Information security guidelines

December 2020

CONTENTS

Definitions

Employee – ADVA's employees globally

Information – the collection of data in a specific context from which conclusions can be derived

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

Information security program – policies, processes, standards, awareness training and other initiatives supporting the information security guidelines

Security incident – suspected, attempted, successful, or imminent threat of vunerability, fault, disturbance, disruption or interruption with regard to information security

Version: 2.0, December 2020

Author: Anne-Katrin Viehoefer, VP, information security, CISO

Validity: This guideline applies to all ADVA companies and all ADVA functions worldwide.

Our company

ADVA is a company founded on innovation and driven to help our customers succeed.

Our technology is the foundation of a shared digital future and empowers networks across the globe. We're continually developing breakthrough hardware and software products that lead the networking industry in performance, speed, and security and create new business opportunities.

Together, we're building a truly secure, connected and sustainable future.

1. Introduction

Every day we process sensitive information to fulfill our duties and obligations towards our customers, contractors, employees, service providers, government agencies and other third parties. The protection against unauthorized access and unauthorized modification of that information is therefore of vital importance for ADVA and reflected in our product lifecycles, business processes and systems.

The management board is committed to implementing information security measures in all relevant product lifecycles and business processes and to maintaining and continuously improving them. These information security guidelines set forth the principles that govern the management of information security at ADVA. These principles are based on the applicable legal provisions and, in large part, on ISO 27001, ISO 27034-1, NIST Cybersecurity Framework and the IT-Grundschutz (IT basic protection) of the German Federal Office for Information Security (BSI). Our commitment to information security is reinforced by our code of conduct.

2. Strategy

The pillars of information security are confidentiality, integrity and availability. ADVA strives for the highest possible level of information security associated with an economic use of its resources to minimize the connected risks. This underlying approach is aligned with ADVA's overall company strategy.

Thus, the management board defined the ADVA information security mission statement as follows:

> **ADVA's management is committed to support all aspects of information security**
>
> **related to its products, services, data, infrastructure and people.**
>
> **... to ensure compliance with domestic and international laws.**
> **... to maintain long term competitive advantage.**
> **... to be a trusted security partner.**
>
> **All ADVA employees support the security mission.**

3. Organization

The management board has appointed a chief information security officer (CISO) who is supported by ADVA's global security board representing all major functions of the company. The CISO oversees, initiates, plans, implements, maintains, and continuously improves the information security program and reports directly to the management board.

The management board will provide sufficient resources, in terms of human resources, budget and time, to implement the necessary information security measures.

The global security board maintains, improves and controls all information security measures and develops concepts and solutions for all relevant product and business processes and procedures to the desired level of protection of the respective information. In exercising its role, the global security board will consider the completeness, reliability and appropriateness of the processes and procedures and will be involved in new projects at an early stage in order to evaluate relevant information security aspects.

All ADVA employees are obliged to address all security-relevant topics related to any form of information security to the global security board and support them in the performance of their duties.

4. Measures

Information security measures are developed and implemented, especially in the areas of personnel, infrastructure, technology and organization, as well as compliance and governance. All measures are selected adequately according to our company's needs and future developments.

As part of the information security program, mandatory training is provided to all ADVA employees to increase information security awareness. All ADVA employees are urged to actively support the implementation and maintenance of those measures and to announce immediately upcoming and occurring security incidents.

ADVA will take immediate actions whenever a potential threat or security incident in its infrastructure or products is being detected.

Adverse behavior threatening the purpose of ADVA's information security guideline may have disciplinary, criminal or employment consequences. These consequences may apply not only to employees who commit violations, but also to those who condone violations, fail to take reasonable measures to prevent, detect and address violations, or seek to retaliate against those who speak up.

Sincerely,

Ulrich Dopfer
CFO