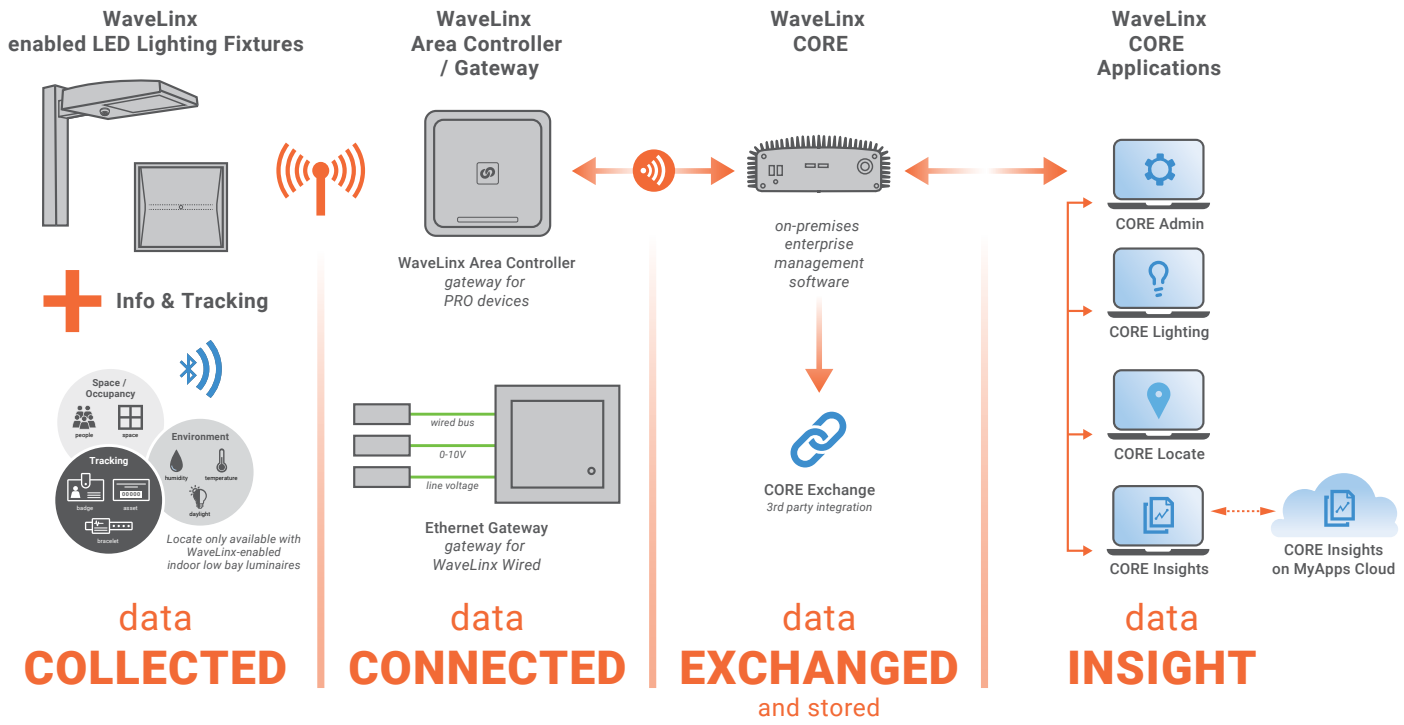
Product Team Guidelines

WaveLinx CORE 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.

In these environments the CORE appliance is assumed to be deployed on the building automation network or lighting automation network behind a firewall or other boundary device supporting similar features including traffic filtering and Denial of Service (DoS) protections. The network would therefore be firewalled from the business network and the world wide web.

It is also assumed that the CORE appliance will be installed in environments with physical access controls limiting physical access to local interfaces (e.g. USB and serial interfaces).



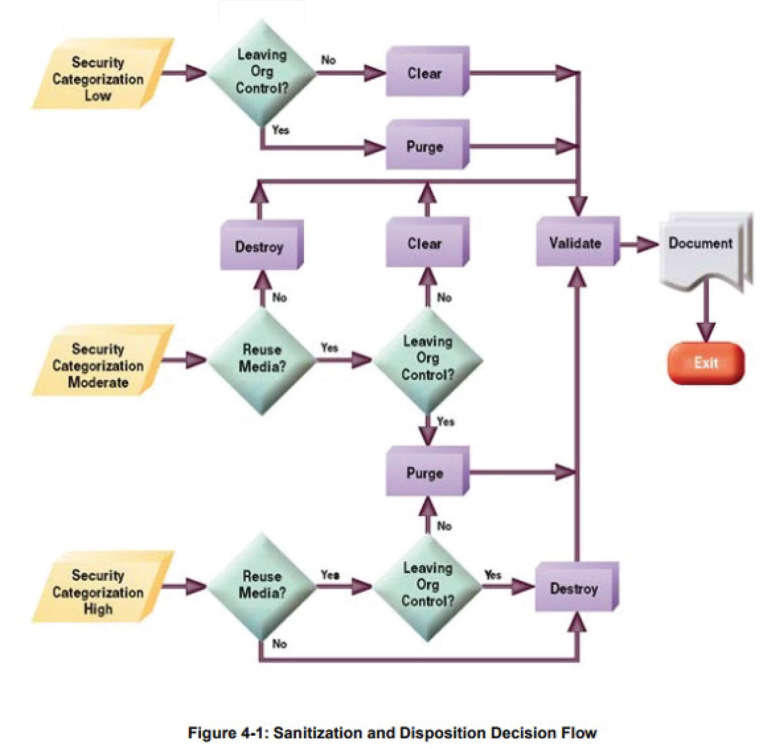
Cooper Lighting Solutions products in general are developed with cybersecurity as an important consideration. Cybersecurity features are designed which if implemented as recommended would minimize Cybersecurity risk to this product. This section “secure configuration” or “hardening” guidelines provides information to the users to securely deploy and maintain their product to adequately minimize the cybersecurity risks to their system.

Cooper Lighting Solutions 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.

Category	Description
Asset Management	Keeping track of software and hardware assets in your environment is a pre-requisite for effectively managing cyber-security. Cooper Lighting Solutions recommends that you maintain an asset inventory that uniquely identifies each important component. To facilitate this, WaveLinx CORE supports the following identifying information: WaveLinx CORE - manufacturer, type, serial number. This information is indicated on the label placed on the appliance. CORE - publisher, name, version. This information is available in the About section of the application.
Risk Assessment	Cooper Lighting Solutions 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.
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. WaveLinx CORE is designed to be deployed and operated in a physically secure location. Following are some best practices that Cooper Lighting Solutions 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. • Restrict physical access to cabinets and/or enclosures containing WaveLinx CORE and the associated system. Monitor and log the access at all times. • 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. • WaveLinx CORE Pro supports the following physical access ports: RJ-45, USB and HDMI. The monitor and keyboard are only used to access the Command Line Interface (CLI) for Tier 2/3 troubleshooting (refer to section 7.1 of the WaveLinx CORE User Manual) for more information with regards to tasks that can be completed via the CLI. • WaveLinx CORE access to local ports including the USB and HDMI lines are assumed to be restricted by a combination of controlled physical access to the site and control room at a customer site. • Do not connect removable media (e.g., USB devices,) for any operation (e.g., firmware upgrade, configuration change, or boot application change) unless the origin of the media is known and trusted. • The WaveLinx CORE Pro is designed to be mounted in an equipment rack inside the electrical or server room. In the target markets, i.e. commercial buildings, Cooper Lighting Solutions assumes the physical environment will be secured to limit remote access.

Category	Description
Account Management	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. CORE 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 CORE Admin's roles / access privileges, i.e. System Administrator, IT Administrator, Facility Manager, Tenant and Viewer 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). • Perform periodic account maintenance (remove unused accounts). • CORE enforces passwords between 8 and 16 characters without spaces. As part of the complexity requirements, the password must contain at least 1 number, 1 special character (+ & % are not allowed), and 1 upper-case letter. The expiration period can be configured to meet your organization's policies. • CORE enforces session time-out after a period of inactivity.
Time Synchronization	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). CORE supports NTP. In an isolated network, WaveLinx CORE can act as a client and/or server based on the application. In an isolated network WaveLinx CORE will act as the NTP server for the networked WaveLinx Area Controller. In a network with access to an external NTP server, WaveLinx CORE will be a client to the external NTP and if necessary, can be a server to the networked WaveLinx Area Controller.
Network Security	CORE supports network communication with other devices in the environment. This capability can present risks if it's not configured securely. Following are Cooper Lighting Solutions recommended best practices to help secure the network. Cooper Lighting Solutions 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 Building Automation Systems network should be segmented into a three-tiered architecture (as recommended by NIST SP 800-82[R1]) for better security control. Communication Protection: CORE uses HTTPS and TLS/SSL to securely allow communication between the WaveLinx CORE and associated WaveLinx Area Controllers and CORE and web clients used to access the WaveLinx CORE applications. Cooper Lighting Solutions 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. Please refer to Section 6.3 in the WaveLinx System Network/IT Planning Guide to learn about the ports being used by the WaveLinx CORE and associated Wireless Area Controllers and to configure your firewall rules to allow access needed for WaveLinx CORE to operate smoothly. Cooper Lighting Solutions has disabled non-critical ports by default. These ports can be found in the "Network Ports and Usage" section in the WaveLinx Network and IT Planning Guide enabled for troubleshooting purposes by an Admin user from WaveLinx CORE's Firewall management page.
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. There are no VPN service running on WaveLinx CORE. To allow remote connectivity, the system administrator will need to provide remote network access to the remote user. The WaveLinx CORE system offers SSH service for troubleshooting purposes. The SSH service is disabled by default. To allow SSH access for troubleshooting purposes, the system admin needs to enable the SSH service using the WaveLinx CORE Admin app. The system administrator shall disable the service once the troubleshooting session has completed.

Category	Description
Logging and Event Management	• Cooper Lighting Solutions 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, taking into account the sensitivity and criticality of the system | device and any data it processes. • System and application events such as import devices, database synchronization between WaveLinx CORE and Wireless Area Controllers are logged and viewable from the WaveLinx CORE Events console/web page. Application logs are maintained for each WaveLinx CORE micro service and operating system. The log files can be downloaded from the WaveLinx CORE application.
Vulnerability Scanning	• It is possible to install and use third-party software with WaveLinx CORE. 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. • Cooper Lighting Solutions recommends running a vulnerability scan to identify known vulnerabilities for software used with the product. Users can refer to the National Vulnerability Database (NVD), available at https://nvd.nist.gov/ for the latest vulnerabilities. • Keep software updated by monitoring security patches made available by Cooper Lighting Solutions 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.*
Secure Maintenance/patch Management	**Best Practices** Update device firmware prior to putting the device into production. Thereafter, apply firmware updates and software patches regularly. Cooper Lighting Solutions publishes patches and updates for its products to protect them against vulnerabilities that are discovered. Cooper Lighting Solutions encourages customers to maintain a consistent process to promptly monitor for and install new firmware updates. Register to Cooper Lighting Solution's website to get real-time notifications and to download latest firmware and software for your system.
Business Continuity / Cybersecurity Disaster Recovery	**Plan for Business Continuity / Cybersecurity Disaster Recovery** Cooper Lighting Solutions recommends incorporating WaveLinx CORE 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: • Backup the WaveLinx CORE system. User has the option to backup configuration and time series/log data. Make it a part of standard operating procedure to update the backup copy prior to the latest firmware application. • Documentation of the current permissions / access controls, if not backed up as part of the configuration. As WaveLinx CORE is a read-only system for most of the components, the application will go back to a known state on reboot.
Customer Application Security	WaveLinx CORE is private platform, i.e. customers cannot host any third-party applications.
Sensitive Information Disclosure	Cooper Lighting Solutions recommends that sensitive information (i.e. connectivity, log data, personal information) that may be stored by WaveLinx CORE be adequately protected through the deployment of organizational security practices. WaveLinx CORE stores the following information: 1. Energy usage of building(s) being managed by WaveLinx CORE 2. Occupancy usage of building(s) being managed by WaveLinx CORE 3. Lighting system configuration of building(s) being managed by WaveLinx CORE 4. Log files 5. Personal information (last name, first name, optionally email and phone information) of individuals given access to the WaveLinx CORE applications.

Category	Description
Decommissioning or Zeroization	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. Cooper Lighting Solutions recommends that products containing embedded flash memory be securely destroyed to ensure data is unrecoverable. WaveLinx CORE has the option to reset the system to default factory. This would result in removing all system configuration data.  **Figure 4-1: Sanitization and Disposition Decision Flow** ** Figure and data from NIST SP800-88* • **Embedded Flash Memory on Boards and Devices** • Cooper Lighting Solutions recommends the following methods for disposing of motherboards, peripheral cards such as network adapters, or any other adapter containing non-volatile flash memory. • **Clear:** Reset WaveLinx CORE to original factory settings via the WaveLinx CORE Admin System>Factory Reset option. • **Purge:** Destroy the WaveLinx CORE board. • **Destroy:** Shred, disintegrate, pulverize, or Incinerate by burning the device in a licensed incinerator.

References

[R1] NIST SP 800-82 Rev 2, Guide to Industrial Control Systems (ICS) Security, May 2015:
https://ics-cert.us-cert.gov/Standards-and-References

[R2] 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

[R3] NIST SP 800-88, Guidelines for Media Sanitization, September 2006:
http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=50819

Cooper Lighting Solutions
1121 Highway 74 South
Peachtree City, GA 30269
P: 770-486-4800
www.cooperlighting.com
For service or technical assistance:
1-800-553-3879

Canada Sales
5925 McLaughlin Road
Mississauga, Ontario L5R 1B8
P: 905-501-3000
F: 905-501-3172