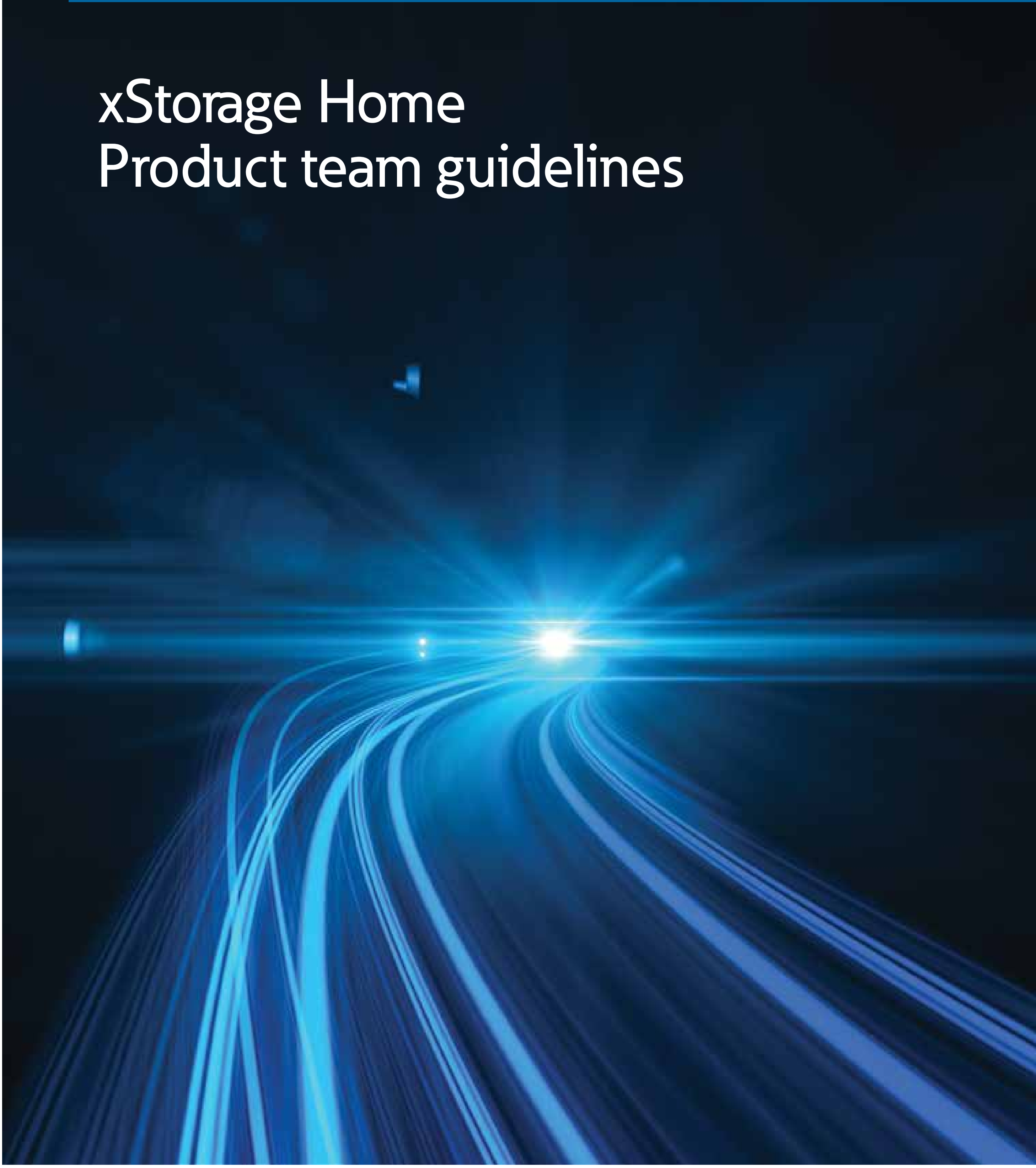
Eaton Cybersecurity Center of Excellence
Cybersecurity recommendations

xStorage Home
Product team guidelines



EATON

Powering Business Worldwide

xStorage Home has been designed with cybersecurity as an important consideration. Several 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 and competitive for customers.

The following Eaton whitepapers are available for more information on general cybersecurity best practices and guidelines:

Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN):

http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf

Cybersecurity Best Practices Checklist Reminder (WP910003EN):

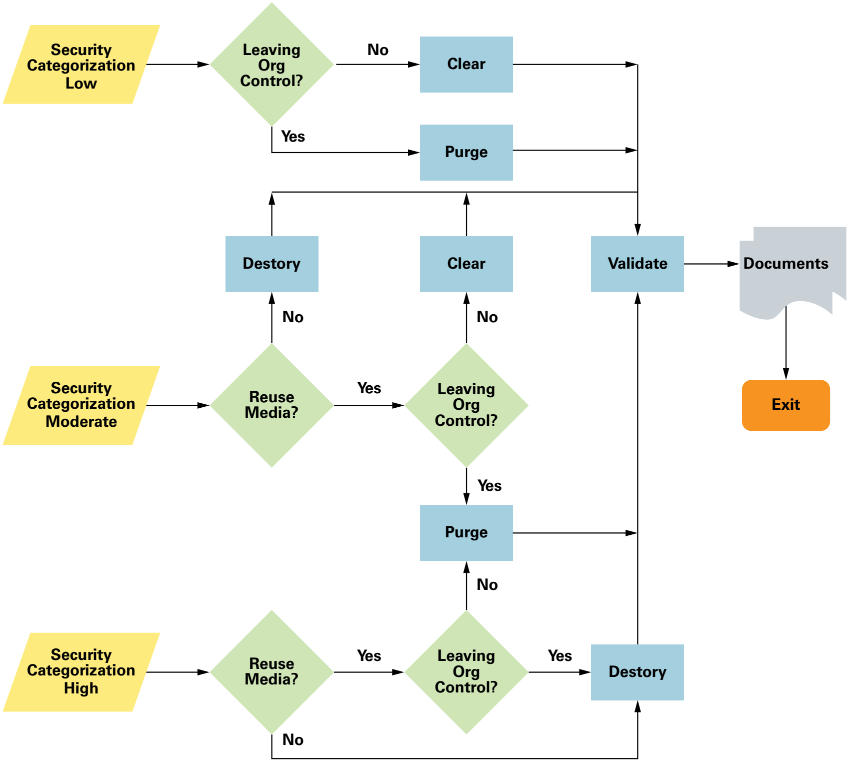
http://www.cooperindustries.com/content/dam/public/powersystems/resources/library/1100_EAS/WP910003EN.pdf

Category	Description
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, xStorage Home supports the following identifying information: Hardware information such as manufacturer, model, serial number, firmware versions and location of the unit can be found visiting the xStorage Home website, the unit settings page, after installing, configuring and connecting the unit. Additionally, in the same unit settings page you will be able to retrieve the version name and version date of all unit components. Manufacturing, model and serial number are also part of the packaging labeling.
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. The Eaton cybersecurity assessment will be repeated periodically or on demand after each major software/hardware release.
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 Industrial Control System (ICS) and Supervisory Control and Data Acquisition (SCADA) communications especially vulnerable to threats to their confidentiality. Physical security is an important layer of defense in such cases. xStorage Home 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: • 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. • 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. • xStorage Home supports the following physical access ports: ◦ Ethernet RJ-47 used for TCP IP connection to the communication card. ◦ USB used for supported Wi-Fi dongle only. ◦ USB Type B used for inverter debugging and local firmware update. ◦ RS485 Pins for Power Meters (Modbus). • Access to these ports should be restricted.
Commercial off-the-shelf (COTS) Platform Security	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.). • Eaton recommends that customers refer to the COTS vendor's documentation for guidance on how to harden these components. • Vendor-neutral guidance is made available by the Center for Internet Security https://www.cisecurity.org/ Irrespective of the platform, customers should consider the following best practices: • Install all security updates made available by the COTS manufacturer. • Change default credentials upon first login. • Disable or lock unused built-in accounts. • Limit use of privileged generic accounts (e.g. disable interactive login). • Disable unneeded ports and services. • Use modern browser like Chrome, or Firefox.

<table>
<tr><th>Category</th><th>Description</th></tr>
<tr><td>Account Management</td><td>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:
• Ensure default credentials are changed upon first login. xStorage Home should not be deployed in production environments with default credentials, as default credentials are publicly known.
• 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.
• 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.
• 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).
• Up to 10 users can access a specific unit.
• A total of 4 different user roles can be used to monitor and/or control each unit.
  ◦ The least privilege role is the "viewer" giving the possibility to only monitor the unit;
  ◦ The "configure" role adds the possibility to change the unit operation mode;
  ◦ The "access management" role adds the possibility to invite/revoke other users to access the unit;
  ◦ The "owner" can change all unit settings.
• Perform periodic account maintenance (remove unused accounts).
• 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).
• Enforce session time-out after a period of inactivity.
• Unit owner and access management role users can invite/revoke other users to access the unit. This can be done at any time directly from the website.
• Password complexity is the following: 8-16 characters, containing 3 out of 4 of the following: Lowercase characters, uppercase characters, digits (0-9), and one or more of the following symbols: @ # $ % ^ &amp; * - _ + = [ ] { } | \ : ' , ? / ` ~ " ( ) .
• Account lockout after 6 wrong login attempts.
• Account timeout after 1 hour.</td></tr>
<tr><td>Time Synchronization</td><td>Many operations in power grids and IT networks heavily depend on precise timing information.
• Ensure the system clock is synchronized with an authoritative time source (using manual configuration, NTP, SNTP, or IEEE 1588).
• Setting the time of the unit is indeed an important step, as this will impact measurements visualization and features directly impacted by weather forecast. To protect a misconfiguration of the system the communication card software will verify that the location of the unit and the selected time zone are compatible. The installer and/or owner of the unit can specify the system clock in the local website used for setup and onboarding of the unit to the Cloud. By default, the system will use an automatic date and time server from the internet, but if desired the user can select to manually set the date and time.</td></tr>
</table>

Category	Description
Network Security	xStorage Home 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]. 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. Communication Protection: xStorage Home 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: By default, only HTTPS communications are enabled. Any HTTP traffic will be redirected to HTTPS servers. 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 xStorage Home to operate smoothly. The user can get the communication card configured networks in the unit settings page, General Settings. Section Network interface eth0 will list the IP and Mac of the Ethernet interface. Section Network interface wlan0 will list the IP and Mac of the Wifi dongle. Home router will need to keep the standard HTTPS port open (443) to allow the user to connect to the cloud or local website. Furthermore, the port 3333 will need to be open to allow the gRPC Remote Procedure Call communication between device and cloud servers. Default static IP and failover IP of the communication card is set to be 192.168.2.254. The reset button should reset that IP if user loses communication after playing with the configurations (DHCP, static, Wi-Fi). grpc.xstoragehome.com needs to be whitelisted as this is the server endpoints for the Cloud connectivity.
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. Client has the choice to use the local web server to monitor and control his unit, or to connect it to xStorage Home cloud servers. The web portal provided in both cases are very similar in terms of core features. Cloud Portal provides extra features such as more historical data, user management roles and weather forecast. Network configuration, Date and Time Server and Topology can only be modified by the installer and/or owner using the local web portal. The cloud web portal is available at https://xstoragehome.com and anyone can create a free account. In order to have access to a unit that user needs to own one or to be invited to an existing connected unit. All unit operation modes updates are listed, and the user can visualize who triggered the change.
Logging and Event Management	• Eaton recommends logging all relevant system and application events, including all administrative and maintenance activities. • 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.). • Ensure that logs are retained for a reasonable and appropriate length of time. • Review the logs regularly. The frequency of review should be reasonable, considering the sensitivity and criticality of the system | device and any data it processes. • The system provides different type of logs. On the communication card, under /var/log/controller the software will log all the important activities of the communication between the client and the system and between the communication card and the other system components, like inverter and power meters. On the cloud side, Microsoft azure logs will provide relevant statistics about the usage of any of the IT resources. API's, virtual machines, databases, etc. • Login, logouts and all relevant authentication details are logged in Microsoft Azure Active Directory. Authentication in the local website is also logged into the communication card logs. (Syslogs) • Logs can be exported using the local API. In the future we will be able to also export them using the Cloud Portal. • Logs are automatic and are enabled by default.

Category	Description
Vulnerability Scanning	It is possible to install and use third-party software with xStorage Home. 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. • 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/. • Keep software updated by monitoring security patches made available by COTS vendors and installing them as soon as possible. **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.
Malware Defenses	Eaton recommends deploying adequate malware defenses to protect the product or the platforms used to run the Eaton product.
Secure Maintenance	**Best Practices** Update device firmware prior to putting the device into production. Thereafter, apply firmware updates and software patches regularly. 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. Frequently the system will receive updates totally free of charge for the client and recommended in order to keep the unit working properly, safely and to provide new features. The updates can be easily accepted and installed using the Cloud User Interface. The update bundle will provide the new software for the communication card, inverter firmware and BMS firmware. If the client is not connected to the cloud, he can still keep his system updated downloading the latest software from the Eaton official website and using the local web portal to upload the file and trigger the update. Please check Eaton's website for information bulletins about available firmware and software updates. http://www.eaton.com/gb/en-gb/catalog/energy-storage/xstorage-home.resources.html
Business Continuity / Cybersecurity Disaster Recovery	**Plan for business continuity / cybersecurity disaster recovery** Eaton recommends incorporating xStorage Home 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: • Updated firmware for xStorage Home. Make it a part of standard operating procedure to update the backup copy as soon as the latest firmware is updated; • The current configuration; • Documentation of the current permissions / access controls, if not backed up as part of the configuration; The following section describes the details of failures states and backup functions: • In the event of a grid failure the system will go automatically into backup mode. Your critical loads will still be supplied by the unit as long as the battery has some energy. • In case of a network connectivity issue (no internet) the system will try to reconnect and establish the connection as soon as the internet connectivity is restored. If more than one day passes without internet the system will work in "offline" mode using the local UI. Later the client can visit the local UI setup page and reconnect it again to the cloud. • A section with system alarms is under development. The user will receive different types of notifications with different types of severity. The document Error codes provides you a complete list of all possible system errors with detailed description and diagnosis together with a list of action for troubleshooting. • The hard-reset button in the communication card provides a way to restore the card to the factory configuration. • There is a section for support in the unit settings page.

Category	Description
Sensitive Information Disclosure	Eaton recommends that sensitive information (i.e. connectivity, log data, personal information) that may be stored by xStorage Home be adequately protected through the deployment of organizational security practices. xStorage Home Cloud and Local UI only uses the minimum information needed to support the core functionalities of the system. In terms of personally identifiable information (PII) for the cloud connectivity and account creation we require a valid email and a first and last name for better UX and texting. We do not require the complete address of the unit, despite that we use the city location in order to provide accurate weather forecast and time zone features.
Decommissioning or Zeroisation	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.  Security Categorization Low Leaving Org Control? No Clear Yes Purge Destory Clear Validate Documents No No Exit Security Categorization Moderate Reuse Media? Yes Leaving Org Control? Yes Purge No Security Categorization High Reuse Media? Yes Leaving Org Control? Yes Destory No **Sanitization and disposition decision flow** • **Embedded flash memory on boards and devices** Eaton recommends the following methods for disposing of motherboards, peripheral cards such as network adapters, or any other adapter containing non-volatile flash memory: - **Clear:** If supported by the device, reset the state to original factory settings. - Using the small red button in the front panel of card (labeled Default), press and hold for 10 seconds to be able to reset the card to the factory configuration. - **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. - The whole board should be destroyed or flashed. - **Destroy:** Shred, disintegrate, pulverize, or incinerate by burning the device in a licensed incinerator.

References

[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):

http://www.cooperindustries.com/content/dam/public/powersystems/resources/library/1100_EAS/WP910003EN.pdf

[R3] NIST SP 800-82 Rev 2, Guide to Industrial Control Systems (ICS) Security, May 2015:

https://ics-cert.us-cert.gov/Standards-and-References

[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

Powering Business Worldwide

Eaton
EMEA Headquarters
Route de la Longeraie 7
1110 Morges, Switzerland
Eaton.com

Publication No. MZ700001EN
March 2019

Follow us on social media to get the
latest product and support information.