hagergroup

Version 1.0

Cybersecurity technical and organizational measures for connected products and services.

The Hager Group pays special attention to safeguard the data and connection for its digital products and services. We utilize a large framework of state of the art technical and organizational measures to achieve a secure processing of your data and provide **security**, **privacy** and **protection** of your data guided by a global IT security policy.

What is "Security of Processing" about?

It is about analyzing the risks of a data processing activity and protecting the data accordingly by implementing state of the art technical and organizational measures that are regularly reviewed, adjusted and updated. Those measures ensure the confidentiality and integrity of the data as well as the availability and resilience of the systems and service, in order to effectively protect the data against destruction, loss, modification, unauthorized disclosure and unauthorized access.

HAGER approaches the task of securing its products and services through the following activities:

- **Network security:** is a practice of securing a computer network from intruders
- **Application security:** focuses on keeping software and devices free of threats. Applications contains data, as a consequences to be often targeted
- **Information security:** protects integrity and privacy of data
- **Operational security:** includes the processes and decisions for handling and protecting data assets

What measures does HAGER take?

Here is a selection of measures that apply to each product and service:

- **Perform a risk assessment** to define appropriate technical and organizational measures. This action is customer centric: it takes into account the data sensitivity, legal requirements, and business concerns
- **Define the appropriate technical and organizational measures** for the connected products and services based on strong recognized industry standards.
- **Maintain the products and services** in optimal security condition during the lifecycle of the offers with the right assurance level.
- **Provide awareness and training** of risks among all our employees and ensure that they have the necessary knowledge, skills, experience and technological capabilities

How do we address these measures?

The measures are embedded in our development cycle for connected IP products and services (Secure Development Lifecycle) with the following basic principles: security "by design" and "by default":

- **by design:** this means that HAGER implements technical and organizational measures from the earliest to the final stages of the development of the product to enhance the security efficiency,
- **by default:** this means that a product out of the box is configured with the appropriate level of privacy and security. Furthermore, HAGER provides guidance to maximize security when using the product.

How do we implement the Secure Development Lifecycle?

HAGER's IT Security is inspired by the IEC-62443 standards family which defines how to enforce IT Security for Industrial Automation and Control Systems (IACS). It also applies to smart-building and energy management systems.

HAGER implements defense in depth. This means that we use several independent methods to defend the system against possible threats. Among the wide variety of security measures implemented by HAGER, we would like to emphasize the foundational ones:

- **Encryption:** we value your interest of your private data staying private. We use the state of the art implementation of the strongest encryption algorithms to protect your personal information at rest or in transit from your device up to our Cloud.
- **Authentication, Authorization, Auditing:** we limit access to data on a "need to know" basis. We enable Multi-Factor Authentication (MFA), least privilege authorization and strong access control in particular for administrators.
- **Trusted partners:** Our cloud approach based on Microsoft Azure strategy ensures a high level of resilience and protection.
- **Security assessment:** Penetration test done by a third party (ethical hackers) and other security audits, challenge the actual level of security provided by our solutions.
- **User Guidance:** HAGER provides IT Security guidance to use its product properly. We help customer to integrate our products into their network in a complete secure way. Recommendations are about LAN security, physical security and secure usage of products with best practices.

How do we secure Operations?

HAGER provides an appropriate level of security and resilience to its product to ensure operational performance over time:

- Security updates over the cloud services are offering a fast and efficient patch management mechanism for IoT endpoints
- Vulnerability management for the centralized cloud based services
- Continuous monitoring of the systems to prevent or react quickly on unexpected events
- An IT Security incident management is offered over a professional support in case of data breach over each market segment organization (Privileged Customer Touchpoint).