SICK CYBER SECURITY - REQUIREMENTS FOR SUPPLIERS

Introduction

It is a vital goal of SICK to offer high quality products and services to its customers. In order to achieve this goal, certain procedures have to be implemented for continual risk management relating, for example, to the cyber security of SICK products. An acceptable security level must be achieved by mitigating threats and following industry best practices.

This document states the minimum cyber security requirements that must be met for every software-related product that is supplied to SICK (hereinafter referred to as "*Product*").
A supplied item is a software-related *Product* if it uses any type of software, is partly software-based or is in itself a type of software and which SICK provides for use in its own products or for distribution to customers.

This document specifies the requirements that the supplier must meet with regard to:

- General responsibilities
- Organizational responsibility of the supplier
- Product security
- Vulnerability management, communication, notification and immediate actions on security related incidents
- Assessment of maturity

General responsibilities

The supplier and SICK view cyber security as their common responsibility to protect the customers of SICK. Within this responsibility, the supplier is responsible for complying with the specifications in this document. Furthermore, the supplier shall deliver to SICK secure and legally compliant *Products* reflecting the industry standards within the cyber security field, other regulatory standards in the country of delivery as well as SICK security requirements.
The supplier shall provide for its *Products* state-of-the art security against tampering, malware, eavesdropping, spying, network attacks, unauthorized access to end user data or any other malicious activity by an unauthorized third party.
The supplier shall in particular implement, and comply with, the security principles and standards of the IEC 62443 series of standards throughout the *Product* lifecycle.

Organizational responsibility of the supplier

The supplier is responsible for the cyber security of its *Products*. The supplier shall implement technical and organizational safeguards to ensure such cyber security. This includes the careful selection, instruction and training with regard to the cyber security of the *Products* of all (internal and external) employees involved in the supplier's business operations.

Product security

The supplier shall develop and deliver secure *Products* to minimize impacts associated with potential security issues.

This includes but is not limited to

- responsibility for ensuring that the *Products* do not contain any weaknesses or vulnerabilities; and
- taking all reasonable steps to ensure that the *Products* are free from of any backdoors or other mechanisms which could result in a circumvention of security mechanisms or unauthorized access or control.

Vulnerability management, communication, notification and immediate action in the event of security related incidents

The supplier shall develop, document, and implement a process to respond adequately and without undue delay to vulnerabilities and security issues associated with its *Products* (so-called vulnerability management). This process shall conform to commonly accepted industry standards and practices (including the IEC 62443 standard series) and include but not be limited to the continuous monitoring of security advisory sources and assessments with regard to the *Products*. Where indicated, the supplier shall take immediate action.

The supplier shall provide the following contacts:

1. Immediate contact for cyber security-related matters to be discussed in the future:

   _____

2. Key account manager to handle escalations or breaches of conditions agreed upon in this document:

   _____

The supplier shall keep the contacts up-to-date at all times.

All communication related to vulnerability management shall be initiated via email correspondence in such a manner that confidentiality and integrity are maintained. Please use the e-mail address psirt@sick.de for this purpose.

The supplier shall notify SICK without undue delay about any cyber security incidents within its organization that may affect the security of the *Products* and, upon the request of SICK, cooperate closely with SICK to address the *Products'* vulnerabilities.

The supplier shall promptly deliver a solution if a cyber security incident is identified in a *Product*.

Assessment of maturity

SICK reserves the right to thoroughly test and inspect the supplier's *Products* regarding their vulnerability. In the event that the test and inspection results reveal security risks, SICK will notify the supplier and request remedial action. The supplier shall take remedial action to the extent that this is possible in particular consideration of the interests of SICK. Test and inspection by SICK will not release the supplier from its responsibility to develop and deliver secure *Products*.

SICK reserves the right to request further documentation and evidence as well as to perform or order a compliance audit at any time in order to determine whether the listed requirements have been met. Each Party shall bear the costs it incurs in connection with the audit.
If the supplier documentation or audit results reveal gaps in the fulfilment of the SICK requirements, the supplier shall, at its own expense, take all steps and follow all reasonable instructions of SICK to close such security gaps without undue delay.

Signed in acceptance of the above

_____
Place, Date

_____
Signature

_____
Name

_____
Function

_____
Company