



Information Security and Privacy Issue Brief

Importance to Elanco and our Stakeholders

Elanco prioritizes the trust and confidence of our customers and workforce. In today's increasingly sophisticated data environment, protection of company information and electronic assets is vital. Similarly, consumers expect companies to safeguard personal data and effectively manage the collection, processing, storage and sharing of their data – while responsibly using such information to innovate and improve available products and services.

Our Action

Elanco has built a risk-based, fit-for-purpose and innovative information security program. Our Chief Information Security Officer (CISO) leads an information security team that develops and implements strategies and processes to protect the confidentiality, integrity and availability of our information assets. This includes helping prevent, identify and appropriately address cybersecurity threats.

Our information security architecture is designed to accept and embrace the realities of modern working, with a cloud-heavy footprint and extended remote workforce. Our program leverages and aligns with various frameworks and good practices including the National Institute of Standards and Technology (NIST) Cyber Security Framework and other good practice control methods.

Employees play a key role in maintaining our information security. We've invested in a security awareness program that promotes a culture of security via quarterly training and regular security exercises. This culture empowers employees to report suspicious activities through the Protect Elanco and IntegrityLine portals. Additionally, we augment our information security team with strategic cybersecurity partners. We utilize a 24x7 managed detection and response service for escalation of critical events, as well as a risk-based vulnerability management service.

We perform ad hoc monitoring of our vendors and business partners to validate the security of information in our supply chain. We practice cyber resilience through documented incident response plans and associated playbooks based on industry standards, customized for Elanco and our operating environments.

Privacy

Elanco is committed to the ethical management and processing of personal data related to our customers, consumers, employees and other individuals. We are transparent about how we process personal data and are intentional about protecting it – while being respectful of



individuals' privacy rights. We have standards, procedures and policies governing the collection, use, disclosure, transfer, storage and retention of personal data.

Elanco's dedicated Global Privacy Office, led by our Head of Investor Relations and ESG, manages the privacy inquiries of our consumers, customers, employees and any other individual, addresses the Privacy Reviews and ensures compliance with privacy laws and regulations globally. Our [Global Privacy Center](#) explains how we collect, use, disclose, transfer and retain personal data – and provides individuals with information about how to exercise their privacy rights with Elanco.

Metrics and Targets

Information Security metrics are shared regularly with the Elanco Board of Directors and cover the following topics:

- NIST CSF maturity score
- External rating
- Priorities, assets
- Awareness and education
- Detect and respond
- Risks

Governance and Risk Management

The [Audit Committee](#) oversees our program, policies and procedures related to information asset security and data protection as it relates to financial reporting and internal controls – including data privacy and network security. Broad oversight is maintained by our full Board.

The Audit Committee and the full Board regularly receive reports from our CISO on, among other topics, assessments of risks and threats to our systems and processes to maintain and strengthen information security systems. Our CISO also meets twice annually with the Audit Committee and the full Board in executive session without other members of management present.

Additionally, cyber risks are incorporated into our enterprise risk management program and reviewed annually at a full Board meeting.



External Affiliations and Collaborations

Microsoft Security is part of our suite of innovative solutions. Grounded in Zero Trust architecture, this partnership allows us to build a future-forward landscape that supports our innovative teams while also helping secure data and applications.

The content of this brief is informed by global ESG disclosure standards and frameworks.

Updated July 2024