**Information Security at Fresenius Kabi**

At Fresenius Kabi, we know information security is important to our customers, patients, and business partners. We are committed to maintaining information security through responsible management, appropriate use, and protection in accordance with legal and regulatory requirements.

**Organization of Information Security**

We published a written Cybersecurity Policy outlining cybersecurity roles and responsibilities that are defined within the organization.

Our security team focuses on information security, global security auditing and compliance, as well as defining the security controls for protection of Fresenius Kabi’s hardware and infrastructure. The security team receives information system security notifications on a regular basis and distributes security alert and advisory information to the organization on a routine basis.

**Information Security Capability Model**

We have adopted an Information Security Capability Model based on the Critical Security Controls (CIS 18), that is complemented by other security measures based on industry best practices. This allows us to maintain a holistic approach to compliance with respect to security.  Also, periodic maturity assessments of our security capabilities are regularly conducted, and the results reported to the Fresenius Kabi management.

**Security Compliance Management**

We are in the process of developing a set of rules that are aligned with the Fresenius Group baseline requirements, a Fresenius Group wide internal control catalog in alignment with industry best practices.

Fresenius Kabi has a formal internal audit program​​​​​ implemented to ensure compliance with our internal policies, relevant cybersecurity laws and regulations.

**Secure Data Management**

We have established a process for classifying data to apply appropriate security measures to protect the data of our customers, patients, and business partners.

We encrypt sensitive data in transit and at rest where possible and practical.

**Access Control Management**

We have established access management requirements for granting, managing, and revoking user access. Role based access controls are implemented for access to Fresenius Kabi information systems.

Access controls to sensitive data in our databases, systems, and environments are set on a need-to-know principle. Furthermore, we grant access permissions only on the principle of least privilege.

Users of information systems are given unique user accounts and passwords, the password requirements are defined and enforced.

We restrict administrator privileges to dedicated administrator accounts.

Virtual private network (VPN) software is provided to our users to enable secure, internet-based remote access to key systems. We also require multi-factor authentication for remote network access.

**Vulnerability and Patch Management**

We strive to apply the latest security patches and updates to operating systems, endpoints, and network infrastructure to mitigate exposure to vulnerabilities.

A patch management process is in place to implement security patch updates as they are released by vendors.

We perform periodic scans of externally exposed and internally assets.

**Penetration Testing**

We have processes established to assess and correct vulnerabilities discovered during bi-annual penetration testing by our qualified and independent pentesting partner Cobalt Labs Inc.

**Incident Response Management**

We have a formalized incident response plan and associated procedures that are triggered in case of a security incident. The incident response plan defines the responsibilities of key personnel and identifies processes and procedures for notification, and escalation. Incident response personnel are trained, and execution of the incident response plan is tested periodically.

We follow the SANS Incident Response Process, an industry standard framework for incident response, to help prepare, identify, prevent, detect, and respond to security incidents. We are supported in this by the Fresenius Cybersecurity Emergency Response Team (CERT).

**Endpoint Protection**

Our endpoints are equipped with a centrally managed antivirus solution to ensure that the latest virus definitions are always available on the endpoints and that consistent security policies are enforced on all endpoints.

All laptops are full disk encrypted with the keys managed using a security vault.

We have configured automatic session locking on enterprise assets after a defined period of inactivity.

Mobile devices are subject to a mobile device management system and access is only permitted from devices configured in accordance with our security policy. This security policy requires a code to be entered to access the device and allows remote erasure if it is reported lost or stolen.

**Network & Email Security**

We perform traffic filtering between network segments.

Only Fresenius Kabi managed wireless networks are permitted within our environment. Wireless access security controls include segregation of corporate and guest access and rotation of wireless keys.

We have deployed a solution that regularly updates URL filtering software that blocks access to inappropriate web sites from its network.

Our email gateways act as barriers that filter malicious traffic and stop the phishing and allow only authentic communications.

**Logging & Monitoring**

Application and infrastructure systems logs are stored for troubleshooting, security reviews, and analysis by authorized personnel. Logs are preserved in accordance with regulatory requirements.

Centralized security event alerting across enterprise assets for log correlation and analysis is implemented. A log analytics platform configured with security-relevant correlation alerts also satisfies this safeguard.

**Employee Training and Awareness**

Fresenius Kabi employees are required to participate in cybersecurity awareness training. For this purpose, we provide various formats to present the topic of cybersecurity and make it simple to understand. Our slogan is "Cybersecurity is a team sport" and in this spirit we regularly strive to inspire our employees with various awareness campaigns, with news articles and blog posts on the topic of security to become an active member in the defense strategy of our company.

Accompanying our security awareness program, every person with access to our IT systems is provided quarterly with phishing simulation tests. The quarterly campaigns support security awareness as they increase everyone’s knowledge and vigilance of phishing emails.

**Physical Security**

Physical access controls are implemented at our offices. Controls include building security and secured access to Fresenius Kabi premises. Proximity card access is required to enter Fresenius Kabi offices and production plants. There are defined procedures for visitor access control, requiring all visitors to report to reception.

If you have any further questions about information security at Fresenius Kabi, we will be happy to answer your questions on this important topic at any time. You can reach us at **Infosec@Fresenius-kabi.com**.