

# SECURITY POLICY

## This security policy applies to the following organizations:

- NGK SPARK PLUG EUROPE GmbH
- NGK SPARK PLUGS (UK) Ltd
- NGK SPARK PLUGS (France) S.A.S.
- LLC NGK SPARK PLUGS (Eurasia)
- NGK SPARK PLUG ME FZE
- NGK SPARK PLUGS SA

Hereinafter referred to as "NGK EMEA"

## 1. Introduction

This information security guideline is NGK EMEA's overall information security management policy. This document is binding for all stakeholders. Stakeholders include all persons<sup>1</sup>, groups, and institutions which can be directly or indirectly affected by decisions of NGK EMEA. This includes employees, shareholders as well as third parties who work for NGK EMEA (suppliers, partners, etc.). NGK EMEA has set up an effective information security plan to protect its core business and related information and fulfil its obligations to its stakeholders. Appropriate handling of information security issues is essential for business success and a reliable partnership with all stakeholders. As a modern, forward thinking company, NGK EMEA is aware of the need to ensure smooth and uninterrupted business operations. The management of NGK EMEA is responsible for the implementation of information security.

Appropriate resources are provided. The permanent improvement of information security levels throughout the NGK EMEA is continuously supported, demonstrating the management's full awareness of the importance of information security.

Data and information processed with NGK EMEA IT systems are essential for a variety of business processes. Due to the complexity of IT structures, they are at risk of abuse, loss, and sabotage. Therefore, adequate protection is mandatory. As a consequence, all technical and organizational measures to protect the information are of strategic importance to NGK EMEA. Ensuring information security is not a one-time process, but an ongoing process consisting of planning, implementation, control, and optimization (PDCA cycle).

Information security is not only a question of technology, but is also decisively dependent on the organizational and personal framework conditions.

As part of this commitment, an Information Security Management System (ISMS) has been set up to meet the requirements of the International Trusted Information Security Assessment (TISAX) standard. This standard is based on the DIN standard ISO / IEC 27001. Compliance with the ISMS is assumed by all stakeholders.

## 2. Definition information security

---

<sup>1</sup> For the sake of readability and simplification, only one gender-specific form is used. However, it always means male, female and gender neutral genders.

Information security means ensuring the implementation of appropriate technical, organizational and infrastructural measures to ensure the confidentiality, integrity and availability protection objectives. Information security identifies hazards so that concepts can be created to minimize risks.

### 3. Objectives

This common guideline for information security not only pursues the overriding protection goals but also the authenticity and resilience of information and data. In addition, the technical organizational measures required by the GDPR are effectively implemented in terms of transparency, data subject rights and purpose limitation.

### 4. Organization of information security

An information security organization has been set up to design the necessary processes. It consists of the Chief Information Security Officer (CISO) and the local Responsible Information Security Managers.

If you have any questions or comments, please contact our Information Security Officer.

**Josef Malik**

Chief Information Security Officer EMEA

Phone: +49 2102 974-555

Mobile: +49 1520 1600 171

E-Mail: [j\\_malik@ngkntk.de](mailto:j_malik@ngkntk.de)

**NGK SPARK PLUG EUROPE GmbH**

Managing Director: Damien Germès

Harkortstr. 41 • D-40880 Ratingen • AG Duesseldorf HRB 43118

