Section 1: Purpose

This Information Security Standard (or "Standard") sets forth Eli Lilly and Company's and its Affiliates ("Lilly") information security requirements for third parties/suppliers (each, a "Supplier") with respect to the Confidentiality, Integrity, and Availability of information (defined below). Any additional Supplier obligations related to information security under any agreement with Lilly are in addition to the requirements of this Information Security Standard. These commitments apply to Supplier and its Personnel.

For clarification, this Information Security Standard applies to all information handled by a Supplier including, handling by: (i) creating; (ii) editing; (iii) managing; (iv) processing; (v) accessing; (vi) receiving; (vii) transferring; (viii) destroying; (ix) storing; or (x) hosting, in any format, including, but not limited to: (a) systems; (b) cloud environments; (c) production and non-production environments; (d) electronic assets and devices (including company-provided and "bring your own device"); and (e) hard copy versions.

Section 2: Definitions

The definitions below are for the purposes of this Standard. Any capitalized terms not defined shall take the meaning ascribed to them in the Agreement.

a. **"Personnel"** means Supplier's employees, agents, subcontractors, and other authorized users of its systems and network resources.
b. **"Confidentiality, Integrity, and Availability"** refers to the three properties of the information-security model known as the "CIA Triad." Confidentiality is the property that data or information is not made available or disclosed to unauthorized persons or processes. Integrity is the property that data or information have not been altered or destroyed in an unauthorized manner. Availability is the property that data or information is accessible and useable upon demand by an authorized person.
c. "**Physical, Administrative, and Technical Safeguards**" refers to the controls an organization implements to maintain information security. Physical safeguards address physical measures, policies, and procedures to protect electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion. Administrative safeguards address administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic data or information and to manage the conduct of Personnel in relation to the protection of that data or information. Technical safeguards address the technology, and the policies and procedures for its use, that protect electronic data or information and control access to it.
d. "**Process**" means to perform any operation or set of operations on data, such as access, use, collection, receipt, storage, alteration, transmission, dissemination or otherwise making available, erasure, or destruction.
e. **"Security Incident"** means (i) any confirmed or reasonably suspected compromise of the Confidentiality, Integrity, or Availability of Lilly Information; (ii) any compromise of, or unauthorized access to, any system that Processes Lilly Information that presents a risk to the Confidentiality, Integrity, or Availability of Lilly Information; or (iii) receipt of a complaint, report, or other information regarding the potential compromise or exposure of Lilly Information Processed by Supplier.

Section 3: Permitted Purposes

1. **Authorized processing:** Supplier may only Process Lilly Information as follows (each a "Permitted Purpose"):
    a. As expressly authorized under the Agreement; or

b. If there is no express authorization, only as strictly necessary to perform the services under the Agreement.

2. **Authorized data:** Supplier may only Process Lilly Information necessary for a Permitted Purpose.
3. **Sale or other transfer prohibited:** Supplier must not transfer, barter, trade, sell, rent, loan, lease, or otherwise distribute or make any Lilly Information available to any third party.
4. **Data aggregation prohibited:** Supplier must not aggregate Lilly Information, even if anonymized or pseudonymized, except as expressly authorized under the Agreement.

Section 4: General Security Requirement

1. **General security requirement:** Supplier must establish and maintain Physical, Administrative, and Technical Safeguards consistent with industry-accepted best practices (such as the International Organization for Standardization's standards ISO 27001 and 27002, the National Institute of Standards and Technology (NIST) Cybersecurity Framework, or other similar industry standards for information security) to protect the Confidentiality, Integrity, and Availability of Lilly Information.
2. **Written Security Program:** Supplier must implement a written information security program, including appropriate policies, procedures, and risk assessments for implementing the Physical, Administrative, and Technical Safeguards. The written information security program must be reviewed and approved by senior management on an annual basis. The program must be applicable to the Supplier's employees, agents, subcontractors, and suppliers.
3. **Specific security requirements:** In addition to the above requirements, Supplier must implement the specific Physical, Administrative, and Technical Safeguards listed below in the following sections of this Standard.
4. **Security Training Program:** Supplier must conduct periodic security training sessions for its Personnel on relevant threats and business requirements.
5. **Vendor assessment questionnaires.** Upon Lilly's request, Supplier will complete a new Lilly cybersecurity risk assessment questionnaire.

Section 5: Identity and Access Controls

1. **Unique User Identification:** Supplier will assign a unique ID to each individual accessing information, including accounts with privileged access. Accounts with access to Lilly Information must not be shared.
2. **Access Control:** Supplier will implement rigorous access controls consistent with best practices, including granting access strictly based on the individual's need to know and the principle of least privilege.
3. **Privileged Account Management:** Supplier will manage and monitor the use of administrative privileges and privileged accounts on computers, networks, and applications consistent with industry best practices, including revoking privileged access when no longer needed and separating privileged accounts from standard user accounts.
4. **Multi-Factor Authentication (MFA):** Supplier will implement multi-factor authentication for all systems that process Lilly Information.
5. **Password Management:** For accounts that have access to Lilly Information, Supplier will implement password management policies consistent with industry best practices.
6. **User Access Reviews:** Supplier will regularly review and validate the necessity and appropriateness of access rights to Lilly Information, with a frequency that reflects the sensitivity of the information accessed.
7. **Account and Session Lockout:** Supplier will implement account and session lockout policies to deter unauthorized access attempts, including disabling accounts or sessions after a predetermined number of failed login attempts.
8. **Notification:** Supplier will notify Lilly within 24 hours of changes to Personnel who have access to Lilly systems.

Section 6: System Security and Integrity

1. **Secure Configuration and Hardening**: Supplier will manage security settings and configurations of its systems, including endpoints, consistent with industry best practices to protect Lilly Information from exploitation through vulnerable services and settings.
2. **Vulnerability and Patch Management:** Supplier will ensure the timely application of security patches and updates across all systems and applications, including quickly identifying vulnerabilities to patch and prioritizing remediation of high-risk vulnerabilities.
3. **Disablement of services:** Supplier will disable all non-essential services, protocols, and ports. Services that are authorized must be clearly documented with a rationale for their use along with a formally documented justification and management approval.
4. **Network Security and Malware Protection:**
    a. Supplier will implement firewall policies and configure intrusion detection/prevention systems to monitor and control both inbound and outbound network traffic.
    b. Supplier will deploy and maintain anti-malware solutions on all workstations and servers within Supplier's network.
    c. Supplier will regularly review and update firewall configurations to ensure that all firewall rules are justified by valid business needs.

Section 7: Security Management

Supplier will implement an integrated Security Management approach that ensures comprehensive oversight and management of security risks, including:

1. **Audit Log Management, Monitoring, and Analysis:** Supplier will collect, manage, retain, and analyze audit logs (including continuous monitoring) to detect, investigate, mitigate, and recover from unauthorized activity that may impact Lilly Information. Logs must be retained for at least 18 months. In environments where resources are shared (such as in a SaaS model), Supplier will tag all logs with a distinct identifier for Lilly implementations and supply this data to Lilly upon request.
2. **Penetration Test:** Supplier will conduct penetration tests on networks and applications that handle information, at least every two years.
3. **Change Management:** Supplier will maintain a formal change management process, ensuring all changes are documented, reviewed, and approved according to a structured protocol that includes segregation of duties and emergency change procedures.

Section 8: Data Security

1. **Suitable Environment:** Supplier will Process Lilly Information only in environments that are designed and configured to ensure the Confidentiality, Integrity, and Availability of the Lilly Information, including secure storage and data protection policies and appropriate physical security measures. Production data will not be used on test systems or equipment and test data will not be used on production systems or equipment.
2. **Data Segregation:** Supplier will implement logical (and physical, where applicable) measures to isolate Lilly Information from the information of the Supplier, its other customers, and any third parties at all times.
3. **Encryption Standards:** Supplier will encrypt all Lilly Information at rest and when in transit in accordance with industry best practices. Encryption is required for data at rest regardless of storage medium, including fixed and portable or removable storage.

4. **Data Inventory Management:** Supplier will establish and maintain a detailed inventory of all Lilly Information that it Processes, including systems and assets that process Lilly Information.

Section 9: Record Retention, Return and Destruction

1. **Retention.** Supplier will retain Lilly Information only as necessary for the Permitted Purposes.
2. **Return and secure deletion of Lilly Information.** At any time during the term of the Agreement at Lilly's request, or upon the termination or expiration of the Agreement for any reason, Supplier will, within 30 days, return to Lilly and securely delete all copies of Lilly Information in its possession or control. Supplier will confirm in writing that all copies of Lilly Information have been returned and/ or securely deleted.
3. **Archival copies.** If Supplier is required by law to retain archival copies of Lilly Information for tax or similar regulatory purposes, Supplier will (i) not use the archived information for any other purpose; and (ii) remain bound by its obligations under the Agreement, including, but not limited to, its obligations to protect the information using appropriate Physical, Administrative, and Technical Safeguards and to notify Lilly of any Security Incident.
4. **Deletion standard.** Supplier will securely destroy all Lilly Information designated for deletion using an industry accepted and approved method designed to prevent data from being recovered using standard disk and file recovery utilities (e.g., secure overwriting, degaussing of magnetic media in an electromagnetic flux field of 5000+ GER, shredding, or mechanical disintegration). With respect to Lilly Information encrypted in compliance with this Standard, Supplier may delete information by permanently and securely deleting all copies of the encryption keys.
5. **Media destruction.** Before permanently discarding or disposing of storage media that (1) Supplier has physical access to or control of (e.g., laptop hard drives, desktop hard drives, USB or "thumb" drives, backup media, hard drives used in the Supplier's own data center, or other portable storage media) and (2) contains, or has at any time contained, Lilly Information, Supplier will destroy the storage media using a technique designed to render the media unusable and the information unrecoverable (e.g., disintegration, incineration, pulverizing, shredding, and melting). This section does not apply to storage media that Supplier does not have physical access to or control of, such as storage media used in a public cloud or other third-party environment. In such cases, Supplier will ensure that all Lilly Information stored in the third-party environment is securely deleted when no longer needed using an industry-accepted practice (see Section 9.4, Deletion standard).

Section 10: Information Security Incident Response, Management and Reporting

1. **Incident response.** Supplier will have incident response procedures for detection, investigation, response, mitigation, and notification of Security Incidents. These incident response procedures must be documented, tested, and reviewed at least annually. Supplier will provide the procedures to Lilly upon request.
2. **Incident response plan**. Supplier will maintain a written incident response plan and provide a copy of the plan to Lilly upon request. Supplier will remedy each Security Incident in a timely manner following its response plan and industry best practices.
3. **Notice required**. Supplier will notify Lilly of any Security Incident within 48 hours of becoming aware of the Security Incident by sending email to Cyber@Lilly.com. The notification will include information necessary for Lilly to understand the impact of the incident, including but not limited to the following information, to the extent known: the nature of the Security Incident, a description of the Lilly Information impacted by the Security Incident, and actions Supplier is taking to respond to the Security Incident.
4. **Cooperation with Lilly's investigation**. Supplier will reasonably cooperate with Lilly in Lilly's handling of a Security Incident, including, without limitation: (i) coordinating with Lilly on Supplier's response plan; (ii) assisting with Lilly's investigation of the Security Incident; (iii) facilitating

interviews with Supplier's Personnel and others involved in the Security Incident or response; and (iv) making available all relevant records, logs, files, data reporting, forensic reports, investigation reports, and other materials required for Lilly to comply with applicable laws, regulations, or industry standards, or as otherwise requested by Lilly.

5. **Third-party notifications**. Supplier agrees that it will not notify any third party (including any regulatory authority or customer) of any Security Incident without first obtaining Lilly's prior written consent. Further, Supplier agrees that Lilly shall have the sole right to determine: (i) whether notice of the Security Incident is to be provided to any individuals, regulators, law enforcement agencies, or others; and (ii) the form and contents of such notice.

Section 11: Secure System Development Life Cycle

Suppliers will adhere to documented Secure Software Development Life Cycle (SSDLC) industry best practices for all systems, software, or applications that process Lilly Information throughout all stages of their development lifecycle, including planning, analysis, design, implementation, testing, deployment, and maintenance.

Section 12: Remediation

In any instance where the Supplier and Lilly agree in writing to cybersecurity-related remediations with respect to Supplier's obligations under this Standard ("Remediation(s)"), Supplier will provide status updates on a periodic basis (in no case less often than once every 15 business days) or as otherwise agreed in advance and in writing between the parties (email accepted), detailing the progress and completion of any Remediations identified. Supplier shall also provide documentary evidence demonstrating the successful closure and resolution of each agreed-upon Remediation within 120 business days of agreement on the applicable Remediation. Failure to provide such documentary evidence shall be considered a material breach of this Agreement.