情報セキュリティ基準

1. **目的**:

本情報セキュリティ基準（または「本基準」）では、情報（以下に定義）の機密性、完全性、および可用性に関する、社外の第三者／取引業者（以下「サプライヤー」）を対象としたイーライリリー・アンド・カンパニー及びその関連会社（総称して「リリー」）の情報セキュリティ要件を定める。リリーとの何らかの合意の下、情報セキュリティに関連してサプライヤーに課される追加義務は、本情報セキュリティ基準の要件に追加される。これらの義務は第三者／取引業者およびその従業員に適用される。
なお、本情報セキュリティ基準は、サプライヤーによって以下のように取り扱われるすべての情報に適用される：（i）作成、（ii）編集、（iii）管理、（iv）処理、（v）アクセス、（vi）受領、（vii）転送、（viii）破棄、（ix）保存、（x）ホスティング。 また、あらゆる形式のものが対象であり、次に挙げるものに限定されない：（a）システム、（b）クラウド環境、（c）本番および非本番環境、（d）電子資産およびデバイス［会社提供および個人所有を含む］、（e）ハードコピー。

2. **定義**:

以下の定義は、本基準の目的のためのものである。定義されていない太字の用語は、本契約で定義された意味を持つものとする。

a. **「従業員」**とは、サプライヤーの従業員、代理人、下請け業者、およびそのシステムおよびネットワークリソースのその他の認可されたユーザーを指します

b. **「機密性、完全性、および可用性」**とは、「CIA トライアド」として知られる情報セキュリティモデルの 3 つの特性を指します。機密性は、データまたは情報が認可されていない人物またはプロセスに対して利用可能とならないまたは開示されない特性です。完全性は、データまたは情報が認可されていない方法で変更または破壊されていない特性です。可用性は認可された人物が要求したときにデータまたは情報がアクセス可能で使用可能である特性です。

c. **「物理的、管理的、および技術的な保護手段」**とは、組織が情報セキュリティを維持するために実施する管理措置を指します。物理的保障手段は、電子情報システム及び関連する建物・設備を、自然・環境上の危険及び不正侵入から保護するための物理的措置、方針及び手続を指します。管理的保障手段は、電子データまたは情報を保護するためのセキュリティ手段の選択、開発、実施、維持を管理し、当該データまたは情報の保護に関連する従業員の行動を管理するための管理上の行動、方針、手続を指します。技術的保障手段は、電子データまたは情報を保護し、それへのアクセスを管理するための技術、およびその使用に関する方針と手続を指します。

d. **「処理」**とは、データに対してアクセス、使用、収集、受信、保管、変更、送信、普及もしくはその他の方法で利用可能にする行為、消去、または破壊するなどの操作または操作セットを実行することを指します。

e. **「セキュリティインシデント」**とは、(i) リリー情報の機密性、完全性、または可用性に対する確認された、または合理的に疑われる侵害、(ii) リリー情報を処理するシステムへの侵害または不正アクセスで、リリー情報の機密性、完全性、または可用性にリスクをもたらすもの、または(iii) サプライヤーが処理するリリー情報の潜在的な侵害または脆弱性に関する苦情、報告、その他の情報の受領を意味します。

3. **許可された目的**:

1) **認可された処理**：サプライヤーは以下の方法でのみリリー情報を処理することができます（各「許可され

た目的」）。

a. 契約の下で明示的に許可されている場合。

b. 明示的な認可がない場合、契約書に基づくサービスを実行するために厳密に必要な場合。

2) **認可されたデータ**：サプライヤーは許可された目的に必要なリリー情報のみを処理することができます。

3) **販売またはその他の転送の禁止**：サプライヤーは、リリー情報を第三者に転送、交換、取引、販売、賃貸、貸与、リース、またはその他の方法で配布または提供してはなりません。

4) **データの集約の禁止**：サプライヤーは契約の下で明示的に許可されている場合を除き、匿名化または仮名化されている場合でも、リリー情報を集約してはなりません。

4. **一般的なセキュリティ要件**：

1) **一般的なセキュリティ要件**：サプライヤーはリリー情報の機密性、完全性、および可用性を保護するために、業界で受け入れられているベストプラクティス（国際標準化機構の ISO 27001 および 27002 標準、米国国立標準技術研究所（NIST）サイバーセキュリティフレームワーク、またはその他の類似の業界標準）に従った物理的、管理的、および技術的保護手段を確立し、維持する必要があります。

2) **書面によるセキュリティプログラム**：サプライヤーは物理的、管理的、および技術的保護手段を実施するための適切なポリシー、手順、およびリスク評価を含む書面による情報セキュリティプログラムを実施する必要があります。書面による情報セキュリティプログラムは、毎年、上級管理職によってレビューおよび承認される必要があります。このプログラムは、サプライヤーの従業員、代理人、下請業者、およびサプライヤーに適用される必要があります。

3) **特定のセキュリティ要件**：上記の要件に加えて、サプライヤーはこの基準の以下のセクションに記載されている特定の物理的、管理的、および技術的保護手段を実施する必要があります。

4) **セキュリティトレーニングプログラム**：サプライヤーは、従業員に対し、関連する脅威およびビジネス要件に関する定期的なセキュリティトレーニングセッションを実施する必要があります。

5) **ベンダー評価アンケート**：リリーの要求に応じて、サプライヤーはリリーのサイバーセキュリティリスク評価アンケートを完了します。

5. **アイデンティティとアクセスコントロール**：

1) **ユーザーの一意識別**：サプライヤーは情報にアクセスする各個人に一意の ID を割り当てます。これには、特権アクセスを持つアカウントも含まれます。リリー情報にアクセスするアカウントは共有してはなりません。

2) **アクセス制御**：サプライヤーは個人の知る必要性と最小特権の原則に基づいてアクセスを厳格に制御する、ベストプラクティスに従ったアクセス制御を実施します。

3) **特権アカウント管理**：サプライヤーは業界のベストプラクティスに従って、コンピュータ、ネットワーク、およびアプリケーション上の管理特権および特権アカウントの使用を管理および監視します。特権アクセスが

不要になった場合は、特権アクセスを取り消し、特権アカウントを標準ユーザーアカウントから分離します。

4) **多要素認証（MFA）**：サプライヤーはリリー情報を処理するすべてのシステムに対して多要素認証を実施します。

5) **パスワード管理**：リリー情報にアクセスするアカウントに対して、業界のベストプラクティスに一致するパスワード管理ポリシーを実施します。

6) **ユーザーアクセスレビュー**：サプライヤーはアクセスする情報の機密性に応じた頻度で、Lilly 情報へのアクセス権の必要性と適切性を定期的にレビューおよび検証します。

7) **アカウントおよびセッションのロックアウト**：サプライヤーは不正アクセス試行を抑止するために、アカウントおよびセッションのロックアウトポリシーを実施します。これには所定の回数のログイン失敗後にアカウントまたはセッションを無効にすることが含まれます。

8) **通知**：サプライヤーは、リリーシステムにアクセスする従業員の変更について、24 時間以内にリリーに通知します。

6. **システムセキュリティおよび完全性**：

1) **安全な構成および強化** ： サプライヤーは脆弱なサービスや設定を通じてリリー情報が悪用されないように、業界のベストプラクティスに従ってシステム（エンドポイントを含む）のセキュリティ設定と構成を管理します。

2) **脆弱性およびパッチ管理**：サプライヤーはすべてのシステムおよびアプリケーションに対してセキュリティパッチと更新を迅速に適用し、脆弱性を迅速に特定し、高リスクの脆弱性の修正を優先します。

3) **サービスの無効化**：サプライヤーはすべての不要なサービス、プロトコル、およびポートを無効にします。承認されたサービスは、その使用理由と正式に文書化された正当化および管理承認とともに明確に文書化される必要があります。

4) **ネットワークセキュリティおよびマルウェア保護**：

a. サプライヤーはファイアウォールポリシーを実施し、侵入検知/防止システムを構成して、ネットワークトラフィックの入出力を監視および制御します。
b. サプライヤーはサプライヤーのネットワーク内のすべてのワークステーションおよびサーバーに対してアンチマルウェアソリューションを展開および維持します。
c. サプライヤーは、すべてのファイアウォールルールが有効なビジネスニーズによって正当化されることを確認するために、ファイアウォール構成を定期的にレビューおよび更新します。

7. **セキュリティ管理**：

サプライヤーは包括的なセキュリティリスクの監視と管理を確保する統合されたセキュリティ管理アプローチを実施します。これには以下が含まれます。

1) **監査ログ管理、監視、および分析**：サプライヤーは、リリー情報に影響を与える可能性のある不正な活動を検出、調査、緩和、および回復するために、監査ログを収集、管理、保持、および分析します（継続的な監視を含む）。ログは少なくとも 18 か月間保持される必要があります。リソースが共有される環境（SaaS モデルなど）では、サプライヤーはすべてのログにリリー実装用の識別子をタグ付けし、要求に応じてこのデータをリリーに提供します。

2) **ペネトレーションテスト**：サプライヤーは、情報を取り扱うネットワークおよびアプリケーションに対して少なくとも 2 年ごとにペネトレーションテストを実施します。

3) **変更管理**：サプライヤーはすべての変更が文書化され、レビューされ、職務分離および緊急変更手順を含む構造化されたプロトコルに従って承認されることを保証する正式な変更管理プロセスを維持します。

8. **データセキュリティ**：

1) **適切な環境**：サプライヤーはリリー情報の機密性、完全性、および可用性を確保するために設計および構成された環境でのみリリー情報を処理します。これには、安全な保管およびデータ保護ポリシー、適切な物理的セキュリティ対策が含まれます。生産データはテストシステムや機器で使用されず、テストデータは生産システムや機器で使用されません。

2) **データの分離**：サプライヤーはリリー報をサプライヤー自身の情報、他の顧客の情報、および第三者の情報から常に論理的（および適用可能な場合は物理的）に分離する措置を実施します。

3) **暗号化標準**：プライヤーは業界のベストプラクティスに従って、保存時および転送時にすべての Lilly 情報を暗号化します。暗号化は、固定およびポータブルまたは取り外し可能なストレージを含む、保存媒体に関係なく保存データに必要です。

4) **データインベントリ管理**：サプライヤーは処理するすべてのリリー情報の詳細なインベントリを確立および維持します。これにはリリー情報を処理するシステムおよび資産が含まれます。

9. **記録の保持、返却および破棄**：

1) **保持**: サプライヤーは許可された目的のためにのみリリー情報を保持します。

2) **リリー情報の返却および安全な削除**: 契約期間中にリリーが要求した場合、または契約が終了または満了した場合、サプライヤーは 30 日以内に Lilly にすべてのリリー情報のコピーを返却し、安全に削除します。サプライヤーはすべてのリリー情報のコピーが返却され、安全に削除されたことを文書で確認します。

3) **アーカイブコピー**: サプライヤーが税務または類似の規制目的でリリー情報のアーカイブコピーを保持することが法律で要求される場合、サプライヤーは(i)アーカイブされた情報を他の目的で使用しないこと、および(ii)適切な物理的、管理的、技術的保護手段を使用して情報を保護し、セキュリティインシデントをリリーに通知する義務を含む契約上の義務を遵守することを約束します。

4) **削除基準**: サプライヤーは標準的なディスクおよびファイル回復ユーティリティを使用してデータが回復されないように設計された業界で受け入れられ、承認された方法（例：安全な上書き、磁気媒体の電磁フラックスフィールドでの消磁、シュレッディング、機械的分解）を使用して、削除対象のすべてのリリー情報

を安全に削除します。本基準に準拠して暗号化されたリリー情報に関しては、サプライヤーは暗号鍵のすべてのコピーを永久に安全に削除することで情報を削除することができます。

5) **メディアの破棄**: サプライヤーが物理的にアクセスできるまたは管理できるストレージ媒体（例：ラップトップのハードドライブ、デスクトップのハードドライブ、USB または「サム」ドライブ、バックアップ媒体、サプライヤー自身のデータセンターで使用されるハードドライブ、その他のポータブルストレージ媒体）を永久に廃棄または処分する前に、サプライヤーは媒体を使用不能にし、情報を回復不能にする技術（例：分解、焼却、粉砕、シュレッディング、溶解）を使用してストレージ媒体を破壊します。このセクションは、サプライヤーが物理的にアクセスできないまたは管理できないストレージ媒体（例：パブリッククラウドまたはその他の第三者環境で使用されるストレージ媒体）には適用されません。このような場合、サプライヤーは、第三者環境に保存されたすべてのリリー情報が不要になったときに業界で受け入れられた方法を使用して安全に削除されることを確認します（セクション 9.4、削除基準を参照）。

10. **情報セキュリティインシデントの対応、管理および報告**:

1) **インシデント対応**: サプライヤーはセキュリティインシデントの検出、調査、対応、緩和、および通知のためのインシデント対応手順を持つ必要があります。これらのインシデント対応手順は、文書化され、テストされ、少なくとも年に一度レビューされる必要があります。サプライヤーはリリーの要求に応じて手順を提供します。

2) **インシデント対応計画**: サプライヤーは書面によるインシデント対応計画を維持し、リリーの要求に応じて計画のコピーを提供します。サプライヤーは、対応計画および業界のベストプラクティスに従って、各セキュリティインシデントをタイムリーに改善します。

3) **通知の必要性**: サプライヤーはセキュリティインシデントを認識してから 48 時間以内に、Cyber@Lilly.com にメールを送信することでリリーに通知します。通知には、インシデントの影響をリリーが理解するために必要な情報が含まれます。これには、セキュリティインシデントの性質、セキュリティインシデントによって影響を受けたリリー情報の説明、およびセキュリティインシデントに対応するためにサプライヤーが取っている行動が含まれますが、これらに限定されません。

4) **リリーの調査への協力**: サプライヤーはリリーのセキュリティインシデントの取り扱いにおいて合理的に協力します。これには、以下が含まれますが、これに限定されません。

(i) サプライヤーの対応計画についてリリーと調整すること。

(ii) セキュリティインシデントのリリーの調査を支援すること。

(iii) セキュリティインシデントまたは対応に関与するサプライヤーの従業員やその他の関係者とのインタビューを促進すること。

(iv) 適用される法律、規制、業界標準に準拠するために、またはリリーの要求に応じて必要なすべての関連記録、ログ、ファイル、データ報告、フォレンジックレポート、調査レポート、およびその他の資料を提供すること。

5) **第三者への通知**: サプライヤーはリリーの事前の書面による同意を得ることなく、セキュリティインシデントについて第三者（規制当局や顧客を含む）に通知しないことに同意します。さらに、サプライヤーはリリーが以下を単独で決定する権利を有することに同意します。

(i) セキュリティインシデントの通知を個人、規制当局、法執行機関、その他に提供するかどうか。

(ii) その通知の形式と内容。

11. **安全なシステム開発ライフサイクル**:

サプライヤーは計画、分析、設計、実装、テスト、展開、および保守を含む開発ライフサイクルのすべての段階において、リリー情報を処理するすべてのシステム、ソフトウェア、またはアプリケーションに対して、文書化された安全なソフトウェア開発ライフサイクル（SSDLC）業界のベストプラクティスに従います。

12. **修復**:

サプライヤーとリリーが本基準に基づくサプライヤーの義務に関してサイバーセキュリティ関連の是正措置について書面で合意した場合、サプライヤーは定期的に（少なくとも 15 営業日ごとに 1 回以上）または事前に書面で合意された頻度で是正措置の進捗状況と完了状況を詳細に報告します。サプライヤーは合意された是正措置の成功裏の完了と解決を示す文書証拠を適用される是正措置に関する合意から 120 営業日以内に提供するものとします。このような文書証拠を提供しない場合、本契約の重大な違反と見なされます。