# Information Security Policy

NEXEN TIRE upholds the core security principle of "ZERO TRUST," which dictates that trust should not be automatically granted. Our highest priority is to safeguard the valuable information assets of our customers, employees, and key stakeholders, including partner organizations. We are committed to achieving zero incidents of information leaks and breaches. Recognizing that information protection is now an essential rather than an optional endeavor, we have established a set of information security principles with full backing from the management. Our aim is to cultivate a robust information security culture where every employee actively participates.

To achieve this objective, we execute a comprehensive range of activities across crucial domains, encompassing management security, technical security, and physical security. We place great emphasis on establishing an efficient information security system and robust compliance measures, ensuring the security of our systems, conducting simulated cyber response exercises, and enhancing employee awareness.

All employees bear the responsibility of safeguarding information assets by adhering to regulations and guidelines stipulated in the information security policy. This obligation also extends to our entrusted information processors and key partners, thereby ensuring the utmost protection of customer information.

## Information Security Principles

1. Employees shall comply with the information security policy, regulations, and guidelines to protect information assets.
2. Employees shall not use information assets for personal purposes and shall not disclose them to unauthorized external parties.
3. Employees shall not access or leak unauthorized information assets or data.
4. Employees shall comply with legal requirements related to information security and fulfill their social responsibilities.
5. Management shall actively support the allocation of necessary budgets and resources for information security.
6. Management shall proactively establish and enforce information security policies.
7. Management shall lead by example and adhere to the information security policy.

## Information security codes of practice

### 1. Information Security Guidelines

In order to maintain a consistent level of information security within the company, strict adherence to the recommended essential requirements specified in the codes and guidelines is mandatory.

1) Information Security Regulations:

   i. Personnel Security Guidelines

   ii. Information Asset Management Guidelines

   iii. Security Incident Response Guidelines

iv. Information Security Organization Operation Guidelines

v. User Security Guidelines

vi. Technical Security Guidelines

vii. Physical Security Guidelines

viii. Information Security Risk Management Guidelines

ix. Partner Security Management Guidelines

x. Personal Information Protection Guidelines

## 2. Information Security Incident Response System

In the event of an information security breach, our company has implemented a robust incident response system aimed at promptly addressing the issue during its initial stages and mitigating potential damages, thereby ensuring no further harm ensues. This system is consistently managed through simulated training exercises conducted on a regular basis.

**[Information Security Incident Response Process]**

i. Incident Identification

ii. Reporting of Suspicious Activities (to Information Security Department and Responsible Personnel)

iii. Formation of Incident Response Team

iv. 4-Stage Incident Response Process

a) Initial Measures b) Root Cause Analysis c) Problem Resolution d) Follow-up Actions

v. Reporting to Relevant Authorities (if necessary)

vi. Development and Implementation of Preventive Measures

vii. Monitoring and Post-Incident Management

| | | | |
|---|---|---|---|
| **Title** | NEXEN TIRE Information Security Policy | **Version** | 1.0 |
| **Establishment Date** | 26.06.2023 | **Revision Date** | - |
| **Establishment & Revision Department** | Information Security Team | **Management Department** | ESG Team |