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, the ISO 27000 family of standards, Information Technology Infrastructure Library (ITIL) processes 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. 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 (including NIST 800-61), 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 Global Privacy, 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 & 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 security systems and processes to maintain and strengthen information security systems. Our CISO also meets twice annually with the Audit Committee and the full Board 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 the following ESG disclosure standards:

- Policies and commitments that guide Elanco's approach to the material issue (GRI Disclosure 3-3c)
- Actions taken to respond to the material issue, with a qualitative assessment of how these actions support the 'resilience' of Elanco (IFRS S1 General Requirements Standard)
- Action taken to manage impacts related to the issue (GRI Disclosure 3-3d)
- Targets related to the material issue (IFRS S1 General Requirements Standard, GRI Disclosure 3-3e)
- Processes used to track effectiveness and lessons learned (GRI Disclosure 3-3e)
- Industry associations, other membership associations, and national or international advocacy organizations in which Elanco participates in a significant role (GRI 2-28)