

# Ewon & NIS2

Tips and Tricks



# NIS2 compliance secured through ISO 27001 Certification





# NIS2



NIS2 is still being regulated by each EU member state, but the guidelines are already in place.

## What is NIS2?

NIS2 is an **EU-wide directive** that **strengthens cybersecurity** for critical and important sectors like energy, healthcare, and digital infrastructure.

It calls for **stricter requirements** and **improved cooperation** among member states.

The aim is to **improve resilience** to cyber threats across the EU.



Be prepared so that incidents don't catch you by surprise.

## Ewon by HMS Networks: your key partner for NIS2

Partnerships require that the mechanisms put in place are used correctly.

Here's a breakdown of the NIS2 security standards, along with some **tips and tricks to help you achieve the highest level of protection.**

# Network Security and Encryption

**Secure data connections:** ensure all data connections are fully encrypted.

**Centralized access control:** manage access rights, ensuring only authorized users have access at the appropriate times.



Stay updated with Ecatcher patches for the latest security methods.

# Network Security and Encryption

Control access with **multi-factor authentication**.

Maintain **connection audit trails** to **monitor** system usage.



Multi-factor authentication is a must and makes it easy to add an extra layer of protection.



# Network Security and Encryption

To ensure the highest level of protection,  
refer to our best practice guide.



Control access rights by using a  
physical switch or key on machine.

# Incident Reporting Obligations

NIS2-covered entities must **report significant service-impacting incidents** and **take action to mitigate consequences**.

Timeline:

- **Report incidents within 24 hours**
- **Submit follow-up reports within 72 hours** with detailed information and action plans



Advices:

- Subscribe to alerts for incidents updates
- Regularly install security updates to stay resilient





ISO 27001



ISO 27001 is the foundation for Ewon's security practices, including NIS2 requirements.

## Certifications and Standards

To address the varied regulations across EU countries, **NIS2 promotes the adoption of standardized certifications.**















# Cybersecurity is an ongoing process

As the world evolves, so do the threats.





















Systems must continuously adapt to new challenges.

True security is a collective effort—there is no such thing as a completely secure system without ongoing vigilance and collaboration.

# NIS2 Conformance Table

NIS2 Requirements					
	Response Plans / Disaster Recovery	Supply Chain Security	Encryption/ Data Security	Incident Reporting / Plans	Certifications
Cosy Series					ISO27001
Flexy Series					ISO27001
Talk2m					ISO27001

# NIS2 Technical Recommendations for Remote Access

 Apply controls/policies for Remote Access	 Explicitly forbid or deactivate unneeded connections and services	 Network Security
 Segment systems into networks or zones	 Allow connections of service providers only after an authorization request and for a set time period	 Access Control
 Establish communication between systems only through trusted channels that are not isolated from other communication channels	 Provide identification of the end points and protection of the channel data from modification	 Incident Handling
 Establish policies for management of privileged accounts	 Terminate inactive sessions after pre-defined period of inactivity	 Patch Management
 Implement authentication procedures based on least privilege principle	 Separate credentials to access privileged access or administrative accounts	
 Strength of authentication appropriate to the asset to be accessed	 Regularly review the identities and if no longer needed deactivate	
 Change of authentication credentials initially	 Use multi-factor authentication	
 Use tools to monitor and log activities on the remote access to detect events that could be considered as incidents	 Specify and apply procedures for ensuring that security patches are applied within a reasonable time	



Stay Connected!  
[www.hms-networks.com](http://www.hms-networks.com)

Hardware Meets Software™