Information Security, Cyber Security, and Data Protection Policy

ElringKlinger AG relies heavily on information and telecommunications technology to render its services. The necessary processes, information, and systems are of substantial value to the company and play a key role in meeting its corporate mission. In order to protect those values, the Management Board has decided to introduce an Information Security Management System (ISMS) based on the principles of the ISO 27001 standard, a Data Protection Management System (DPMS), and a Cyber Security Management System (CSMS) based on ISO 21434. The aim is to run the ISMS, DPMS, and CSMS as an integrated management system.

The fundamental goal of information security activities is to provide suitable support for the business of ElringKlinger AG and protect the relevant corporate assets from risks in all essential subdivisions/units. The corporate assets requiring protection include:

- Intellectual property of ElringKlinger AG, its customers, and partners
- Special planning and management knowledge
- Knowledge and skills of employees
- Personal data of employees, partners, and customers
- Brands of the ElringKlinger Group or the reputation of the company and other material assets

It is also the goal of ElringKlinger AG to adhere to all statutory data protection and information security requirements, thus reducing any risk to the rights and freedoms of affected individuals to an acceptable level and ensuring the right to informational self-determination is preserved at all times.

All employees of ElringKlinger AG are responsible for upholding measures relevant to data protection, information security measures, and cyber security according to their fields of activity. The employees and all individuals working on behalf of ElringKlinger AG are obliged to comply with the laws and preserve company secrets. The Management Board of ElringKlinger AG is responsible for compliance with the legal requirements governing data protection, information security, and cyber security as well as provision of the necessary resources. The Group Information Security Officer (GISO) is responsible for compiling and implementing the relevant information security guidelines and measures; the Group Data Protection Officer (GDPO) is responsible for data protection, and the Chief Cyber Security Officer (CCSO) is responsible for cyber security.

Compliance with data security, information security, and cyber security guidelines ensures the confidentiality, availability, and integrity of data across all networks, systems, development processes, and production processes. Data must be protected against loss, with archiving performed where required by law. Disposal and deletion of information must also be dealt with in compliance with data protection law. Any contractual partners involved in order processing must follow and implement the instructions of ElringKlinger AG. When processing personal data or confidential data, all contractual partners must comply with the relevant standards, such as EU-DSGVO/ISO27701, VDA-TISAX/AIAG-TPISR, ISO 21434, ISO 27001, or similar.

Across the entire product lifecycle (i.e., from development to decommissioning), ElringKlinger AG implements the legal and customer-specific requirements as part of a cyber security management system. Overall responsibility for the establishment of this lies with the CCSO. At product level, the Cyber Security Manager is responsible for safeguarding against cyber attacks, with the support of the Functional Safety Manager and the departments.

Access to information according to classification must be restricted through authorizations, thereby utilizing the latest technology, and documented in accordance with data protection regulations to ensure transparency.

The relevant corporate assets must be protected against Acts of God (natural disasters/war), pandemics, fire, water, and theft. Information security risks must be assessed on a regular basis and appropriate counter measures taken as soon as possible to address any acute risk situation.

For all corporate divisions/units, risks are defined and evaluated internally and externally at regular intervals. If necessary, suitable counter measures must be defined and the effectiveness of these verified.

2024

THOMAS JESSULAT

REINER DREWS

DIRK WILLERS