Information Security Standard

This Information Security Standard sets forth Eli Lilly and Company's ("Lilly") information security requirements for third parties/suppliers (each, a "Third Party/Supplier") with respect to the confidentiality, integrity and availability of Information (defined below). Any additional Third Party/Supplier obligations related to information security under any agreement with Lilly are in addition to the requirements of this Information Security Standard.

As used herein, "Information" encompasses both Confidential Information and Personal Information that is used for business purposes (hereinafter independently and/or collectively referred to herein as "Information"). Personal Information means any information as defined in Lilly's Supplier Privacy Standard. Confidential Information means any confidential or proprietary information as defined as such (or with a similar designation) in any written agreement between Third Party/Supplier and Lilly.

For clarification, this Information Security Standard applies to all Information handled by a Third Party/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.

1. **Information Security Policies and Procedures:**

Third Party/Supplier must have and comply with documented information security polices, standards and procedures to establish its control environment related to the protection of confidentiality, integrity and availability of Information. Policies and procedures must be reviewed, updated, and approved by senior management on an annual basis.

If the use of personal devices to access Information or systems is allowed by Third Party/Supplier, a "bring your own device" policy must be implemented.

2. **Governance and Training:**

Third Party/Supplier personnel must complete relevant information security training with requirements for protection and secure handling of Information. A summary of completed training must be made available upon request.

Third Party/Supplier shall provide a representative as a single point of contact for all information security related items. In addition, the Third Party/Supplier shall have a representative assigned who is responsible for overseeing compliance with this Information Security Standard.

3. **Human Resources Security Practices:**

Pre-employment screenings, including criminal background checks (where permitted under local law), review of curriculum vitae or resume, review of credentials and experience, and interviews must be conducted prior to hiring.

Confidentiality, non-disclosure or equivalent agreements must be in place for all employees. Agreements include but are not limited to:

a. Confidentiality obligations post-employment/engagement.
b. Provisions governing acceptable use of electronic resources including but not limited to using electronic resources in a professional, lawful and ethical manner.

Processes must be in place to identify and collect assets (physical and electronic) from individuals when exiting the company or for those who no longer require access.

4. **Access to Information:**

Third Party/Supplier must have at a minimum the following account activation controls in place when Third Party/Supplier has Information belonging to or entrusted to Lilly that resides outside Lilly's environment and/or when Third Party/Supplier has a remote access connection to Lilly's environment:

a. A formal approval process to grant access based on having a business need to perform job duties (i.e., least privilege, meaning the level of access needed but not more).
b. Segregation between request, approval and granting of access.
c. User accounts for access to systems, services and applications must be assigned to individual users and not shared.
d. Privileged and/or administrative user accounts must be different than the standard user account and have unique user login ID's. Privileged accounts (elevated level of access, which grants powers within a computer system, which are significantly greater than those available to the ordinary user) must be restricted and only assigned to authorized users.

Password controls must be appropriately implemented by Third Party/Supplier, including the following requirements:

a. History and periodic expiration.
b. Temporary passwords securely communicated and prompted to change after first use.
c. Change passwords immediately when there is reason to believe an account has been compromised.
d. Shared system, service, and application accounts' passwords must be changed when anyone who knows the password, either leaves the Third Party/Supplier or changes to a different position that no longer requires the access.
e. User's identity must be verified before a password is reset.
f. All default passwords must be changed from default values.
g. Password strength requirements must meet common security standard (e.g. ISO, NIST) length and complexity.

The following deactivation controls must be in place for Third Party/Supplier:

a. A formal process for timely deactivating accounts of those exiting and/or those who no longer have a business need to have access (e.g., within 24 hours of termination).
b. Process to ensure notification to Lilly of Third Party/Supplier personnel changes, within 24 hours, when those personnel have accounts or are granted access to Lilly information systems.

The following access controls must be implemented by Third Party/Supplier:

a. Periodic access reviews of all users, system accounts, test accounts, and generic accounts must be performed and documented at least annually.
b. User accounts must be locked out after a defined number of failed attempts.
c. Accounts without recent activity (e.g., the last 90 days, with the exception of those only used for quarterly, semi-annual and annual processing) must be disabled.
d. Session controls, including account lockout and session timeout must be in place.
e. Multi-factor authentication (MFA) must be in place for any privileged and/or administrative accounts.
f. MFA must be in place for any applications that are internet facing.
g. MFA must be in place for any remote access methods (e.g., virtual private networks, remote desktop protocols).

5. **Network and System Security:**

Third Party/Supplier must have, at a minimum, the following network and system security controls in place when Third Party/Supplier has Information belonging to or entrusted to Lilly that resides outside Lilly's environment and/or when the Third Party/Supplier has a remote access connection to Lilly's environment:

a. Hardening standards for operating systems, applications, and network devices.

b. All systems must be patched for operating system and major component updates upon security related patch release and evaluation in accordance with common security standards (e.g., ISO, NIST).

    - High risk vulnerabilities for internet facing applications must be patched as soon as possible but not to exceed 30 days.

c. Systems must be maintained at levels to allow the latest security patches/service packs to be applied.

Network Security Controls:

a. Information belonging to or entrusted to Lilly must not be stored in a demilitarized zone (DMZ).
b. Firewall policies must be implemented on all networks interfaces that restrict inbound and outbound traffic based on need.
c. Intrusion detection or intrusion prevention systems must be implemented to detect and respond to unauthorized or malicious network traffic.
d. If an availability service level agreement exists on a system or application between Lilly and Third Party/Supplier, Distributed Denial of Access (DDoS) protection is in place.

Systems Security Controls:

a. Endpoint devices must be encrypted and secured with a password.
b. Mobile endpoints (smartphones, tablets) must be secured using a mobile device management system.
c. Servers and endpoints must be secured using virus/malware protection that are kept up to date.

6. **Logging and Monitoring:**

Logging activities must be documented and performed in accordance with common security standards (e.g., ISO, NIST). Monitoring should minimally identify cybersecurity events and verify the effectiveness of protective measures.

7. **Threat and Vulnerability Management:**

Third Party/Supplier shall have continuous vulnerability assessment and timely remediation process for application, operating system and other infrastructure components. In addition, services and processes shall be designed to identify, assess, mitigate, and protect against new and existing security vulnerabilities and threats, including viruses, bots, and other malicious code.

Third Party/Supplier must have the following controls in place:

a. Annual independent penetration tests on its networks and applications that handle Information.
b. Quarterly vulnerability scans must be performed on its platforms and networks that handle Information to ensure alignment with common security standards specifically related to system hardening.
c. A risk-based remediation program to timely resolve findings from penetration tests, vulnerability scans and compliance assessments.
d. As needed, Third Party/Supplier will work to accommodate Lilly's network penetration test requests

8. **Change Management:**

Third Party/Supplier shall implement a documented change control policy that includes:

a. Approval, classification, testing, and back out plan requirements.
b. Segregation of duties among request, approval, and implementation.
c. Management and review of emergency changes within a fixed time period (e.g., 24 hours).

9. **Asset Management:**

Third Party/Supplier must maintain an asset inventory, including system/device and software assets when Third Party/Supplier has Information belonging to or entrusted to Lilly that resides outside Lilly's environment and/or when Third Party/Supplier has a remote access connection to Lilly's environment.

The Third Party/Supplier must have asset disposal controls in place to ensure Information (hard copy and electronic) is disposed of according to common security standards (e.g. ISO, NIST) and applicable legal requirements when no longer needed, and documented evidence of proper disposal must be maintained.

10. **Information Handling:**

Third Party/Supplier must ensure physical or logical separation of Information from other customer information and Third Party/Supplier's own information when Third Party/Supplier has Information belonging to or entrusted to Lilly that resides outside Lilly's environment. In addition, Third Party/Supplier must be able produce a description of the flow of Information throughout their environments.

Electronic exchanges of Information between Lilly and the Third Party/Supplier (including email, file transfer, remote connectivity, etc.) must be secured using mutually agreed services.

Processes and tools shall be used to prevent, detect, and respond to Information loss.

Information must not be stored or transferred using removable storage devices without approval documented through the Lilly business owner (obtained through the Lilly removable storage request process). If such devices are utilized, all Information stored on the device must be encrypted.

11. **Encryption:**

Encryption is required for Information in transit when Third Party/Supplier has Information belonging to or entrusted to Lilly that resides outside Lilly's environment.

Encryption keys owned or managed by the Third Party/Supplier must be stored in a secure location separate from the location where Information is stored with access managed, along with demonstrated key recovery capability.

Encryption procedures and practices shall meet common current security standards (e.g. ISO, NIST).

12. **Physical Security:**

Process and physical controls shall be established and enforced to protect hard copies and information systems (e.g., hardware, software, documentation, and data) when Third Party/Supplier has Information belonging to or entrusted to

Lilly that resides outside Lilly's environment and/or when the Third Party/Supplier has a remote access connection to Lilly's environment.

Data centers must be under physical control, with access formally managed based on business need. Data Centers must have environmental controls (temperature, humidity, power backup) to prevent disruptions or loss.

Annual independent physical security assessment of facilities shall be required for Third Parties/Suppliers that transmit, store, or process Information.

13. **Resiliency / Continuity of Business / Information Backup and Recovery:**

In addition to any agreement requirements for business continuity and disaster recovery in the event of a disaster or interruption in line with contractual business requirements and criticality of the Information, the Third Party/Supplier shall ensure the following controls are in place.

Redundant power and processing capability must exist within the primary data processing facility.

Ensuring an alternate processing site must be available to continue business processes and recover Lilly functionality within the specified time window of the agreement, if applicable.

Annual Resiliency testing to demonstrate effective business continuity and recovery ability must be in place.

Applicable systems and data must be backed up regularly based on criticality. Backups must be tested for viability on a periodic basis.

Backup tapes and/or transmissions must be appropriately secured and segregated from primary storage.

14. **Record Retention and Destruction:**

Third Party/Supplier shall retain 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 the Third Party/Supplier must return, delete or securely destroy Information as instructed by Lilly.

At the request of Lilly, the Third Party/Supplier must certify that Information has been destroyed as instructed.

15. **Information Security Incident Response, Management and Reporting:**

Third Party/Supplier must have security incident (e.g., exposure, breach, theft, etc.) management and response procedures that allow for reasonable detection, investigation, response, mitigation and notification of events that involve a threat to the confidentiality, integrity and/or availability of Information when Third Party/Supplier has Information belonging to or entrusted to Lilly that resides outside Lilly's environment and/or when the Third Party/Supplier has a remote access connection to Lilly's environment. The incident response and management procedures must be documented, tested, and reviewed at least annually. Lilly shall have the option to review such procedures upon request.

Third Party/Supplier shall notify Lilly within 24 hours of suspected or known security incidents that have potential impact to Information. In addition, Third Party/Supplier shall have a documented process, with defined Lilly and Third Party/Supplier contacts, to ensure compliance with this notification requirement.

The Third Party/Supplier shall fully cooperate with Lilly to understand the situation, root cause and determine necessary remediation in the event of an actual or suspected security incident.

16. **Subcontractor Management:**

This Information Security Standard shall apply to all subcontractors utilized by the Third Party/Supplier that handle Information belonging to or entrusted to Lilly that resides outside Lilly's environment and/or when the Third Party/Supplier has remote access connection to Lilly's environment. It is the responsibility of the Third Party/Supplier to ensure the Information Security Standard is communicated to and complied with by each subcontractor. For the avoidance of doubt, subcontractors include, but not limited to: reprographics third parties/suppliers, off-site storage third party/supplier, software developers, cloud hosting facilities and data center facilities.

Formal contracts between Third Party/Supplier and subcontractors must be executed that outline the controls to be provided, including controls to maintain the confidentiality, availability, and integrity of Information.

Initial and on-going assessments must be conducted to ensure subcontractors are adhering to the Information Security Standard and security incidents and problems are managed appropriately.

Third Party/Supplier must inform Lilly and obtain written approval prior to the use of subcontractors who will either handle Information or have access to Third Party/Supplier or Lilly systems in which such Information resides, as well as the country location(s) where any Information will be handled.

17. **Information Security Review Rights:**

Third Party/Supplier shall allow Lilly and its agents, auditors (internal and external), regulators, and other representatives to inspect, audit, examine, and review the facilities, books, systems, records, access rosters, data, practices and procedures of the Third Party/Supplier (and any subcontractors that the Third Party/Supplier may use) to verify the integrity of Information and to monitor compliance with this Information Security Standard.

18. **System Development Life Cycle:**

These requirements will be applicable only for Third Parties/Suppliers building systems, software or applications for Lilly.

Software Development Engineering Methodology:

a. A defined systems development methodology must be formally implemented with policies, procedures and standards communicated and followed and must be aligned to industry standards. Programming standards must be developed and communicated to relevant workforce members. The standards include architecture and design specifications, business logic review, adoption of secure algorithms and libraries, removal of test code, and the remediation of common security flaws (e.g., OWASP top ten vulnerabilities).
b. Code reviews must be performed to confirm adherence to the foregoing programming standards.
c. The use of production data in non-production environments must be only done when necessary and the same security controls must be in place that exist in the production environment, or the production information used in testing must be sufficiently obfuscated.

d. Software that is available in the public domain (e.g., Open-source software, shareware, freeware), if used, must be appropriately scrutinized for potential risk, including potential legal risk (e.g., copyright violation).
e. Software that is available in the public domain (e.g., Open-source software, shareware, freeware), if used, must include controls to ensure that the introduction of this type of software will not have a negative impact (e.g. virus, Trojan horse, security breaches such as "backdoor").
f. Source code must be maintained in an industry-accepted, non-public version control tool, with strict controls related to source code checkout. The Third Party/Supplier must have monitoring systems that monitor changes of environment code.
g. Manage the security lifecycle of all in-house developed and acquired software

Code Release:

a. Third Party/Supplier shall seek continuous improvement on their chosen model of development.
b. The Third Party/Supplier must have a formal change/release management policy/procedure for planned software upgrades which demonstrates that releases are planned, managed, tested, approved, and communicated appropriately, and Lilly shall be notified in advance of scheduled changes.
c. Change/release management cycles begin with requirements definition. Lilly impact, feedback and need must be appropriately factored into the requirements of planned releases.
d. Regression testing must be performed during each release cycle. Testing must be conducted at various levels. (e.g., unit, integration and system, user). User testing must be based on formal test plans, performed by independent parties to those designing and developing the system.
e. Formal approvals must be captured at each stage of the development lifecycle (Requirements, Design, Testing, User Acceptance, Production rollout, etc.). When approvals are captured, it must be clear who is approving, the date they are approving, and what they are approving.
f. Releases and patches must be provided with sufficient instructions for deployment and/or use. This includes those solutions where Lilly is provided the release or patch to apply itself, as well as those where Lilly is notified of a change that the Third Party/Supplier has applied in a Lilly environment.
g. System designs must be formally created to assist in translating requirements to code.

Interim Changes/Bug Fixes:

a. A formal procedure for implementing emergency/bug fix changes, including those to address security vulnerabilities, must be in place to confirm that these changes can be made in a timely yet controlled manner
b. A formal process must be in place to communicate known bugs or defects to Lilly.
c. Bug fix changes must be formally tested and demonstrate proper documentation and approvals. Approval must be granted by someone other than the individual(s) making the change.