OPEN

L-06
Rev Nr. 02
21.11.2023

Information Security Guideline of the Nikon SLM Solutions AG

Guideline

Nikon SLM Solutions AG
(hereinafter Nikon SLM)

Scope

The information security policy applies to all locations and employees of Nikon SLM Solutions AG.

Responsibility

The Management Board of Nikon SLM bears overall responsibility for information security and has adopted this information security policy with the recorded objectives and the concepts derived and to be derived from them. It supports their achievement through appropriate personnel, material, organizational and technical measures, and the provision of the necessary resources.

The management supports and promotes the necessary structures and processes and has appointed responsible persons to implement this information security policy in procedural instructions, work instructions and documentation and to anchor it in day-to-day business.

Purpose

This security guideline is a summary of all guidelines on information security of Nikon SLM. It specifies the importance of information processing and information security, its objectives, the security strategy, the defined scope, the security process and the security organization.

The protection of sensitive data and information of SLM's business, customers and employees is one of Nikon SLM's core values.

Security Goals

The establishment and maintenance of information security as a key success factor for project work at Nikon SLM is realized through the objectives formulated below:

- continuous improvement of information security within Nikon SLM,
- early risk identification and risk minimization,
- Sensitization of employees regarding information requiring protection,
- cooperation with manufacturers and developers in the relevant industries,
- security deficiencies or incidents must not lead to critical failures and impairments of project and production processes,
- the laws and regulations relevant to the operation as well as contractual and regulatory obligations must be complied with,
- no unacceptable financial damage may result from safety deficiencies or incidents,

- safety deficiencies or incidents must not cause intolerable reputational damage,
- security deficiencies or incidents must not cause an intolerable outflow of personal data, IT operational data, development data, management data or productive data,
- the maintenance of information security must have the same priority as an overriding objective,
- the security objectives relate to all basic values of information security and are based on the statutory provisions, in particular the current protection requirements of the information worth protecting:

    - **Confidentiality:** Access to information objects by unauthorized persons must be prevented, in particular through technical measures, but also through appropriate sensitization of employees, to protect confidentiality and prevent manipulation.

    - **Integrity:** Malfunctions and irregularities in information objects and IT systems are acceptable only to a limited extent and only in exceptional cases.

    - **Availability:** The availability of information objects and IT systems in all areas relevant to operations is ensured in such a way that the expected downtimes can be tolerated.

Principles

Nikon SLM is committed to taking appropriate measures to protect sensitive data during electronic processing, documenting them, communicating them to employees and raising their awareness of data protection and information security issues.

Data and information are classified and processed using procedures appropriate to their classification.

SLM has implemented a risk management system that identifies risks to the confidentiality, integrity or availability of data and information and limits them to an appropriate level.

Changes to systems and applications are subject to a defined change management process that takes into account aspects of data protection and information security.

Regular internal audits ensure that data privacy and information security requirements are implemented and complied with by employees, and that weaknesses are identified and opportunities for improvement are exploited.