Responsibility for cybersecurity

LANCOM Systems regards the requirements for secure and trustworthy IT infrastructures as a fundamental prerequisite for the digitization of the economy and public administration. Cybersecurity has therefore been an integral part of solution development since the company's founding.

The development and quality assurance of LANCOM Systems' solutions take place in Germany in accordance with high security standards. The „IT Security made in Germany" quality label of the German IT Security Association, as well as certifications from the Federal Office for Information Security (BSI), attest to the level of security achieved.

Cyberattacks constitute a major risk for businesses and public institutions. With the Cyber Resilience Act, the European Union has defined binding requirements for the cybersecurity of products with digital elements, thereby creating a uniform regulatory framework.

Although the requirements of the Cyber Resilience Act (CRA) will only become fully applicable from December 2027, LANCOM Systems already incorporates key provisions of the CRA into the development of its solutions today.

Accordingly, LANCOM Systems aligns the design of its solutions with the following principles:

→ to design them so that, even when external interfaces are present, they offer the smallest possible attack surface (e.g., minimizing concealed access credentials and backdoor mechanisms),

→ to develop them in such a way that the impact of a security incident is mitigated through appropriate mechanisms and techniques (e.g., avoiding weak encryption),

→ and to ensure that security-related information is provided by recording or monitoring relevant internal events, such as access to data, services, or functions and any changes thereto, while also offering users an opt-out mechanism.

We continuously implement comprehensive technical and organizational measures to achieve a very high level of cybersecurity for our solutions. Despite all due diligence and our ongoing commitment to maintaining a high level of cybersecurity, complete and constant security cannot be guaranteed. An effective level of security requires not only technical measures but also appropriate organizational processes and their consistent implementation by users.

Wuerselen, March 23, 2026

Constantin von Reden,

CEO

Robert Mallinson,

Co-CEO