Security Statement

Introduction

This security statement is intended to provide you with information about our security culture and practices in information security.

The security of our data and the data of our customers and partners is a high priority for us. We take targeted measures to ensure that all data provided to us is processed and stored securely. The security of our IT systems, our products and all data are therefore a matter of course for us and part of the corporate culture.

Our privacy policy with further information on how we handle, for example, the personal data we collect, can be found next to the imprint on the Framatome GmbH homepage.

Objectives and Continuous Improvement

Our main objectives in information security are

Confidentiality, integrity, availability, and traceability.

We are continuously expanding our information security management system (ISMS) and are guided by international standards such as ISO/IEC 27001. We are continuously working to improve information security and are guided by current findings and developments.

Information Security Policies (Policy) and Organization

The company issues written information security policies covering a wide range of security-related topics; from general standards for each employee, such as password policy, use of IT systems or building security, to more specific security standards for specific applications and information systems.

The obligations of employees and the permitted use of the information systems are defined. Every employee has unlimited access to relevant instructions as well as further documents and links in the company-wide intranet.

Framatome maintains a security organization with appropriately staffed staff units and a clear distribution of roles. Special teams (e.g. SOC=Security Operation Center, CERT=Computer Emergency Response Team) are responsible for continuity and security during operation as well as for incident response and reconnaissance.

Personal Safety / Awareness

Framatome performs a security check at the time of hiring. In addition, Framatome communicates its information security guidelines to all employees who must acknowledge them. In addition, all employees are expected to sign a non-disclosure agreement. All employees are trained annually in data protection and information security. We always pay attention to a high level of security awareness of current attack scenarios and risks.

For particularly sensitive, strategic and security-relevant positions, repeated security checks take place regularly.

Asset Management

Framatome has an asset management policy that includes the identification, classification, storage and disposal of information and assets. Company-owned devices are equipped with hard disk encryption and up-to-date application against malware. Only approved or proprietary devices may access corporate and production networks. Private devices are not permitted for official use.

Vulnerability Management and Penetration Testing

Framatome maintains a documented vulnerability management program that includes regular scans, identification and remediation of vulnerabilities on servers, workstations, network devices and applications. All networks, including test and production environments, are scanned regularly. Critical patches are applied prioritized.

We also carry out regular internal and external penetration tests and react accordingly to the results found after risk analysis.

Logging and Monitoring

Application and infrastructure systems log information in a centrally managed log repository for troubleshooting, security review and analysis by authorized Framatome personnel. Logs are kept in accordance with legal requirements.

Incident Management

Framatome lives a process of responding to security incidents in information security along with data protection. This includes initial incident response, classification and prioritization, investigation, customer notification, public communication, and remediation. This process is regularly reviewed and tested every two years.

Breach Notification

Despite all efforts, no method of transmission from the Internet and no method of electronic storage are absolutely secure. However, if Framatome detects a security breach, we will notify the affected stakeholders to take appropriate protective measures. Our procedures for reporting violations are consistent with our obligations under applicable laws and regulations of the countries and all applicable industry rules or standards. We inform and support our clients on safety issues and provide all the relevant information they need to comply with their own regulatory reporting obligations.

Risk Management and Audits

Information security measures are based on a systematic risk-based approach. An annual review and assessment of the risks is carried out. Regular internal and external audits lead to a continuous improvement of our information security.

Product Development

Our development team uses secure coding techniques and best practices according to recognized standards. Developers are trained in hiring and regularly developing safe applications.

Development, testing and production environments are separate. All changes are reviewed by experts and logged for performance, audit and forensic purposes prior to deployment in the production environment.

Physical Security

Framatome has policies, procedures and infrastructure to ensure both the physical security of its data centers and the environment from which the data centers are operated.

Both Framatome’s information systems and technical infrastructure are hosted in state-of-the-art data centers that are geographically separated to ensure high availability and redundancy for Framatome and its customers. Physical security controls in these data centers include 24-hour surveillance using cameras, electronic access control systems, visitor logs, access restrictions, fire detection and extinguishing systems.

Framatome’s premises, buildings and facilities are protected against burglary, theft and vandalism by various physical, organizational and technical measures. These include, for example, factory security, video surveillance, access control mechanisms via separation systems or reception.

Depending on the sensitivity of the activities and the information processed, there are different physically separated areas: public (visitor) area, office area, server and IT system areas.

Business Continuity Management

Framatome uses a comprehensive backup strategy for all systems to ensure minimal downtime and data loss. The Business Continuity Plan is regularly tested and updated to ensure its effectiveness in the event of a disaster. Backups are stored encrypted to maintain their confidentiality and integrity.

Servers have redundant internal and external power supplies. Data centers have backup power supplies and can source power from diesel generators and UPS.

Information Security at our Partners

Our high requirements in information security are an integral part of our contracts with our subcontractors, service partners, stakeholders and other partners. We monitor compliance with and implementation of our principles in audits.