Impact
tomorrow

Cybersecurity Policy

As a globally recognized provider of sustainable e-mobility solutions, we place the highest priority on safety, reliability, and future readiness. Our products and customized system solutions meet the highest standards and have earned the trust of our customers worldwide. To achieve these goals, we take the challenges and risks of cybersecurity seriously, considering them across the entire product lifecycle – both for road and rail vehicles as well as the growing e-mobility market.

With our certified Cybersecurity Management System, we identify and analyze cyber threats and risks from development through the end of a product's life. This ensures that our systems are protected at every stage and that we deliver solutions resilient to future threats.

Comprehensive Security Strategy

This approach is closely linked to our commitment to information security, firmly anchored in KIEPE's strategic orientation through our Information Safety Policy. At the same time, our safety policy focuses on developing functionally safe products. We deliberately leverage the interactions and synergies arising from this to continuously optimize our products and bring them to market even more securely.
Our efforts do not begin during product development. Cybersecure products require a corporate culture that actively incorporates cybersecurity not just in processes and legally required measures but also in day-to-day operations. This includes regular training and awareness programs for our employees, as well as a continuous improvement process where every contribution counts. Through these and other measures, we enhance awareness of the critical role cybersecurity plays in our products and systems, creating added value for our customers.

Cybersecurity Across the Entire Product Lifecycle

In implementing our various cybersecurity activities, we follow recognized standards such as ISO/SAE 21434 and CLC/TS 50701. These standards enable us to take a risk-based approach to identify and analyze threats to our products and define and continuously optimize countermeasures from the very start of the product lifecycle. This also includes evaluating cybersecurity across the entire supply chain. From the smallest component to the finished system, we hold ourselves and our suppliers accountable to very stringent standards that ensure risks are identified and adressed efficiently and effectively.

During product development, we rely on recognized industry standards and guidelines for secure programming. Additionally, we use advanced analytical methods to detect and address vulnerabilities early. Supported by software tools, we analyze our products from various perspectives – from hardware to the system level. Even after commissioning, we ensure through continuous vulnerability management that our products remain cybersecure over time. Our goal is to quickly identify new threats and maintain system operations through appropriate measures. With the help of our Software Update Management System, which conforms to ISO 24089, we can reliably and securely provide software updates to efficiently address cybersecurity-related incidents.

Cybersecurity Policy

kiepe.

Cybersecurity as a Collective Task

At every level of our organization, we are aware of the increasing scale of threats. WE are committed to providing the necessary resources and expanding our required competencies to effectively counter these growing risks. Only in this way can KIEPE continue to supply our customers with cybersecure products.

Alexander Ketterl
Chief Executive Officer

Roland Russo
Chief Operating Officer