NITERRA EMEA REGION

# SECURITY POLICY

## This security policy applies to the following organizations:

- Niterra EMEA GmbH
- Niterra UK Ltd.
- Niterra France S.A.S
- Niterra Middle East FZE
- Niterra South Africa (Pty) Ltd.

Hereinafter referred to as "Niterra EMEA"

## 1. Introduction

This information security guideline is Niterra EMEA's overall information security management policy. This document is binding for all stakeholders. Stakeholders include all persons, groups, and institutions which can be directly or indirectly affected by decisions of Niterra EMEA. This includes employees, shareholders as well as third parties who work for Niterra EMEA (suppliers, partners, etc.). Niterra 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, Niterra EMEA is aware of the need to ensure smooth and uninterrupted business operations. The management of Niterra EMEA is responsible for the implementation of information security.

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

Data and information processed with Niterra 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 Niterra 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

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

**Niterra EMEA GmbH**
Managing Director: Damien Germès
Harkortstr. 41 • D-40880 Ratingen • AG Duesseldorf HRB 43118