Axis supply chain security

Introduction

Customers in the information, technology and security industries need assurance that the solutions being implemented in their business are safe and can be trusted. Systems and data must be accessible, but only to the intended users, and devices must be able to operate on the network without unauthorized intrusion or unintended exposure. The solution must function as designed and intended, with maintained integrity and uninterrupted functionality.

Security threats are always present. New threats arise, and their nature might change at any point in time. This means that risks and their consequences must be assessed continuously, so that the appropriate risk-mitigating steps can be taken. It's important to partner with a supplier that is prepared to offer transparency and support at every level.

Axis is 100% focused on minimizing security risks and support customers and partners by:

- **Designing and manufacturing secure products with built-in protection**
- **Share knowledge and tools for putting safeguards in place**
- **Provide speedy response and free upgrades in case of newly discovered vulnerabilities**

> **Axis is dedicated to ensuring that all products have a safe journey through the entire supply chain, from component level to finished product.**
>
> Per Ädelroth, Vice President Operations at Axis Communications

Axis supply chain and supply chain partners

Component supplier

Manufacturing partner

Axis configuration and logistics center

Distributor

System integrator

End customer

Axis keeps information, systems, components, equipment, facilities, software, and products, safe in our supply chain. This document will give you an overview of how we work with **supplier governance, physical security, information security, personnel security** and **product integrity.**

> **Establishing long-term partnerships with our suppliers, built on trust and transparency, is key to our success.**
>
> Anton Gustavsson, Operations Manager at Axis Communications

Supplier governance

Supply chain security begins with choosing the right supply chain partners. Axis works with partners who share our view that security is key. All of our suppliers have gone through a rigorous evaluation process before being added to the Axis approved vendor list. The evaluation process includes an analysis of the company's quality environmental and sustainability management process. We require the company to be certified by a third party according to ISO 9001 or IATF 16949. The company's process for risk management is evaluated, as well as the production facilities and production process. To get an in-depth understanding of the potential new supply chain partner, Axis looks at the company's financial position, ownership, and ownership structure, as part of the evaluation process.

Axis partnerships with suppliers of critical components and manufacturing partners are particularly close and long-term. Together with these strategic suppliers, we drive joint projects and development, set targets and make long-term mutual commitments and plans. Collaboration and communication are close and occur daily, and onsite visits by Axis personnel are frequent.

Critical components in our products are procured directly by Axis from strategic suppliers, and stored inhouse. Non-critical components are procured by manufacturing partners according to our requirements, from suppliers on the Axis approved vendor list. We work with the manufacturing partners to produce the majority of the product lines in our portfolio. Production processes are defined and monitored by Axis, critical production equipment is developed, produced, and provided by Axis, as is the system for testing the components, modules, and products, at the different levels during production. All software and tests are also developed inhouse by Axis, and we provide all testing computers and other IT hardware infrastructure. **Production data is shared 24/7 with Axis, enabling real-time data analysis. The high level of transparency makes it possible for us to assess any potential security risks in collaboration with the manufacturing partner, as well as implementing mitigation plans.**

We ensure that our suppliers comply with Axis requirements by conducting onsite audits according to a risk-based audit plan that is updated regularly. Quality teams from Axis audit everything from process compliance, including documentation, to facilities, making sure that requirements for security, physical handling, inventory handling, production equipment, quality control, and traceability records are met. Quarterly business reviews are also a common way to follow up on performance against expectations. For strategic suppliers, the reviews are done on top management level within Axis Operations.

Physical security

Every site within Axis supply chain, from the component supplier to the distribution center, must meet high requirements for facility security. For example:

> **Entries and exits must be continuously guarded, access controls and visitor registration must be logged and stored**

> **Scanning of equipment may be used to detect undesirable objects or materials**

> **Transportation is arranged with recognized, well-known forwarders, maintaining rigorous security regulations and controls**

> **All air-freight cargo is x-rayed, and chauffeurs and trucks are subject to a long list of safety regulations at pickup and dropoff**

> **Incoming and outgoing goods are often surveilled and documented using CCTV cameras**

Most of the Axis configuration and logistics centers (CLCs) outside of Sweden maintain certification with the Authorized Economic Operator (AEO) program maintained by the EU or the United States Customs and Border Patrol's Customs-Trade Partnership Against Terrorist (C-TPAT) logistics security programs. These programs prevent contraband and require protections which in turn guard against tampering with products.

Information security

Information security is integral to the Axis brand, as is our commitment to safeguarding the data of customers and partners. We apply multi-layer protection to ensure data confidentiality, preventing disclosure of stored, processed or transported data to unauthorized users. Further, it ensures data integrity, protecting data from unauthorized change and manipulation while keeping the data available for intended users. Data transfer in the supply chain network is protected by **security protocols, utilizing encryption methods and authentication.** We always follow the latest technology development and applies continuous improvement. We require suppliers and partners to maintain a high level of information security, to mitigate risk of any gaps in the supply chain. Axis has a systematic approach to information security, using an information security management system (ISMS) to manage sensitive company information. The system covers people, processes, information systems, and physical security and complies with ISO 27001 and the General Data Protection Regulation (GDPR). The ISMS enables effective risk management and improves awareness of strengths and weaknesses. The substantial work within security is conducted in line with ISO 27002.

Personnel security

Quality and security in the recruitment process are key at Axis. Knowing who you are hiring is critical, not only from an educational, competence, and work experience perspective, but also from a security perspective. Overall, it is also important to share Axis core values. Approaches include identity verification, reference requests, and making security background checks prior to employment. New employees and consultants are required to sign a non-disclosure agreement (NDA) protecting intellectual property and other sensitive information, both during employment and after departure. All employees get education and training on information security awareness and are called on to exercise caution and stay alert. Access to information, systems, and resources is restricted at Axis, and granted to only those employees who need it to conduct their duties. The same goes for employees at suppliers and manufacturing partners, sharing information, systems, and resources with us.

Product integrity

Product integrity can be achieved if the product's hardware and firmware are successfully protected from unauthorized change or manipulation during the product's journey through the supply chain.

Together with our suppliers and manufacturing partners, Axis applies a multitude of quality controls to maintain and protect the integrity of our products. For example:

- Axis Information Security Management System (ISMS) is ISO 27001-certified, which means it follows internationally recognized processes and best practices in managing the internal information infrastructure and systems that support the product's journey through the supply chain
- We apply the concept of "zero trust" which is based on the principle of by default not trusting anyone, whether human or machine, connecting to and within the networks and architectures
- Components are always sourced from a supplier on the approved vendor list, according to Axis bill of materials in the Axis specification
- The supplier may not change critical production specifications without permission from Axis. Any approved change must be documented and logged
- A material handling process always ensures status of materials, revealing any deviations that could compromise quality
- Suppliers and manufacturing partners are required to maintain a traceability system, which ensures traceability of produced batches from incoming material to finished part. During production, the part will undergo multiple tests, such as Incoming Quality Control (IQC) and Automatic Optical Inspection (AOI), that can check that no counterfeit components are mounted.
- Critical production equipment and the underlying test system is developed, produced, and provided by Axis, as is the system for testing the components, modules, and products at the different levels during production, thereby limiting the risk for tampering. We provide a long list of built-in enhanced security features.
- ARTPEC® is Axis in-house developed system-on-chip (SoC) which are NDAA compliant chipsets. ARTPEC has built-in security features exclusively for Axis devices, including signed firmware so only secure authorized firmware can be installed and secure boot, which prevents booting of unauthorized firmware.
- On top of this, further enhancing security controls, all test data is shared with Axis 24/7 from our production partners, so unauthorized modifications can be immediately identified

> **"The US government and companies are at the forefront when it comes to cyber, and Axis product portfolio is 100% NDAA- compliant which is a result not only of our technology and in-house chipset knowledge, but also our culture. This is an important piece in our total value proposition to our partners and end customers.**
>
> Fredrik Nilsson, Vice President, Americas

Read more about cybersecurity

Built-in cybersecurity features
www.axis.com/solutions/built-in-cybersecurity-features

Cybersecurity
www.axis.com/cybersecurity

About Axis Communications
Axis enables a smarter and safer world by creating solutions for improving security and business performance. As a network technology company and industry leader, Axis offers solutions in video surveillance, access control, intercom, and audio systems. They are enhanced by intelligent analytics applications and supported by high-quality training.

Axis has around 4,000 dedicated employees in over 50 countries and collaborates with technology and system integration partners worldwide to deliver customer solutions. Axis was founded in 1984, and the headquarters are in Lund, Sweden.

©2023 Axis Communications AB. AXIS COMMUNICATIONS, AXIS, ARTPEC and VAPIX are registered trademarks of Axis AB in various jurisdictions.
All other trademarks are the property of their respective owners.