Cybersecurity at the core of digital trust

www.kone.com

Dedicated to People Flow™

Foreword: Leading with confidence in a connected world

As cities constantly evolve and urban populations increase, we at KONE stand with one clear purpose: to shape the future of cities. This fuels our journey to the forefront of digital transformation in the industry.

Our elevators and escalators now form part of the digital nervous system that keeps modern cities moving, enabling seamless people flow and intelligent services across buildings, campuses, and communities. As KONE connects ever more products and solutions, we must consider how we can strengthen our role in this wider ecosystem – one where cybersecurity and trust are essential to keeping people and data safe.

This paper outlines how KONE approaches cybersecurity across our products, services, and customers. It reflects our commitment to transparency, continuous improvement, and leadership in secure smart infrastructure. We share tangible facts about how we protect our systems, collaborate with ethical hackers, and embed cybersecurity into every phase of our products and services – from design to deployment.

"At KONE, we see cybersecurity not just as a safeguard, but as a strategic enabler of trust, innovation, and smarter urban living. It's how we ensure our customers can move forward with confidence – knowing that every digital interaction, every connected service, and every person who moves within the urban ecosystem is protected by design. By embedding cybersecurity into everything we do, we help our customers unlock new value, operate with confidence, and shape smarter, safer cities together."

Petteri Rantanen
CISO, KONE Corporation

The new reality in the digital age

Our business is shaped by three megatrends: urbanization, sustainability, and technology. Technological development, with the adoption of digital technologies and AI, accelerates and plays an increasing role as a driver of competitiveness across industries.

Elevators are no longer just mechanical systems that move people between floors. Modern elevators, embedded in digital ecosystems, communicate with cloud platforms, exchange data with building management systems, and offer remote monitoring and predictive maintenance. We aim for 100% connectivity in our service base and to securely connect customer-level and operational data to the cloud.

The resulting transparency means we are not only able to work in smarter ways but also improve employee experience, leading to higher productivity. Technological innovation brings immense value to elevator users and building owners alike. New capabilities enhance safety, efficiency, and user experience.

As digitalization reshapes the built environment, cybersecurity affects every aspect of our business – from customer trust and regulatory compliance to innovation and operational continuity. That's why we've made cybersecurity a strategic priority. Our ambition is to lead the industry by example.

What's at stake for our customers

Smart cities are efficient, sustainable, and empowering, with connected devices allowing citizens control over everything from mobility to home appliances. But as technology becomes smarter, so do the threats that target it. Protecting customer journeys demands constant vigilance and the integration of cybersecurity at every level.

Whether transporting patients in hospitals, travelers in airports, or employees in office towers, our customers rely on uninterrupted service and safe operation. Cybersecurity safeguards more than systems. It enables compliance with evolving regulations, supports sustainable innovation, and ensures that every elevator ride, service interaction, and data exchange is built on trust.

Confidence in connectivity, communication and assurance

Our customers expect the same level of security from their elevators and escalators as they do from their networks and cloud platforms. KONE's secure-by-design approach ensures that connectivity enhances their operations without compromise.

To give our customers clarity into how our cybersecurity protects their operations, we provide straightforward, credible materials that help them make informed decisions and communicate confidently with their own stakeholders.

KONE cybersecurity approach: Built for trust

We build urban environments with sustainable and secure smart solutions. Cybersecurity at KONE is not just a technical function – it's a cross-functional community enabling digital trust and resilience. This chapter outlines how KONE embeds cybersecurity into its operations, products, and culture.

2023

KONE's commitment to cybersecurity was recognized when it became the first in the industry to gain the internationally recognized IEC 62443 cybersecurity certification for its DX class elevators, and ISO 27001 certification for its digital services.

60,000

suspicious messages reported annually via KONE employees.

50+

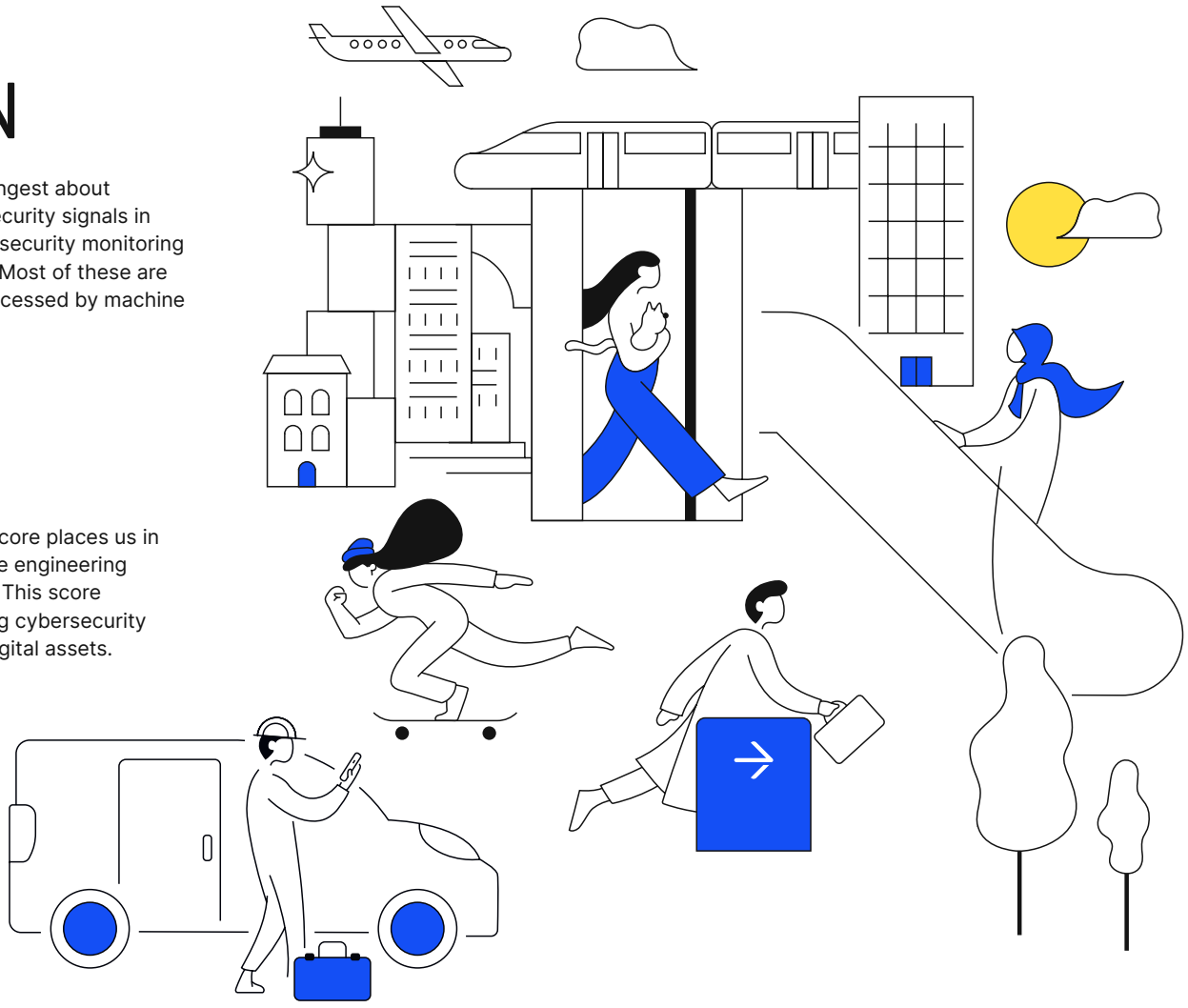
Cybersecurity experts worldwide: Our global team of cybersecurity professionals spans multiple regions and disciplines, ensuring deep expertise across enterprise, product, and supply chain security domains.

41 BN

On average, we ingest about 41 billion cybersecurity signals in our cloud-based security monitoring system monthly. Most of these are automatically processed by machine intelligence.

10%

KONE's BitSight score places us in the top 10% of the engineering industry globally. This score reflects our strong cybersecurity posture across digital assets.



Building resilience with smart governance

Our cybersecurity governance ensures that frameworks are effectively implemented at all levels of the organization – policies and principles are not just documented but lived. The status of cybersecurity is reported regularly to senior leadership and we connect cybersecurity, business, and compliance risks to drive informed decisions on building resilience.

We operationalize ISO 27001 across the enterprise. A centralized cybersecurity control catalog guides the implementation of controls across domains such as identity and access management, threat and vulnerability management, and supplier security. With our governance year clock, we make sure that internal and external audits, maturity and risk assessments and readiness reviews are completed across geographies. This structured approach helps us synchronize efforts and ensures timely compliance.

We foster a proactive “I own cybersecurity” culture through awareness programs, targeted training, and active communication. Our security champion program helps us drive sustainable behavior change.

We build organizational resilience through simulations and exercises. We conduct targeted crisis simulations to test incident response and stakeholder coordination. These drills help teams rehearse real-world scenarios and improve readiness across geographies.

Data privacy at KONE: Our commitment to digital trust

Data privacy is a foundational principle embedded into the design and operation of our smart solutions. As our digital ecosystem evolves, we remain steadfast in our commitment to protecting the privacy of our customers, users, and employees.

We adhere to a privacy by design and by default philosophy, ensuring that personal data is collected only when necessary, processed as anonymously as possible, and deleted once it is no longer needed. Access to personal data is strictly limited to authorized personnel, and all processing activities are governed by robust internal controls and aligned with applicable data protection regulations, including the EU General Data Protection Regulation (GDPR).

Our approach is guided by a multi-layered cybersecurity and privacy framework, which integrates people, processes, and technology. We foster a culture of awareness and accountability through continuous training and clear responsibilities, recognizing that every employee plays a role in safeguarding data. Our policies and procedures are regularly reviewed and updated to reflect the evolving threat landscape and regulatory requirements. We deploy advanced security technologies, such as, encryption, intrusion detection, and secure cloud infrastructure, to ensure data integrity and confidentiality across our digital platforms.

Whether it’s managing access to building entry logs, securing cloud administration, or ensuring the resilience of our connected equipment, KONE’s privacy practices are designed to uphold trust and deliver peace of mind in every interaction.

Built-in security for connected enterprise and manufacturing

KONE’s security policies define controls to safeguard premises, information and information systems which are both in development and in operation, in order to detect cybersecurity incidents and to respond and recover in a timely manner. KONE works with third-party security service providers and trusted technology partners to manage risks through the control framework. KONE conducts tests, reviews, and exercises to identify areas of risk and to ensure appropriate preparedness. The company continues to invest in its cybersecurity capabilities based on these findings.

KONE safeguards the digital backbone of its operations and customer services, from core IT infrastructure to supplier ecosystems, through a comprehensive cybersecurity strategy. We deploy layered security controls across endpoints, networks, cloud platforms, and AI systems. By leveraging encryption, identity management, and proactive threat detection, we can ensure that our employees can get their work done securely without compromising innovation or agility.

In manufacturing environments, cybersecurity needs often differ from those of typical office setups. We protect factory systems by establishing secure architectures, segmented networks, and remote access controls.

Security by design: protecting products and experiences

At KONE, security is a mindset deeply embedded into every phase of product development and operations. Security champions and subject matter experts guide product teams in integrating secure practices into their daily work, fostering a culture where security is not simply a checklist, but a core principle of daily practice.

Our Product Security Index (PSI) assigns each product a 0-100% score to highlight critical gaps, such as missing inventories, overdue vulnerability fixes, or incomplete documentation. This enables teams to prioritize remediation and benchmark security across products.

Technician tools, mobile apps, and connected devices are routinely tested and fortified against threats, following a structured roadmap for secure development and operations. To further strengthen cybersecurity, KONE runs a global bug bounty program that invites ethical hackers and security researchers to report vulnerabilities and earn rewards, fostering a culture of transparency and continuous improvement.

We follow a Secure Development Lifecycle (SDL) process certified according to IEC 62443-4-1, ensuring that security is embedded from ideation to deployment. Threat modeling, risk assessments, and technical security documentation are mandatory for all high-impact products. Our SDL tooling integrates with development pipelines, enabling automated security validatio and continuous improvement.

KONE's approach to product security is anchored in a robust, multi-layered framework that spans governance, technical controls, and operational excellence. Our capabilities are designed to meet the evolving expectations of customers, regulators, and industry standards.

Our cloud platforms are managed with dedicated security architecture, disaster recovery plans, and continuous monitoring. IoT devices undergo external security testing and comply with global standards such as IEC 62443-4-2.

At KONE, cybersecurity is not just a function – it's a mindset-woven into the fabric of every product team. Our champions program is a cornerstone of this approach, ensuring that security is a shared responsibility and an everyday practice. Tribes in our IT and R&D teams have at least one member trained extensively in cybersecurity. These security champions are motivated team members who receive advanced, role-based training from KONE's cybersecurity experts. They serve as the first line of security support within their teams, acting as local advocates and guides for secure development practices.

Cybersecurity standards shaping the elevator industry

As elevators evolve into connected digital platforms, cybersecurity standards have become the backbone of product assurance and regulatory compliance. These standards not only define technical requirements but also shape how manufacturers design, develop, and maintain secure systems. At KONE, we don't just follow these standards – we help shape them.

The ISO 8102-20:2022 standard marks a pivotal moment for the elevator and escalator industry. It is the first global cybersecurity standard specifically for lifts, escalators, and moving walkways

capable of connectivity. The standard builds upon the foundational principles of IEC 62443, applying them to the unique architecture and operational context of vertical transport systems.

KONE has played a leading role in the development of ISO 8102-20, contributing expertise and chairing working groups to ensure the standard reflects real-world challenges and opportunities. Our commitment to this standard is not just theoretical – it is embedded in our product development lifecycle, architecture reviews, and certification roadmaps.

KONE's involvement in shaping ISO 8102-20 and contributing to IEC 62443 reflects our broader commitment to industry leadership. We actively participate in global standardization bodies, collaborate with peers, and advocate for secure-by-design principles across the value chain.

Cyber confidence across our value chain

At KONE, we build confidence in cybersecurity across our value chain by working closely with customers and suppliers. We ensure that our subcontractors and partners also maintain high cybersecurity standards, safeguarding the broader ecosystem and supporting the seamless operation of our customers' activities. Supplier risk is proactively managed through a structured profiling process, requiring all suppliers to meet strict, non-negotiable criteria, including incident notification and documented practices.

Our cyber defense strategy focuses on protecting what matters most, with continuous monitoring of digital environments, early threat detection and rapid incident response. Our cyber defense capabilities include 24/7 monitoring, automated response, threat intelligence, and proactive threat hunting. We conduct regular simulations and follow playbooks to prepare for ransomware, data breaches and supply chain disruptions, enhancing resilience and reinforcing customer trust. Vulnerability and patch management are streamlined across IT and product environments, with clearly defined ownership and measurable outcomes.

Our cybersecurity standards and certifications

KONE products and solutions are developed with cybersecurity in mind from the start. We follow secure software development processes to embed cybersecurity and privacy into our digital solutions throughout their lifespan. Our secure development lifecycle (SDL) process is certified to IEC 62443-4-1 issued by TÜV Rheinland.

Industry standard ISO 8102-20 Read more →

IEC 62443-4-1 Read more →

IEC 62443-4-2 Read more →

ISO 27001 Read more →

UK Cyber Essentials Plus Read more →

Looking ahead: Innovation with integrity

Imagine a city where elevators not only transport people but also think and communicate to ensure smooth and efficient movement. This is the future we are shaping with our innovative solutions.

Our drive for innovation is fueled by our purpose to shape the future of cities and the megatrends that impact our industry: urbanization, technological disruption and sustainability. We solve everyday challenges faced by our customers and the 2 billion people that we move every day in urban spaces.

Innovation is in KONE's DNA – we are proud to find new and better ways of making a difference with our products and services, scaling and deploying them at speed and finding new, efficient ways of working.

Partnership and trust for the long term

We work side-by-side with our customers to ensure resilience, readiness, and peace of mind. With KONE, our customers are able to demonstrate a commitment to protecting their users, their brand, and their reputation.

Cybersecurity is not a one-time feature – it's a long-term commitment. Our customers choose us because they know we will evolve with them, support their compliance needs, and respond to emerging threats and regulatory requirements. Our cybersecurity practices – aligned with global standards like ISO 27001 and IEC 62443 – help reinforce that trust every day.

By embedding security into everything we do, we help our customers unlock new value, operate with confidence, and shape smarter, safer cities together, today and in the future.

At KONE, our purpose is to shape the future of cities. As a global leader in the elevator and escalator industry, we move two billion people every day, making their journeys safe, convenient, and reliable with smart and sustainable People Flow®. In 2024, KONE had annual sales of EUR 11 billion, and at the end of the year over 60,000 employees in close to 70 countries. KONE class B shares are listed on the Nasdaq Helsinki Ltd. in Finland.

Learn more: kone.com

KONE Corporation

Corporate offices

Keilasatama 3
P.O. Box 7
Espoo, 02150
Finland

Tel.: +358 (0)204 75 1
Fax: +358 (0)204 75 4496

Business Identity Code: 1927400-1

Dedicated to People Flow™