# EATON PRODUCT SECURE CONFIGURATION GUIDELINES

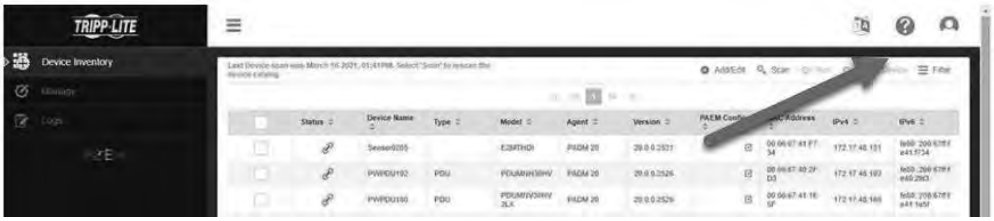
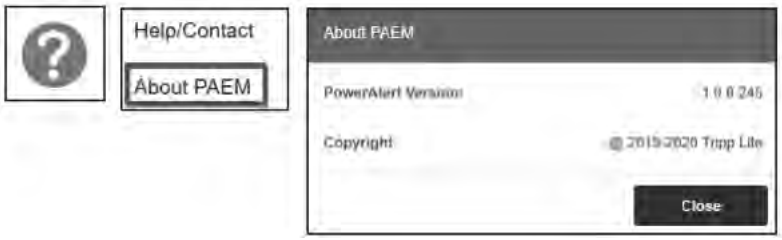
## Documentation to securely deploy and configure Eaton products

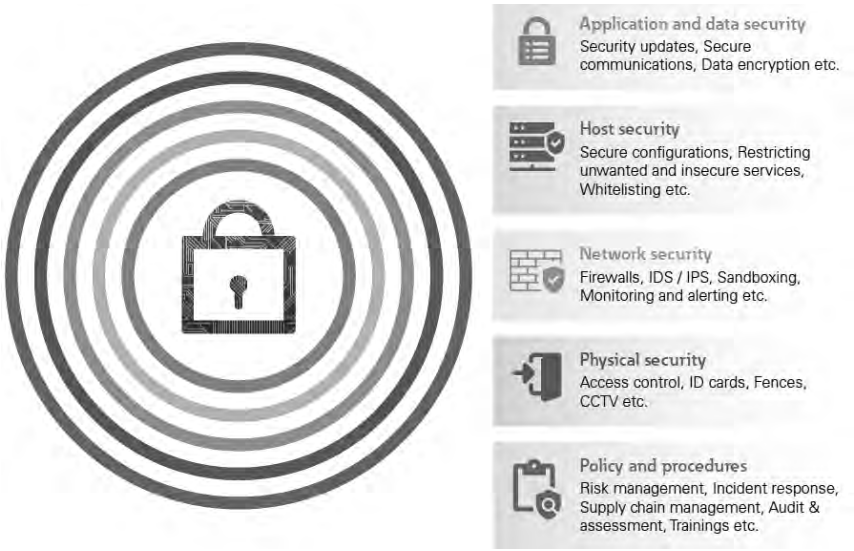
**PowerAlert Element Manager** has been designed with cybersecurity as an important consideration. A number of features are offered in the product to address cybersecurity risks. These Cybersecurity Recommendations provide information to help users to deploy and maintain the product in a manner that minimizes the cybersecurity risks. These Cybersecurity Recommendations are not intended to provide a comprehensive guide to cybersecurity, but rather to complement customers' existing cybersecurity programs.

Eaton is committed to minimizing the cybersecurity risk in its products and deploying cybersecurity best practices in its products and solutions, making them more secure, reliable, competitive for customers.

**INSTRUCTIONS FOR FILLING THIS DOCUMENT –**

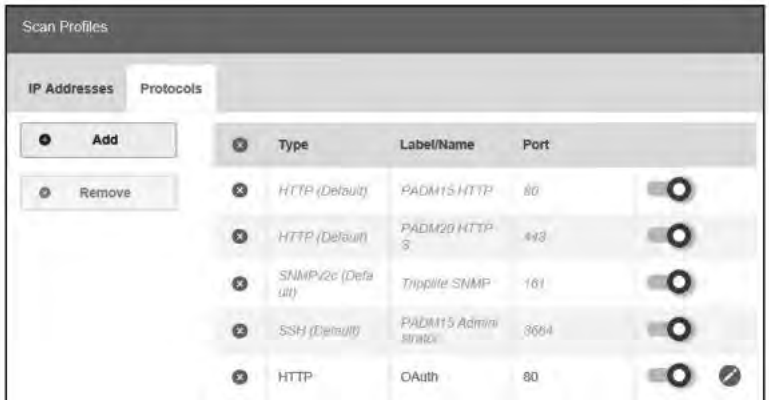
- This document contains a master list of items that need to be part of a secure configuration document for a particular product.
- Please edit the content in RED to make the document product specific.
- Also, you can remove any sections/links/content that may not be applicable to your product.
- Finally this document needs to be part of your product manual that goes to your customers.

| Category | Description |
|---|---|
| **[1] Intended Use & Deployment Context** | PowerAlert Element Manager (PAEM) software consolidates management utilities, simplifying the software-based maintenance of Tripp Lite by Eaton LX Platform devices. PAEM discovers all LX devices on the network, displaying pertinent details in an interactive table from which Mass Configuration and Mass Firmware operations are performed. The outcome of each performed operation can be viewed in a historical log with device-level details.<br><br>PAEM is available as a free download from the Eaton website. Users install the download in a Windows-based computer environment running on the same network as the LX devices which are to be managed. |
| **[2] Asset Management** | Keeping track of software and hardware assets in your environment is a pre-requisite for effectively managing cybersecurity. Eaton recommends that you maintain an asset inventory that uniquely identifies each important component. To facilitate this, **PowerAlert Element Manager** supports the following identifying information:<br><br>Identification information of PAEM - publisher, name and version – can be found by clicking on the question mark icon in the upper right corner of the application user interface, then selecting About PAEM (images below). Additional information can be found in the PAEM Release Notes which are available on the TrippLite/Eaton website at the following URL:<br><br>https://assets.tripplite.com/owners-manual/paem-1-0-3-10-release-notes.txt<br><br>  <br>  |
| **[3] Defense in Depth** | Defense in Depth basically means applying multiple counter-measures for mitigating risks, in a layered or step wise manner. A layered approach to security as shown in the below diagram is what is recommended. Defense in Depth is the responsibility of both the manufacturer and the customer. |

| Category | Description |
|---|---|
| |  <br>Steps Eaton recommends customers take to secure their PAEM deployment include, but are not limited to:<br>• Implement robust network-layer security and access control<br>• Use strong (high- entropy) passwords<br>• Do not share user accounts or passwords<br>• Regularly change passwords (every 90 days or less)<br>• Ensure physical security of the computer environment running PAEM |
| **[4] Risk Assessment** | Eaton recommends conducting a risk assessment to identify and assess reasonably foreseeable internal and external risks to the confidentiality, availability and integrity of the system \| device and its environment. This exercise should be conducted in accordance with applicable technical and regulatory frameworks such as IEC 62443 and NERC-CIP. The risk assessment should be repeated periodically. |
| **[5] Physical Security** | An attacker with unauthorized physical access can cause serious disruption to system/device functionality. Additionally, Industrial Control Protocols don't offer cryptographic protections, making ICS and SCADA communications especially vulnerable to threats to their confidentiality. Physical security is an important layer of defense in such cases. **PowerAlert Element Manager** is designed to be deployed and operated in a physically secure location. Following are some best practices that Eaton recommends to physically secure your system/device:<br>• Secure the facility and equipment rooms or closets with access control mechanisms such as locks, entry card readers, guards, man traps, CCTV, etc. as appropriate.<br>• Restrict physical access to cabinets and/or enclosures containing **PowerAlert Element Manager** and the associated system. Monitor and log the access at all times. |

| Category | Description |
|---|---|
| | • Physical access to the telecommunication lines and network cabling should be restricted to protect against attempts to intercept or sabotage communications. It's a best practice to use metal conduits for the network cabling running between equipment cabinets.<br><br>• **PowerAlert Element Manager** does not contain physical access ports.<br>• Do not connect removable media (e.g., USB devices, SD cards, etc.) for any operation (e.g., firmware upgrade, configuration change, or boot application change) unless the origin of the media is known and trusted.<br>• Before connecting any portable device through a USB port or SD card slot, scan the device for malware and viruses. |
| **[6] COTS Platform Security**<br><br>*<Eaton Internal Note: This section is applicable to products that are meant to run on widely available third-party technology.>* | Eaton recommends that customers harden third-party commercial off-the-shelf (COTS) operating systems or platforms that are used to run Eaton applications / products (e.g., third party hardware, operating systems and hypervisors, such as those made available by Dell, Microsoft, VMware, Cisco, etc.).<br><br>• Eaton recommends that customers refer to the COTS vendor's documentation for guidance on how to harden these components.<br>• Vendor-neutral guidance is made available by the Center for Internet Security https://www.cisecurity.org/<br><br>Irrespective of the platform, customers should consider the following best practices:<br><br>• Install all security updates made available by the COTS manufacturer.<br>• Change default credentials upon first login.<br>• Disable or lock unused built-in accounts.<br>• Limit use of privileged generic accounts (e.g., disable interactive login).<br>• Change default SNMP community strings.<br>• Restrict SNMP access using access control lists.<br>• Disable unneeded ports & services.<br><br>Independent of COTS, PAEM supports the following security features:<br><br>• Ability to enable/disable access protocols for scanning |
| **[7] Account Management**<br><br>*<Eaton Internal Note: This section is applicable to products that support use of one or more accounts to provide logical access to the system or data (e.g., servers, applications, some devices).>* | Logical access to the system \| device should be restricted to legitimate users, who should be assigned only the privileges necessary to complete their job roles/functions. Some of the following best practices may need to be implemented by incorporating them into the organization's written policies:<br><br>• Ensure default credentials are changed upon first login. **PowerAlert Element Manager** should not be deployed in production environments with default credentials, as default credentials are publicly known.<br>• No account sharing – Each user should be provisioned a unique account instead of sharing accounts and passwords. Security monitoring/logging features in the product are designed based on each user having a unique account. Allowing users to share credentials weakens security.<br>• Restrict administrative privileges - Attackers seek to gain control of legitimate credentials, especially those for highly privileged accounts. Administrative privileges should be assigned only to accounts specifically designated for administrative duties and not for regular use. |

<table>
<tr><th>Category</th><th>Description</th></tr>
<tr><td></td><td>
<ul>
<li>Leverage the roles / access privileges to provide tiered access to the users as per the business /operational need. Follow the principle of least privilege (allocate the minimum authority level and access to system resources required for the role).</li>
<li>Perform periodic account maintenance (remove unused accounts).</li>
<li>Ensure password length, complexity and expiration requirements are appropriately set, particularly for all administrative accounts (e.g., minimum 10 characters, mix of upper- and lower-case and special characters, and expire every 90 days, or otherwise in accordance with your organization’s policies).</li>
<li>Enforce session time-out after a period of inactivity.</li>
</ul>
PAEM is accessed using login name “localadmin”. Changing the default password is at the user’s discretion.
</td></tr>
<tr><td>[8] Time Synchronization<br><br><Eaton Internal Note: This section is applicable to products that have a system clock (e.g., servers, some devices).></td><td>Many operations in power grids and IT networks heavily depend on precise timing information.<br><br>Ensure the system clock is synchronized with an authoritative time source (using manual configuration, NTP, SNTP, or IEEE 1588).</td></tr>
<tr><td>[9] Network Security<br><br><Eaton Internal Note: This section is applicable to all products with communications capability.></td><td>
PowerAlert Element Manager supports network communication with other devices in the environment. This capability can present risks if it’s not configured securely. Following are Eaton recommended best practices to help secure the network. Additional information about various network protection strategies is available in Eaton Cybersecurity Considerations for Electrical Distribution Systems [R1].<br><br>
Eaton recommends segmentation of networks into logical enclaves, denying traffic between segments except that which is specifically allowed, and restricting communication to host-to-host paths (for example, using router ACLs and firewall rules). This helps to protect sensitive information and critical services and creates additional barriers in the event of a network perimeter breach. At a minimum, a utility Industrial Control Systems network should be segmented into a three-tiered architecture (as recommended by NIST SP 800-82[R3]) for better security control.<br><br>
Communication Protection: PowerAlert Element Manager provides the option to encrypt its network communications. Please ensure that encryption options are enabled. You can secure the product’s communication capabilities by taking the following steps:<br><br>
When performing PAEM functions, selecting the “Use SSL” checkbox ensures the use of secure protocols.<br><br>
<table>
<tr><th>FUNCTION</th><th>DETAILS</th><th>15.5.x</th><th>20.x.x</th></tr>
<tr><td>Scan</td><td>For HTTP with 20.x.x, select the “Use SSL” checkbox to use HTTPS as the connection method.</td><td>SSH or SNMP</td><td>HTTP or SNMP</td></tr>
<tr><td>Mass Update</td><td>Select the “Use SSL” checkbox to use HTTPS as the connection method.</td><td>HTTP</td><td>HTTP</td></tr>
<tr><td>Mass Configuration</td><td>For 20.x.x, select the “Use SSL” checkbox to use HTTPS as the connection method.</td><td>SSH</td><td>HTTP</td></tr>
</table>
<br>Additionally, non-secure protocols can be disabled.
</td></tr>
</table>

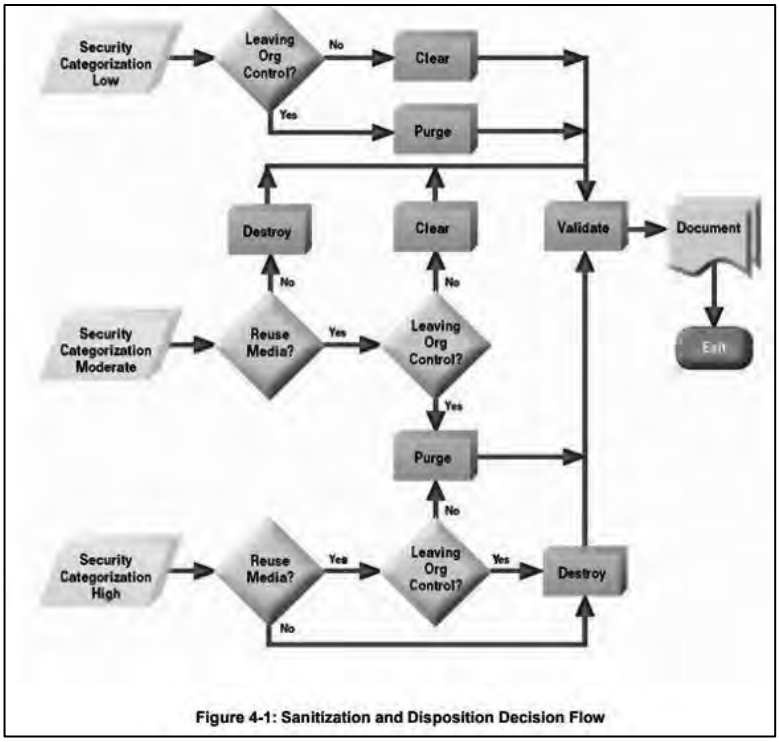
| Category | Description |
|---|---|
| |  <br><br>Eaton recommends opening only those ports that are **required** for operations and protect the network communication using network protection systems like firewalls and intrusion detection systems / intrusion prevention systems. Use the information below to configure your firewall rules to allow access needed for PAEM to operate smoothly<br><br>*<Product Team*<br><br>• *List all ports and services running on the device (sufficient detail for a user to configure an external or host-based firewall)*<br>• *Describe how to configure, enable, and disable protocols and services*<br>• *Describe how to view or obtain a list of ports and services (either via the UI or a console and the netstat command)*<br>• *Provide the details of IP whitelisting for MODBUS/TCP, BACnet and other Industrial protocols [If applicable] >*<br><br>*Note: Many compliance frameworks, and cybersecurity best practices, require an audit of ports and services before and after applying updates and system changes. An end user should be able to refer to the ports and services documentation to determine the required minimum set of ports and services for the product.* |
| **[10] Remote Access**<br><br>*<Eaton Internal Note: This section is applicable to all products that support remote access.>* | Remote access to devices/systems creates another entry point into the network. Strict management and validation of termination of such access is vital for maintaining control over overall ICS security.<br><br>To access PAEM remotely, open a supported web browser. In the address bar, enter the IP address of the server on which PAEM is installed, followed by the configured port, e.g. http://192.168.1.1:8080<br><br>*Describe remote access capabilities and permissions. And also, secure configuration of remote access*<br><br>• *Describe support for multi-factor authentication, use of remote access gateways, IPsec, etc.* |

| Category | Description |
|---|---|
| | • *Reference remote access security recommendations (i.e. securing remote desktop access for Windows, RADIUS and LDAP configuration on the device and server side)*<br>• *List the Session timeouts setting*<br>• *Log the remote sessions and all activities*<br>• *Reference Eaton Cybersecurity Best Practices for description>*<br><br>*<Product Team – Consider whether remote access / remote operation / remote power on or power off capability may present safety issues (e.g., remotely powering on a USP or other electric device may create a risk to a technician who is performing maintenance on it). If so, include a reference / link to the applicable safety information in the product documentation.>* |
| **[11] Logging and Event Management** | • Eaton recommends logging all relevant system and application events, including all administrative and maintenance activities.<br>• Logs should be protected from tampering and other risks to their integrity (for example, by restricting permissions to access and modify logs, transmitting logs to a security information and event management system, etc.).<br>• Ensure that logs are retained for a reasonable and appropriate length of time.<br>• Review the logs regularly. The frequency of review should be reasonable, taking into account the sensitivity and criticality of the system \| device and any data it processes.<br><br>*<Product Team – List the following:*<br><br>• *Any configuration necessary to setup logging or enable verbose logging options, including log target, event types, log sizes, and log persistence.*<br>• *Configuration of external logging sources.*<br>• *Describe what information gets logged (logon, logoff, configuration changes, etc.)*<br>• *How to export the logs.>* |
| **[12] Vulnerability Scanning**<br><br>*<Eaton Internal Note: This section is applicable to all products that support third party software.>* | It is possible to install and use third-party software with **PowerAlert Element Manager**. Any known critical or high severity vulnerabilities on third party component/libraries used to run software /applications should be remediated before putting the device \| system into production.<br><br>• Eaton recommends running a vulnerability scan to identify known vulnerabilities for software used with the product. For COTS components (e.g., applications running on Windows), vulnerabilities can be tracked on the National Vulnerability Database (NVD), available at https://nvd.nist.gov/.<br>• Keep software updated by monitoring security patches made available by COTS vendors and installing them as soon as possible.<br><br>*Note: Many compliance frameworks and security best practices require a monthly vulnerability review. For many non-COTS products vulnerabilities will be communicated directly through the vendor site.* |

| Category | Description |
|---|---|
| **[13] Segmentation & Isolation**<br>*(Vehicle Specific – Remove for Other Sectors)* | Privilege separation with boundary controls is important to improving security of systems. Logical and physical isolation techniques should be used to separate processors, vehicle networks, and external connections as appropriate to limit and control pathways from external threat vectors to cyber-physical features of vehicles. Strong boundary controls, such as strict whitelist-based filtering of message flows between different segments, should be used to secure interfaces. |
| **[14] Critical Safety Communications**<br>*(Vehicle Specific – Remove for Other Sectors)* | Critical safety messages are those that could directly or indirectly impact a safety-critical vehicle control system's operation.<br><br>When possible, sending safety signals as messages on common data buses should be avoided. For example, providing an ECU with dedicated inputs from critical sensors eliminates the common data bus spoofing problem.<br><br>If critical safety information must be passed across a communication bus, this information should reside on communication buses segmented from any vehicle ECUs with external network interfaces. A segmented communications bus may also mitigate the potential effects of interfacing insecure aftermarket devices to vehicle networks.<br><br>Critical safety messages, particularly those passed across non-segmented communication buses, should employ a message authentication scheme to limit the possibility of message spoofing. |
| **[15] Malware Defenses** | Eaton recommends deploying adequate malware defenses to protect the product or the platforms used to run the Eaton product. |
| **[16] Secure Maintenance**<br><br>*<Eaton Internal Note: This section is applicable to all products that incorporate software developed by Eaton.>* | • *<Product Team – Please mention any webpages/methods that exist in the product for troubleshooting/diagnostics purposes. This is important so that such methods are not perceived as potential backdoors*<br><br>The device includes a *<explain the method e.g. tools.html page>* to allow a service engineer with help from site administrator to trouble shoot the device functionality.<br>*This <method/page>allows service engineer to perform following tasks –*<br>• *<List the tasks 1>*<br>• *<List the tasks 2>*<br><br>Note: Enabling of <ports/services> is provided for diagnostic purposes only and shall not be left enabled.<br>*<Mention the intended user of troubleshooting resource>*<br><br>**Best Practices**<br><br>Update device firmware prior to putting the device into production. Thereafter, apply firmware updates and software patches regularly.<br><br>Eaton publishes patches and updates for its products to protect them against vulnerabilities that are discovered. Eaton encourages customers to maintain a consistent process to promptly monitor for and install new firmware updates.<br><br>The latest PAEM version is posted on the TrippLite/Eaton website along with all relevant documentation, including cumulative Release Notes which identify vulnerability fixes. |

| Category | Description |
|---|---|
| | Management Software: PowerAlert Element Manager \| Eaton<br><br>Please check Eaton's cybersecurity website for information bulletins about available firmware and software updates.<br><br>• *<Product Team - Mention the process for acquiring, verifying and updating firmware, updates, patches, and software. Provide the Eaton contact information >*<br><br>Please check Eaton's cybersecurity website for information bulletins about available firmware and software updates. *<Product Website>* |
| **[17] Business Continuity / Cybersecurity Disaster Recovery**<br><br>*<Eaton Internal Note: This section is applicable to all products that are likely to be business critical.>* | **Plan for Business Continuity / Cybersecurity Disaster Recovery**<br>Eaton recommends incorporating **PowerAlert Element Manager** into the organization's business continuity and disaster recovery plans. Organizations should establish a Business Continuity Plan and a Disaster Recovery Plan and should periodically review and, where possible, exercise these plans. As part of the plan, important system \| device data should be backed up and securely stored, including:<br><br>• Updated firmware for **PowerAlert Element Manager**. Make it a part of standard operating procedure to update the backup copy as soon as the latest firmware is updated.<br>• The current configuration.<br>• Documentation of the current permissions / access controls, if not backed up as part of the configuration.<br>• <Product Team – If the product uses a third-party OS that is so customized that it would be advisable to create a full system image, consider addressing that.><br><br>The following section describes the details of failures states and backup functions:<br><br>*<Product Team please provide information as follows:*<br><br>• *Describe failed states*<br>• *Describe communication and power status indicators*<br>• *Configuration of backup and recovery>* |
| **[18] Customer Application Security**<br><br>*<Eaton Internal Note: This section is applicable to products that provide a platform to the customers to run their own applications. Eg: PLCs, HMI etc>* | **PowerAlert Element Manager** provides a platform on which customers can customize and host applications according to their requirements. Security vulnerabilities in these applications may expose the underlying device to attack.<br><br>Eaton recommends observing best practices for secure system development when customers develop and host an application on the device:<br><br>• Privacy and Security by Design: The application should take security and privacy into consideration from the outset, including at the stage of defining requirements and assessing the associated risks. |

| Category | Description |
|---|---|
| | • Communication Protection: If the application communicates over the network, Eaton recommends encrypting the communications in accordance with the applicable level described by the FIPS 140-2 standard.<br>• Access Enforcement: The application should provide the ability to enforce access controls to protect the application against unauthorized access and to protect accounts against unauthorized authentication attempts (for example, through account lockout).<br>• Least Privilege: Any application developed by the customers should not run with root account privileges. The root account has full control over and access to the operating system. Therefore, if an application that requires root privileges has any security vulnerability, it endangers the entire system.<br>• Input Checking: All input to the application should be sanitized before storing and processing by the application to protect against malicious code injection.<br>• Output Handling: Data output by the application for user consumption, including error messages, should be appropriately handled to avoid revealing important information about the application and the underlying system.<br>• Password Management: The application should securely store and transmit credentials (for example, encrypting authentication traffic, and salting and hashing passwords in transit and at rest). Password complexity should be implemented, and password should be masked when entered on-screen.<br>• Secure Coding Practices: Follow secure coding practice while developing applications for the device (for example, implementing multiple security layers, verifying authorization for all requests, conducting code reviews, etc.).<br>• Administration Interface: The interface for administering the application should be separated from the end-user interface.<br>• Session Controls: All application sessions should be encrypted, logged and monitored.<br>• Event Log Generation: The application should have the capability to log security related events at a minimum, including the time, date, and user. |
| **[19] Sensitive Information Disclosure**<br><br>*<Eaton Internal Note: This section is applicable to all product types that are capable of storing data.>* | Eaton recommends that sensitive information (i.e. connectivity, log data, personal information) that may be stored by **PowerAlert Element Manager** be adequately protected through the deployment of organizational security practices.<br><br>*<Product Team – Please list potentially sensitive information.>* |
| **[20] Decommissioning or Zeroization**<br><br>*<Eaton Internal Note: This section is applicable to all product types that are capable of storing data.>* | It is a best practice to purge data before disposing of any device containing data. Guidelines for decommissioning are provided in NIST SP 800-88. Eaton recommends that products containing embedded flash memory be securely destroyed to ensure data is unrecoverable. |

| Category | Description |
|---|---|
| |  <br>Figure 4-1: Sanitization and Disposition Decision Flow<br><br>** Figure and data from NIST SP800-88*<br><br>• **Embedded Flash Memory on Boards and Devices**<br>• Eaton recommends the following methods for disposing of motherboards, peripheral cards such as network adapters, or any other adapter containing non-volatile flash memory.<br><br>• **Clear**: If supported by the device, reset the state to original factory settings. *<Product Team – Please describe the device reset process here.>*<br>• **Purge**: If the flash memory can be easily identified and removed from the board, the flash memory may be destroyed independently of the board that contained the flash memory. Otherwise, the whole board should be destroyed. *<Product Team – Review the device capability and describe the best way to achieve the above recommendation here.>*<br>• **Destroy**: Shred, disintegrate, pulverize, or incinerate by burning the device in a licensed incinerator. |

## References <Remove Not Applicable Ones>

[R1] Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN):
http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf

[R2] Cybersecurity Best Practices Checklist Reminder (WP910003EN):
https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/white-papers/WP910003EN.pdf

[R3] NIST SP 800-82 Rev 2, Guide to Industrial Control Systems (ICS) Security, May 2015:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[R4] National Institute of Technology (NIST) Interagency "Guidelines on Firewalls and Firewall Policy, NIST Special Publication 800-41", October 2009: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

[R5] NIST SP 800-88, Guidelines for Media Sanitization, September 2006:
http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=50819

[R6] A Summary of Cybersecurity Best Practices - Homeland Security
https://www.hsdl.org/?view&did=806518

[R7] Cybersecurity Best Practices for Modern Vehicles - NHTSA
https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf

[R8] Characterization of Potential Security Threats in Modern Automobiles - NHTSA
https://www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2014/812074_Characterization_PotentialThreatsAutos(1).pdf

[R9] Threat Modeling for Automotive Security Analysis
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf