INFORMATION SECURITY POLICY

Classification: Public

Content

Definitions

Employees - all employees of Adva Network Security GmbH

Information - the collection of data in a particular context from which conclusions can be drawn

Information security - the protection and preservation of information, including its confidentiality, integrity and availability.

Security incident - suspected, attempted, successful, or imminent vulnerability, disruption, or interruption related to information security.

Document Owner	Version	Revision	Date	Status	Page
Anne-Katrin Viehoefer	1.0	A	February 18, 2025	>approved<	2 of 6

About us

Adva Network Security GmbH was founded to help enterprises, government agencies and critical infrastructures respond appropriately to increasingly complex threat situations. With our many years of experience in the field of cryptography and our unique encryption technologies, we ensure end-to-end network protection that meets the highest requirements of the industry and thus protects transmission and data networks from cyber-attacks. Our product and service portfolio includes Layer 1 and Layer 2 products and corresponding services.

Introduction

Every day, we process sensitive information in order to fulfill our tasks and obligations to our customers, contractors, employees, service providers, government agencies and other third parties. The protection of this information is of vital importance to Adva Network Security GmbH and is understood as a necessary management task. This is reflected in our IT systems, business processes and product lifecycles. The processing of information is essential for achieving our strategic and operational business goals and, as experts in network security, we ensure comprehensive protection of all information along the value chain.

With this policy, Adva Network Security GmbH acknowledges its responsibility for the security of information. The Executive Management is committed to implementing, maintaining and continuously improving information security measures in all relevant business areas and processes.

Our company's goal is to achieve and maintain the best possible implementation of the three protection goals of information security (confidentiality, availability and integrity), taking into account the economic efficiency of Adva Network Security GmbH.

This policy defines the principles that govern the management of information security in the company. It is the basis for processing company information as well as that of our customers using the necessary IT systems. It serves as the basis for the development and deployment as well as the integration of our network security solutions.

Legal requirements and contracts with customers, employees and other project partners result in additional obligations to ensure information security. The measures to protect sensitive information, data, IT systems and IT resources comply with the applicable and relevant legal requirements and regulations.

The guidelines, standards and procedural instructions based on this policy ensure the transparent and secure handling of information.

Scope

The policy and the guidelines, standards and procedural instructions based on it apply to all Adva Network Security GmbH locations. The policy and all resulting regulations and measures apply to all employees (on-site or remote), partners and, if applicable, other parties who have a contractual service relationship with Adva Network Security GmbH and receive access to information or access to the IT infrastructure for this purpose.

Principles and goal of information security

All sensitive information, data, IT systems and IT resources shall be protected by Adva Network Security GmbH in accordance with their defined level of protection in such a way that:

- only authorized persons can access it and publish information (protection goal: confidentiality), and
- only authorized persons can make permissible changes (protection goal: integrity).

In addition, it must be ensured that authorized persons have access to relevant information, data, IT systems and IT resources at all times (protection goal: availability).

The aim of information security is to reduce the risks related to achieving the protection goals to an acceptable minimum by taking appropriate measures. In addition to the security of IT systems and the data and information stored in them, the protection of non-electronic data and information is of equal importance.

Organization

The **Executive Management** of Adva Network Security GmbH bears the overall responsibility for the security of information. It provides sufficient technical, financial and human resources to be able to implement necessary measures regarding information security. The Executive Management ensures the appropriate priority and attention for the topic and is responsible for the organizational anchoring of activities regarding information security.

To this end, the executive management has appointed an **Information Security Officer** (ISO). The ISO is responsible for establishing, maintaining and continuously improving information security in the company and initiates, plans and implements the necessary measures. The ISO reports directly to the Executive Management.

Furthermore, the **Group Privacy Officer** of Adtran Networks SE has been appointed by the Executive Management to support the management in the area of data protection law and data protection procedures.

Process owners are responsible for identifying risks in their processes and are also the risk owners. It is their responsibility to implement the measures defined by the ISO within the process.

All **employees** of Adva Network Security GmbH are obliged to ensure information security by acting responsibly and complying with relevant laws, regulations, guidelines, instructions and contractual obligations.

They are required to ensure correct, responsible handling of the IT systems, data and information they use. It is their responsibility to report information security-related concerns to the ISO in order to support them in the performance of their duties.

Supervisors play the role of mediator and role model in sensitizing employees to the issue of information security and implementing measures or having them implemented.

Implementation and improvement

The information security management system (ISMS) is a key to the success of ensuring information security at Adva Network Security GmbH. The ISMS supports the protection goals of information security, and thus corporate goals, through a set of rules that specify preventive, detective and reactive measures at an organizational and technical level. These aim to prevent data loss and the standstill of core processes.

The ISMS provides information that helps to raise awareness of information security within the company. Employees receive training on information security and information security threats at regular intervals, but at least once a year.

The guidelines, standards and procedural instructions are formulated in an understandable and comprehensible manner and are made available to each employee, depending on confidentiality.

The information security process and all related documents, guidelines and instructions are reviewed regularly, but at least every two years, to ensure that they are up to date and effective, and are adjusted if necessary. In this context, Adva Network Security GmbH provides for internal audits and management reviews.

The management level contributes to the continuous improvement of the security level by critically analyzing deviations from set targets. Employees are encouraged to communicate potential improvements and vulnerabilities and are required to report security incidents immediately.

Validity and sanctions

This Policy shall be enforced upon its publication.

Management and employees with personnel responsibility ensure that the information security guidelines are followed by all employees.
Violations and infringements of the information security guidelines may have consequences under labor law, civil law and criminal law.

The latest version shall be made available on the company's intranet. Changes and revision statuses must be updated on the intranet without delay.

Approval

Anne-Katrin Viehoefer |

Information Security Officer

Nadja Fräbel |

Deputy Information Security Officer

Josef Sißmeir | Managing Director

Michael Roth | Managing Director

Document Owner	Version	Revision	Date	Status	Page
Anne-Katrin Viehoefer	1.0	A	February 18, 2025	>approved<	6 of 6

- Classified as Public -