Position on Information Security

Background

In any corporation, information is a critical asset that must be managed and protected; its unauthorized use, disclosure, modification or destruction can adversely impact the corporation's ability to achieve its goals. Information assets can include proprietary product formulas, information used in manufacturing processes, customer data or any information systems required for the proper functioning of the company. In today's advanced technological environment, where more information than ever is stored electronically, information assets are under constant threat from malicious cyberattacks that can disrupt business functions and/or compromise sensitive business information or the security of personal data that the organization is committed to protect. A proactive information security strategy to properly manage information assets and protect against such deliberate, as well as inadvertent, threats is necessary to safeguard any business and its stakeholders.

Relevance

As the largest, most diversified healthcare products company, Johnson & Johnson has a wealth of information to protect. The healthcare sector, with our valuable intellectual property covering multiple patents, ongoing discovery and innovation, is a particular target for cyberattacks. To protect our business and continuity of supply, we must maintain robust capabilities to safeguard our systems and information. In doing so, we also protect our patients and consumers who rely upon our products for their health and well-being.

Guiding principles

As stated in Our Credo: "We believe our first responsibility is to the patients, doctors and nurses, to mothers and fathers and all others who use our products and services. In meeting their needs everything we do must be of high quality." Protecting our Company's most vital information so that we can operate without disruption is one of the ways in which we meet this responsibility.

Our guidelines on protecting information are embedded in Johnson & Johnson's Code of Business Conduct: "Our intellectual property and confidential information are irreplaceable assets. We must secure and protect the use of these valuable assets. Intellectual property includes copyrights, patents, trademarks, product and package designs, brand names and logos, research and development, inventions and trade secrets."

Our position

Johnson & Johnson is fiercely committed to protecting its information assets and business integrity. Our Information Security and Risk Management (ISRM) organization, led by our Chief Information Security Officer, has global reach with a presence in all regions of the world, and provides ongoing security consulting on relevant policies, procedures and requirements to all Johnson & Johnson businesses. ISRM has developed a robust program, which constantly enhances our security capabilities, to safeguard the Company's networks, systems, products and information against evolving cyber threats. The program encompasses people, processes and technology with the following activities:

- **Maintaining an experienced team of seasoned information security professionals** who collectively provide expertise to consult with personnel throughout the Enterprise on the appropriate controls to safeguard all forms of information and data; ensure the Company networks, systems and products are secure; and identify, detect and respond to threats. The team is provided training and education to support the above objectives.
- **Conducting annual, mandatory training** for Company personnel on information security, protection of personnel data, and records management. This training is required both for new users and on an annual cycle for existing users.
- **Conducting periodic security awareness activities and events** around the globe to reinforce cybersecurity principles with employees and other users. Such activities include, for example, mock phishing campaigns across the Company to raise awareness on how to protect against phishing attacks that are routinely used by threat actors.
- **Defining appropriate use of electronic communications** and providing guidance for employees and other users on use of email, internet and social media sites to ensure that sensitive information is appropriately handled and protected.
- **Providing clear direction for all employees on secure information handling.** This includes guidance related to sharing of information externally; transmitting information safely using

appropriate tools and technologies; storing information using safeguards such as encryption where needed; disposal of information in line with Company standards; and much more.

- **Systematically identifying and tracking risks** and taking the necessary risk reduction measures, including steps to improve our information security capabilities and build in preventive and/or detective controls.
- **Supporting continuous improvement in information security** through periodic assessments by independent external experts to assess the maturity of existing controls and the effectiveness of information security systems and processes, and to help drive further improvement.
- **Investing in and implementing information security protection, detection and response capabilities,** using industry-leading technologies, processes and providers across our global infrastructure and operations.
- **Ensuring response and recovery capabilities are in place,** encompassing people, process and technology, to respond to actual or potential security incidents; effectively recover from incidents; escalate incidents to management; and notify authorities of applicable incidents as required by laws and regulations.
- **Maintaining robust security systems for use and processing of personal information,** supported by encryption, anonymization and other relevant measures to ensure that personal information is secured against unauthorized access and disclosure. See also our Position on Data Privacy for further details about how we handle personal information.
- **Extending our information security program throughout our supply chain and product spaces** by evaluating and establishing cybersecurity controls across our manufacturing and distribution environments, and ensuring our products (including connected/wearable medical devices) remain secured throughout their lifecycle. For relevant products we maintain a comprehensive cybersecurity framework encompassing both development and operations.
- **Collaborating within our industry to improve information security on a broad scale.** For example, we partner with the U.S. Food and Drug Administration on guidelines for managing medical device security, and we collaborate with other healthcare companies and organizations on mechanisms to improve the overall industry security posture. ISRM maintains working relationships with peer companies, industry associations and government agencies to share best practices and collaborate on effective solutions to the threats and attack methods faced by both public- and private-sector organizations.

Application

This Position is relevant for the Johnson & Johnson Family of Companies, as detailed in our governance materials. We provide updates relating to information security in our annual Health for Humanity Report.

Last updated: March 2023