Recommended Cybersecurity Best Practice

Watlow Is Focused on Cybersecurity

Watlow has incorporated cybersecurity best practices and solutions in our products. Our security by design approach makes our products more resilient against cyberattacks with implemented mechanisms to mitigate threats, reduce exploitable weaknesses and defend against avoidable data breaches and cyberattacks.

Recommended Cybersecurity Best Practices

To help keep your Watlow products secure and protected, we recommend that you implement these cybersecurity best practices. Following these recommendations may significantly help reduce your company's cybersecurity risk:

Implement Strong Authentication Controls (Do this now!)

Change default passwords when new software is installed, particularly for administrator accounts and control system devices, and regularly after that. Using role-based access with multi-factor authentication helps prevent security breaches and provides a log of access activity. Consider adding password security features, for example, an account lockout that activates when too many incorrect passwords are entered.

Set Up Firewalls

Always place Watlow systems and devices behind firewalls and other security protection appliances that limit access to only authorized remote connections. Building a highly protected network that helps prevent outside access is the most critical line of defense against cyberattacks. We recommend that you follow these steps:

- Limit access to the networks on which Watlow devices are placed.
- Ensure that Watlow systems and devices are not accessible from the internet.
- Restrict external network connectivity to your systems and devices.
- Continually monitor for events that could warn of attempted unauthorized access.
- Limit access to internal networks where devices reside.
- Isolate control and safety system networks and remote devices from the business network.

HA033524/2

Manage Patches and Updates

Most vendors work diligently to develop patches for identified vulnerabilities. Even after patches and updates are released, many systems remain vulnerable because organizations are either unaware of or choose not to implement these fixes. Effective patching can stop a large number of attacks, so implement a monitoring system to be sure you always apply the latest patches and updates for operating systems, anti-virus tools and any other software.

Be Aware of Vulnerabilities

Watlow analyzes and evaluates software components and binaries in its products to help identify and track vulnerabilities. We also monitor publicly available vulnerability advisories from recognized industry and government sources. Applying updates and patches is encouraged for any Internet-connected device to address known vulnerabilities.

Implement Secure Access Controls

Laptops that have connected to other networks should never be allowed to connect to the safety or control network without proper sanitation. Also, all methods of data exchange, such as CDs or USB drives, should be scanned before use in any node connected to the network. You may also want to split your networks and devices into groups isolated from one another and restrict access. Reducing the pathways into and within your networks and implementing security protocols on the pathways that exist makes it more difficult for a threat to enter your system and gain access to other areas.

Use Secure Remote Access Methods

Implement secure methods for remote users to access your network. Require all remote users to connect and authenticate through a single, managed interface before conducting software upgrades, maintenance, and other system support activities.

Maintain Current Backups and Test your Recovery Procedures

Backups are the most effective way to recover from a malware attack. In addition to backing up critical systems and data frequently, it is important to test your recovery procedures. Ensure you have multiple backups over time, so you can restore from a version that predates any infection.

Set up Measures for Detecting Compromises

Minimize the risk of compromise by monitoring and auditing system events 24/7. Use intrusion detection systems (IDSs), intrusion prevention systems (IPSs), anti-virus software, and usage logs to help you detect compromises in their earliest stages. Despite implementing these preventive measures, you may still experience compromises. Have a plan in place to quickly detect the issue and respond.

Install Physical Controls to Help Prevent Unauthorized Access

While this isn't just a cybersecurity issue, it's important to put physical controls in place so that no unauthorized person can access your equipment. Keep all controllers in locked cabinets and limit access to any connected devices.

Check the Documentation for Product-specific Information

Watlow provides detailed information with every product. Review the product guides for cybersecurity recommendations and best practices directly related to your Watlow products.

Train your people

Provide cybersecurity training to your employees to help keep your organization secure. Explain phishing emails, infected attachments, malicious websites, and other methods that attack them directly.

For more information and assistance

For guidance on maintaining Watlow products, please contact Watlow Technical Support or refer to the cybersecurity guidelines available in the user assistance.

For additional information on cybersecurity best practices, review these resources.

Document Name	Source	Web Address Link
The Cybersecurity Framework	National Institute of Standards and Technology (NIST)	https://www.nist.gov/cyberframework/framework
Cybersecurity Best Practices	Center for Internet Security	https://www.cisecurity.org/cybersecurity-best-practices/
IEC 62443 Security for Industrial Automation and Control Systems	International Society of Automation (ISA)	https://isasecure.org/en-US/

Note - This document is intended to help provide general security recommendations and is provided on an 'as is' basis without warranty of any kind. Watlow disclaims all warranties, either express or implied, including warranties of merchantability or fitness for a particular purpose. In no event shall Watlow, or its subsidiaries, be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Watlow, or its subsidiaries, has been advised of the possibility of such damages. The use of this document, information contained herein, or materials linked to it are at your own risk. Watlow reserves the right to update or change this document at any time and in its sole discretion.