware. No other software other than the operating system software and anti-virus/security protection software can be installed on any of the computers running PotterNet.

Windows User Permissions

An administrator account does not need to be used, but it is acceptable to do so. PotterNet is intended to always be active on the computer unless performing maintenance on the PC.

PotterNet does not support LDAP or Windows Active Directory accounts.

Windows Updates

It is important that the Windows operating system be kept current with the latest releases. It is also important that Windows updates do not disrupt the monitoring of your life safety system. It is recommended that Automatic Updates are enabled and set to the option for “notify for install”. A site-specific plan should be created that allows for the installation of the updates while minimizing impact to fire protection.

Logging and Accountability

- PotterNet maintains logs of user actions, system events, client/server synchronization, and panel data.
- Configuration changes require authenticated access and create traceable events, supporting NFPA-72 (2025) audit and accountability expectations.

Manufacturer Responsibilities

Potter maintains PotterNet software through periodic updates, security patches, and feature improvements. Installers and owners are expected to apply updates in accordance with Potter's recommendations to ensure ongoing cybersecurity compliance.

8. Supervisory and Graphical Interfaces

Communication and integration devices provide the vital connectivity between Potter fire alarm control panels, cloud services, central station monitoring, and third-party building management systems (BMS/SCADA). Because these devices bridge the fire alarm system to external networks, they represent a key cybersecurity boundary within the overall life-safety architecture. This section describes the cybersecurity practices required for the safe deployment, configuration, and maintenance of the following Potter products:

- **IntelliCom Series:** IntelliCom-5GV, IntelliCom-5GA, IntelliCom-5GMC
- **System Integration Gateways:** Modbus-Link, BACnet-Link, IntelliView-Link
- **Cloud Connectivity Components:** IntelliView cloud services (as part of IntelliCom ecosystem)

All devices in this category must be installed, configured, and maintained in accordance with NFPA-72 (2025), which requires that systems employing networked communication paths incorporate appropriate cybersecurity protections, including authentication, segmentation, encryption, supervised network connections, and physical protection of interface points.

8.1 Secure Communication

Encrypted Communication Channels

- **Modbus-Link** uses TCP/IP communication and supports optional whitelisting to restrict which Modbus masters can connect.
- **BACnet-Link** uses Ethernet BACnet/IP communication and supports segregation through VLAN, VPN, or dedicated fire networks.
- **IntelliView-Link** (PC-based) uses HTTPS/TLS 1.2 to communicate with Potter cloud services.
- **IntelliCom** uses encrypted IP communication to the Potter Communication Center (PCC) using secure cellular or LAN pathways, ensuring alarm data is protected in transit.

Port Restrictions and Protocol Control

Each device uses only specific ports and well-defined protocols:

- **Modbus-Link:**

  Modbus Link requires that specific ports on the external and internal firewalls be open. This section summarizes the ports and protocols that will be used. This information should be provided to the appropriate IT personnel in order to be sure all equipment is configured properly.

Initiating Software or Product	*Receiving Software or Product*	*Port*	*Protocol*	*Definition*
Modbus Link	BMS/SCADA/DCIM	502	TCP	Modbus Link TCP connection
Modbus Link	FACP	32000	TCP	Default port of 32000 is configurable and may be changed
Modbus Link	FACP	69	UDP/TFTP	Periodically copy the configuration from each FACP
Modbus Link	www. potterlink.com	443	TCP/HTTPS	Connection to Potter licensing server

- **BACnet-Link:**

  BACnet Link requires that specific ports on the external and internal firewalls be open. This section summarizes the ports and protocols that will be used. This information should be provided to the appropriate IT personnel in order to be sure all equipment is configured properly.

Initiating Software or Product	*Receiving Software or Product*	*Port*	*Protocol*	*Definition*
BACnet Link	BACnet Device	47808	UDP	Default port for BACnet Communication
BACnet Link	FACP	69	UDP	Panel importer to cope the configuration from the newly added FACP. Trivial File transfer Protocol (TFTP)
BACnet Link	FACP	32000	TCP	This is the default port used by the fire panels. Potter recommends using this port. If the port on the FACP is changed, then it needs to be addressed in the firewall settings
BACnet Link	www.potterlink.com (13.232.138.145)	443	TCP/HTTPS	BACnet Link Connection to Licensing Server.

- **IntelliView-Link:**

  IntelliView Link requires that specific ports on the external and internal firewalls be open. This section summarizes the ports and protocols that will be used. This information should be provided to the appropriate IT personnel in order to be sure all equipment is configured properly.

Initiating Software or Product	*Receiving Software or Product*	*Port*	*Protocol*	*Definition*
IntelliView Link	FACP	32000	TCP	Default port of 32000 is configurable and may be changed
IntelliView Link	FACP	69	UDP/TFTP	Periodically copy the configuration from each FACP
IntelliView Link	www.potterintelliview.com	8883	TCP/MQTTS	Communications with the Potter IntelliView server
IntelliView Link	www. potterlink.com	443	TCP/HTTPS	Connection to Potter licensing server

- **IntelliCom:**
  - ○ Uses cellular encrypted paths and/or LAN with strict protocol mapping to the PCC; supports end-to-end acknowledgment.

  Modbus Link requires that specific ports on the external and internal firewalls be open. This section summarizes the ports and protocols that will be used. This information should be provided to the appropriate IT personnel in order to be sure all equipment is configured properly.

8.2 Logging and Event Tracking

User Authentication

- IntelliCom / IntelliView require authenticated dealer accounts for configuration, cloud access, backups, walk tests, and programming.
- Modbus-Link and BACnet-Link require authentication to PotterLink licensing servers and use local Windows OS user permissions.

Client Access Control

- Modbus-Link includes an optional IP address whitelist to restrict acceptable Modbus master connections.

8.3 System Hardening Requirements

PC-Based Integrations (Modbus-Link, BACnet-Link, IntelliView-Link)

- Must run on Windows 10 or 11 Professional PCs or VMs
- Windows auto-update should be manual only to avoid disruption while maintaining security patching.
- No unapproved software should be installed on machines used for fire system integration.

IntelliCom Gateways

- Require controlled access to the enclosure, protected antenna cabling, and restricted LAN configuration.

8.4 Network Segmentation and Isolation

NFPA-72 (2025) expects that fire system communications are isolated from general-purpose networks when cybersecurity risks exist.

Proper practices include:

- Using dedicated VLANs or physically separate fire networks for Modbus/BACnet traffic.
- Preventing inbound traffic from public networks toward any device in the fire system.
- Allowing only required communication paths (LAN → PCC, LAN → BMS, LAN → Potter panels).

These segmentation and isolation requirements are intended to satisfy NFPA-72 (2025) Section 11.5 for network-connectable equipment using shared pathways, by ensuring that communication paths shared with other systems are documented, supervised, and installed in accordance with the shared pathway requirements of NFPA-72 (2025) Sections 23.6.3.3 through 23.6.3.5 and 7.6.7.

8.5 Data Integrity, Logging, and Supervision

Supervision

- Modbus-Link and BACnet-Link supervise panel connections and license validity
- IntelliCom supervises both cellular and LAN paths, including Link Supervision No unapproved software should be installed on machines used for fire system integration.

Logging

- Events such as alarm transmissions, failures, status checks, and configuration changes are stored at the Potter Communication Center (PCC) to support audit requirements.
- PC-based systems rely on Windows system logs for authentication events and application logs for configuration tracking.

8.6 Physical Security

- All devices must be installed in tamper-resistant enclosures; IntelliCom supports optional tamper switches.
- Ethernet and RS-485 wiring should be protected from damage and unauthorized access.

8.7 Cloud-Connected Services

Products such as **IntelliCom-5G** and **IntelliView-Link** connect to Potter cloud infrastructure for services like:

- Encrypted program backup and restore
- Remote programming
- Test and inspection tools

These connections use **HTTPS/TLS** and require authenticated dealer accounts, satisfying NFPA-72 requirements for secure remote access.

8.8 Installer Responsibilities (NFPA-72 2025 Alignment)

Installers must:

- Change default passwords for all integrated systems
- Implement firewall rules limiting traffic to documented ports
- Isolate fire system devices on dedicated or segmented networks
- Verify licensing systems (where applicable) successfully authenticate
- Protect physical wiring and enclosures
- Document cybersecurity configuration and provide it to the owner

9. Cybersecurity Risk Assessment

NFPA-72 (2025) requires fire alarm equipment manufacturers to conduct and document a high-level cybersecurity risk assessment. This section provides Potter's evaluation of the cybersecurity considerations associated with network-connected fire alarm control equipment, communication devices, integration gateways, and cloud-based services.

The assessment identifies foreseeable cybersecurity threats, summarizes existing system protections, and outlines recommended installation practices to support secure deployment of Potter fire systems.

This assessment is not intended to replace customer IT security policies or detailed organizational risk management processes. Instead, it provides the required manufacturer-level review of cybersecurity considerations as they relate specifically to Potter fire alarm products and system architecture.

This high-level assessment is included in accordance with NFPA-72 (2025), Section 11.8 – Cybersecurity, which requires manufacturers to document foreseeable cyber risks and provide guidance to installers and system owners.

9.1 Assessment Scope

This cybersecurity risk assessment applies to Potter products that perform networking, signaling, configuration transfer, cloud interaction, or integration with external systems, including:

- Fire Alarm Control Panels (IPA, AFC, ARC, PFC series)
- Supervisory software platforms (PotterNet, PotterNet-Lite, PotterNet-UL/TS, PotterNet-FOW)
- Communication devices (IntelliCom-5GV/5GA/5GMC, IntelliView-Link)
- Network and integration gateways (Modbus-Link, BACnet-Link)
- Cloud services

This cybersecurity risk assessment applies to Potter products that perform networking, signaling, configuration transfer, cloud interaction, or integration with external systems, including

9.2 Identified Cybersecurity Risk Areas

Based on Potter's system architecture, communication pathways, and supported networking environments, the following high-level risk areas have been identified:

9.2.1 Unauthorized System Access

Potential Risks:

- Unauthorized access to FACP programming or panel menus
- Unauthorized access to PotterNet or cloud management interfaces
- Reuse of default or weak user credentials

9.2.2 Network-Based Threats

Potential Risks:

- Misconfigured firewalls revealing panel ports
- Exposure of Modbus or BACnet integration points
- Interception or manipulation of data on unsegmented networks

9.2.3 Physical Security Threats

Potential Risks:

- Tampering with panel enclosures, network cards, or gateway devices
- Removal, splicing, or re-routing of supervised wiring
- Unauthorized access to data interfaces

9.2.4 Cloud and Remote Connectivity Risks

Potential Risks:

- Compromise of credentials for IntelliView cloud services
- Misconfigured network equipment allowing unwanted inbound connections
- Loss of supervisory connection to cloud, causing operational delays

9.2.5 Firmware, Software, and Configuration Integrity

Potential Risks:

- Installation of unauthorized or outdated firmware
- Corruption of configuration files due to improper handling
- Malware on Windows-based integration PCs (BACnet-Link, Modbus-Link, IntelliView-Link)

9.3 Likelihood and Impact Summary

Consistent with NFPA-72's requirement for a "high-level" assessment, Potter categorizes risks qualitatively rather than using formal quantitative scoring.

Risk Area	*Likelihood*	*Potential Impact*
Unauthorized access to FACP or PotterNet	Medium	High
Network exposure of panels or gateways	Medium	High
Improperly maintained integration PCs	Medium	Medium
Cloud communication loss	Low	Low
Physical tampering	Low	Medium

9.4 Existing Mitigations Provided by Potter

Potter implements multiple technical and architectural controls that address the above risk areas:

9.4.1 Authentication & Access Control

- PotterNet uses password hashing, salting (PBKDF2), and role-based permissions
- IntelliView and IntelliCom require authenticated dealer accounts for remote programming, reporting, backups, and configuration.
- Panel programming interfaces require installer credentials.

9.4.2 Encrypted Communications

- PotterNet communicates with panels using TLS 1.2 encrypted channels.
- IntelliCom uses encrypted cellular/IP communication to the Potter Communication Center (PCC).
- Cloud connections use HTTPS/TLS

9.4.3 Network Segmentation and Isolation

Supporting documentation instructs that:

- Modbus-Link and BACnet-Link run on dedicated or segmented IP networks (VLAN/VPN recommended).
- Fire alarm networks must not be exposed to public networks or unrestricted corporate LANs.
- Only Potter-documented ports and protocols should be allowed through firewalls.

9.4.4 Configuration and Firmware Integrity

- Automatic cloud backup and restore ensure integrity of panel programs.
- Only validated Potter firmware should be installed on FACPs.
- Gateway devices supervise configuration status and licensing

9.4.5 Physical Protections

- All network cards and gateways must be installed in locked, rated enclosures
- Wiring to NCE-1000/NCF-1000 modules is supervised and must be mechanically protected.
- Optional tamper switches detect enclosure access

9.5 Recommended Installation Mitigations

NFPA-72 (2025) also requires the manufacturer to document security-relevant actions that installers and system owners must perform:

Network Security Requirements

- Use static IP addresses for all panel, server, and integration endpoints.
- Restrict open ports to those documented by Potter
- Block all inbound public network access to fire system component
- Use VLANs, firewalls, or VPNs to isolate fire alarm communication.

Access Control Requirements

- Change all default passwords during installation.
- Limit programming rights to authorized technicians.
- Ensure secure handling and turnover of credentials to the system owner

PC Hardening (PotterNet, BACnet-Link, Modbus-Link, IntelliView-Link)

- Use dedicated Windows 10 or 11 PCs
- Keep antivirus and endpoint protection active
- Control Windows Update behavior to avoid unexpected outages

Physical Security Requirements

- Install all equipment in locked enclosures.
- Protect Ethernet, RS-485, antenna, and P-Link wiring.
- Ensure environmental and physical safeguards for communication equipment.

9.6 Residual Risk Statement

After applying the manufacturer and installer mitigations described here, the residual cyber risk associated with Potter fire alarm systems is assessed as Low to Medium, appropriate for a supervised life-safety system. Potter systems fail safe under loss of communication, incorporate supervised signaling paths, and employ encrypted or isolated communication channels consistent with NFPA-72 expectations. This classification reflects a supervised life-safety system where the primary risks relate to password misuse, physical access, or misconfigured IT environments—all of which can be mitigated through the controls described in this document.

9.7 Ongoing Review & Continuous Improvement

Potter will continue to evaluate cybersecurity considerations as part of product development, software updates, and support processes. Enhancements to encryption, authentication, system monitoring, and resilience will be incorporated into future updates as technologies and industry best practices evolve.

10. Roles and Responsibilities

Roles and Responsibilities Matrix

NFPA-72 requires clearly defined cybersecurity responsibilities across all parties.

Role	*Responsibilities*
Manufacturer (Potter)	Provide secure product design, firmware, software updates, installation guidance, and cybersecurity documentation.
Installer / Integrator	Apply secure configuration, change default credentials, implement network segmentation, configure firewalls, and provide documentation to the owner.
Owner / System Manager	Control physical access, manage user accounts, review credentials periodically, and maintain secure storage of administrative passwords.
IT Department	Provide network segmentation, restrict ports, manage antivirus and OS updates, and ensure isolation of fire systems from enterprise networks.
Monitoring Service	Maintain secure signaling paths, protect receiver infrastructure, and follow authentication requirements for account administration.

11. Secure Product Development

Potter designs, develops, and maintains its fire alarm equipment and software platforms using a controlled and documented product development process that aligns with NFPA-72 (2025) Section 11.2.

Potter's development methodology includes requirements definition, secure design practices, peer review, controlled source-code management, validation testing, and formal release through an Engineering Change Order (ECO) process. Firmware and software are distributed only through authenticated release channels to ensure product integrity.

Potter maintains documented supply-chain controls for critical components, implements change tracking for firmware and software, and evaluates reported cybersecurity issues for remediation. Security-relevant updates are incorporated into product releases and documented for installers and system owners.

These measures fulfill NFPA-72-2025 Section 11.2 requirements for secure product development, software integrity, and vulnerability response.

12. Notification of Termination of Cybersecurity Update Support

Potter provides cybersecurity-related software and firmware updates for supported products as part of its normal product lifecycle. When cybersecurity update support for a covered product is discontinued, Potter will notify the system owner or their designated representative through established communication channels (such as product bulletins, dealer communications, or website notices). This notification is intended to satisfy the NFPA-72 (2025) requirement to inform owners of the termination of cybersecurity update support so they can evaluate any resulting risk and plan appropriate mitigation or system changes

13. Evidence of Compliance

Potter demonstrates compliance with NFPA-72 (2025) cybersecurity requirements through UL 864 certification, encrypted and supervised communication methods, controlled firmware release processes, documented secure installation requirements, authenticated supervisory interfaces, cloud-service security controls, internal development controls, and the publication of this cybersecurity guidance document, which includes a high-level cybersecurity risk assessment.

NFPA-72 (2025) Section 11.11.1 provides three acceptable methods for demonstrating cybersecurity compliance. Potter complies under 11.11.1(2), which allows manufacturers to meet the code by providing documentation that identifies cybersecurity considerations, outlines secure configuration and installation requirements, includes a high-level cybersecurity risk assessment, and demonstrates software and firmware integrity. Potter's established development processes, UL-listed product designs, controlled firmware release procedures, supervised and encrypted communication methods, and the cybersecurity guidance contained in this document collectively fulfill these requirements. Under NFPA-72, this manufacturer-supplied documentation is a fully acceptable evidence path, and a separate third-party cybersecurity certification is not required for compliance.

Potter does not declare SL1, SL2, or SL3 security levels because NFPA-72 does not require fire alarm manufacturers to implement or certify products to those ISA/IEC 62443 levels. Instead, Potter complies using NFPA-72 Section 11.2(4), which allows manufacturers to provide cybersecurity documentation demonstrating a level of security consistent with the standard without needing a formal SL classification. The secure installation requirements, network security guidance, authentication controls, firmware integrity processes, and risk assessment provided in this document satisfy the NFPA-72 cybersecurity requirements for system deployment.