

PRODUCT CYBER SECURITY POLICY

"Every day, more than one billion people around the world put their trust in systems made by Knorr-Bremse." Therefore, Knorr-Bremse RVS must deliver products and services that are secure, reliable, and trusted by our customers. We are committed to embedding product cybersecurity as a fundamental aspect of our organizational culture and operations. This policy mandates all teams and stakeholders to incorporate security considerations into every stage of the product lifecycle – from design and development to production, deployment, and maintenance. Security is a foundational element of our products, ensuring they perform reliably under all conditions and are resilient against evolving cyber threats.

PRODUCT SECURITY IS ONE OF OUR CORE VALUES

- **We** ensure Knorr-Bremse products and services comply with the statutory product security requirements, enhancing their resilience against evolving threats to strengthen the cybersecurity posture of rail operations.
- **We** commit to the requirements of applicable and established product cybersecurity standards and are involved in relevant committees and boards.
- **We** are committed to creating the organizational conditions needed to achieve this objective.
- **We** foster a culture of continuous learning and innovation to enhance our product cybersecurity practices and adapt to the evolving threat landscape.
- **We** are a customer-driven company, and we are committed to fulfilling our customer expectations by continuously improving the cybersecurity of our products and services.

PRODUCT SECURITY IS A CRITICAL FACTOR OF SUCCESS

- **We** strive to set the standard for product security in the rail industry by developing, manufacturing, and operating secure products and services.
- **We** are committed to being the technology and market leader for product cybersecurity throughout the entire product life cycle.
- **We** actively engage with our customers to develop and deliver products and services that are resilient and cyber-secure for rail operations.
- **We** collaborate closely with suppliers and partners to ensure that security is maintained throughout the supply chain of our products and services.

INDIVIDUAL RESPONSIBILITY AND OWNERSHIP ARE ESSENTIAL

- **We** strive to foster a security culture rooted in trust and confidence, where every employee understands the importance of product cybersecurity and takes personal responsibility in guaranteeing secure development and manufacturing processes.
- **We** collectively assume responsibility for the security and resilience of our products and services.
- **We** each are responsible for acting as security gatekeepers, ensuring that only products, services, and deliverables in compliance with established and applicable security standards and customer requirements are authorized for release.
- **We** encourage employees throughout our global companies and cultures to take ownership of product security within their roles, benefiting from everyone's skills, experience, and competence to strengthen our cybersecurity posture.



Harald Schneider
Member of the Management Board



Andreas Meyer
Chief Product Security Officer