資訊處理安全管理辦法

目的：管理由 Lilly

或代表其發布相關資訊的關鍵準則，以下簡稱為資訊。資訊的重要性？

- 我們相當重視您的經營團隊對 Lilly 的貢獻。您和您的員工所採取的行動是防止資訊洩漏最關鍵的重要防線。
- 保護資訊對於 Lilly 以及對於其所服務的患者至關重要。

由業界最佳典範，包括美國國家標準暨技術研究院 (NIST)
網路安全框架在內所提供的重要訊息，應納入目前實務，以持續降低資訊處理的風險。

一般而言：

- 除非絕對必要，否則請避免複製包含資訊的電子檔或紙本副本。

電子資料儲存媒體：

- 包含資訊的電子檔案必須妥善儲存。未經 Lilly 公司允許，不得使用抽取式儲存裝置，例如：外接式硬碟和 USB。
    - 檔案的存取權限應適用最小特權原則
      (亦即，存取資訊的權限應限於相關人員，存取資訊不超過所需資訊，並且僅在所需的時間範圍內)。存取權限需根據對應的資訊敏感程度進行審查。包括您
      管理的儲存位置以及分包商管理的儲存位置。
    - 離職或個人業務不再需要存取資訊時，應及時解除存取權限。
- 未經 Lilly 允許，不得將資訊儲存在以下位置：
    - 員工的個人裝置，例如：筆記型電腦、iPad 等
    - 外部儲存服務或網站。

電子資料傳輸：

- 包含資訊的電子檔案必須經由安全的方式進行傳輸。請諮詢您的 Lilly 聯絡窗口，以建立資訊傳輸的偏好方式。未經 Lilly 允許，不得使用抽取式儲存裝置，例如：外接式硬碟、CD/DVD 和 USB。
- 資訊不得透過以下方式傳輸：
    - 不安全的電子郵件 (除非不具敏感度)。
    - 外部儲存裝置，例如：外接式硬碟或 USB (未經 Lilly 允許)。
    - 私人電子郵件。

電話會議/線上會議：

- 使用 Lilly 核准的會議服務和舉行公司業務相關會議。如果您對電話會議/線上會議有疑問，請諮詢您的 Lilly 聯絡窗口。
- 討論資訊時，請留意四周環境並保持謹慎。

人身安全：

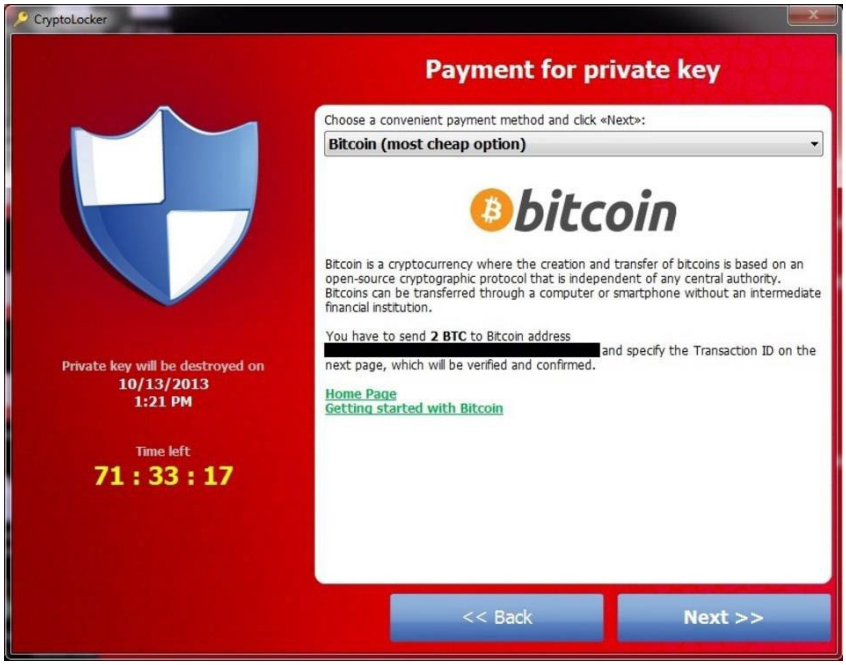
- 維護安全的工作環境：
    - 每當您離開裝置時，都應鎖定對裝置的存取權限。
    - 當您請假、出差或度假時，應隨時將裝置放在可上鎖的機櫃中，並用電腦鎖上鎖或隨身攜帶。
    - 當您請假、出差或度假時，請將辦公桌、機櫃和儲物櫃/辦公室上鎖。
    - 請勿將紙本文件留在印表機。
    - 謹慎地銷毀資訊 (例如：碎紙機)。

即時通訊和簡訊：

- 使用 Lilly 核准的設備發送公司業務相關的即時通訊和簡訊。如果您對即時通訊或簡訊有疑問，請諮詢您的 Lilly 聯絡窗口。

資訊安全事件通報：

- 及時向您的 Lilly 聯絡窗口通報相關事件。事件包括但不限於：
    - 將包含資訊的電子郵件誤傳至非指定收件人。
    - 包含資訊的筆記型電腦、硬碟或抽取式儲存裝置遺失或遭竊。
    - 擁有資訊存取權限的分包商會向您的公司發出事件警示。
    - 收到勒索病毒，這是一種惡意程式，用來阻止對裝置的存取，直到支付贖金為止。請參見以下範例。立即執行以下步驟可能有助於降低風險：
        - 拔下網路線或停用無線網卡。
        - 休眠模式。



提防社交工程 *(*例如：網路釣魚、語音釣魚、簡訊釣魚*)*：

- 社交工程是利用欺騙手段操縱個人使其洩露可能用來詐騙的機密或個人資訊。詐騙集團偽裝成信譽良好的源頭，以竊取身分或擷取資訊，例如：密碼、銀行資料和信用卡的卡號等。
    - **網路釣魚** (電子郵件)
        - 網路釣魚企圖以意外訊息引起注意，其特徵包括：
            - 引起恐慌的行動呼籲 (例如：您的信用卡已延遲付款)。
            - 時間元素 (例如：兩天內到期)。
            - 後果 (例如：解決此問題，否則您可能會遭遇不好的事情)。
            - 語法不正確或拼字錯誤。
            - 以及，一定會有「點選」的選項，例如：連結或附件。
        - 如果點選未知附件或電子郵件中的連結，您的電腦和整個網路可能會遭到威脅。
    - **語音釣魚** (電話或語音留言)
        - 語音釣魚 (語音網路釣魚) 企圖以一通意外電話引起注意，可能會：
            - 要求確認資訊確認或要求資訊。
            - 用來搭配網路釣魚攻擊。

- **簡訊釣魚** (簡訊)
  - 簡訊釣魚企圖以意外的簡訊引起注意，可能會：
    - 要求確認資訊確認或要求資訊。
    - 用來搭配網路釣魚攻擊。
    - 通常會有「點選」的選項，例如：連結或附件。

- **如果您有 Lilly 的電子郵件位址**，您將參加 Lilly 正式的網路釣魚教育訓練。
  - 重複點選者將通報給第三方，並將接受後續指導。如果您對 Lilly 的正式網路釣魚教育訓練有疑問，請諮詢您的 Lilly 聯絡窗口。
  - 如果您使用的是 Lilly o365 電子郵件帳戶，請透過 Outlook「Home (首頁)」功能區中的「Report Phishing (通報網路釣魚)」按鈕舉報可疑的電子郵件。

  - 如果您通過 VPN 或 virtual.lilly.com 連接到 Internal Lilly 網路，以下是報告可疑消息的方法cyber@lilly.com。

- **暫停和檢查。善用您的直覺：**
  - 如果電子郵件看起來很可疑，請花點時間仔細檢查郵件。
  - 如果您並未預期會收到電子郵件，請勿點擊或開啟其中的連結或附件。
  - 如果您沒有 Lilly 的電子郵件位址，並且在您認為可疑的郵件中點選了連結或開啟附件，請依照貴公司規定的程序進行舉報。

如果您有任何問題或疑慮：

- 有關上述任何項目的問題或疑慮，請諮詢您的 Lilly 聯絡窗口。
- 您也可以在供應商資源的經營責任項目內的 Supplier Portal (供應商入口網站) 上找到此資訊。