ELANCO INFORMATION SECURITY STANDARD

This Information Security Standard sets forth Elanco Animal Health Incorporated's and its affiliated entities' (collectively, "**Elanco**") information security requirements for Suppliers with respect to the confidentiality, integrity, and availability of Elanco Information (defined below). Any additional Supplier obligations related to Elanco information security under any agreement with Elanco are in addition to the requirements of this Information Security Standard.

I. Definitions

"**Company Information**" means any Elanco confidential or proprietary information, including any information defined as such in any written agreement between Supplier and Elanco.

"**Elanco Information**" encompasses both Company Information and Personal Information.

"**Personal Information**" means any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural, or social identity. "Personal Information" also includes the terms "personal data," "personal information," "sensitive data," "sensitive personal information," and equivalent terms as those terms are defined by applicable data protection laws.

"**Processing**" (and its conjugates, including without limitation, "**processes**," "**processed**," and "**processing**," regardless of whether such terms are capitalized or not) shall mean any operation or set of operations which is performed upon Personal Information, including (without limitation) collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**Supplier Information System**" means an information system that is owned or operated by a Supplier or Supplier's subprocessor(s) that Processes Elanco Information in any format, including, but not limited to (a) systems; (b) cloud environments; (c) electronic assets and devices; and (e) hard copy versions.

II. Requirements

Supplier shall ensure the confidentiality, integrity, and availability of Elanco's Information by maintaining a comprehensive written information security program. The comprehensive written information security program shall be reviewed and updated as necessary, on no less than an annual basis, or upon a material change in services provided, and shall utilize at least the following minimum safeguarding requirements, controls, and procedures (collectively, the "**Minimum Safeguards**"):

1. Limit access to and Processing of Elanco Information to authorized users and Supplier Information Systems:

    a. Identify and authenticate the identities of authorized users as a prerequisite to allowing access to Supplier Information Systems;
    b. Limit Supplier Information System access to trained, authorized users that have a business need to know to perform job duties, with password strength requirements that meet common

security standards (*e.g.*, ISO, NIST); and

c. Provide periodic training to Supplier personnel that covers general information security and safe data processing practices.

2. Limit physical access to Supplier Information Systems, devices, equipment, and their respective operating environments:

    a. Escort visitors and monitor visitor activity, maintain audit logs of physical access, and control and manage physical access to devices;
    b. Maintain physical controls for data centers, with access formally managed based on business need; and
    c. Maintain environmental controls for data centers (*e.g.*, temperature, humidity, power backup).

3. Monitor, control, and protect Elanco Information at the external boundaries and key internal boundaries of Supplier Information Systems, including:

    a. Harden operating systems, applications, and network devices, such as via intrusion detection, anti-virus, and anti-malware;
    b. Patch operating system and major component updates upon security-related patch release and evaluation in accordance with common security standards (*e.g.*, ISO, NIST);
    c. Prohibit authentication of network resources, platforms, devices, services, workstations, and applications by default passwords;
    d. Where reasonable, implement role-based access control, single sign-on and federated identity management, and multi-factor authentication;
    e. Perform and document logging activities in accordance with common security standards (*e.g.*, ISO, NIST);
    f. Encrypt data in transit with encryption procedures and practices that meet common security standards (*e.g.*, ISO, NIST);
    g. Allow storage and transfer of Elanco Information using removable storage devices only through a documented process;
    h. Perform periodic scans of Supplier Information Systems and real-time scans of files from external sources as files are downloaded or opened;
    i. Regularly back up Supplier Information Systems and data, appropriately secure back up storage from loss, damage, and unauthorized access, and periodically test back up storage for security and viability; and
    j. Document privileged administrative user accounts as different than standard user accounts.

4. Supplier shall document, implement, and maintain all appropriate legal, operational, technical, and organizational measures to protect against a Data Security Breach (as defined in the Data Processing Agreement). Supplier shall regularly test or otherwise monitor the effectiveness and resilience of its data security controls, systems, and procedures.

5. Supplier shall maintain documented and operational business continuity and/or disaster recovery plans, as reasonably appropriate in the context of the services provided.

6. Supplier shall retain Elanco Information only for as long as specified within the applicable agreement, except to the extent that a longer retention period is required by applicable law or

regulations. At the conclusion of the engagement, Supplier must return or destroy Elanco Information, per Elanco's choice, using asset disposal controls that meet common security standards (*e.g.*, ISO, NIST).

7. Supplier shall maintain a third-party risk management program that, at minimum, shall require compliance with the Minimum Safeguards by Supplier's subprocessors that Process Elanco Information.

8. To the extent Supplier builds or supplies systems, software, or applications for Elanco:

    a. Implement a defined Systems Engineering methodology that is aligned to industry standards and managed via appropriate policies and procedures; and
    b. Implement a defined change/release management procedure for planned software changes and bug fixes.