안전한 정보 취급을 위한 비즈니스 규칙

목적: Lilly 에서 제공한 정보 또는 Lilly 를 대신하여 제공된 정보(이하 정보라고 함)를 취급하는 일에 대한 핵심 메시지입니다.

이것이 중요한 이유

- 귀하의 조직 및 직원은 Lilly 의 소중한 기여자이며, 귀하 및 귀하의 직원이 취하는 조치는 정보 침해를 예방하는 최초이자 최고의 방어선에 해당합니다.
- 정보 보호는 Lilly 는 물론 Lilly 가 서비스를 제공하는 환자에게 매우 중요합니다.

다음 핵심 메시지는 NIST 사이버 보안 프레임워크 등의 업계 모범 사례를 고려하여 마련된 것으로, 현행 방침에 통합하여 정보를 취급할 때 위험을 줄일 수 있도록 해야 합니다.

일반 유의 사항:

- 반드시 필요한 경우가 아니라면 정보가 포함된 문서의 전자 또는 종이 사본을 복사하지 마십시오.

전자 데이터 저장:

- 정보가 포함된 전자 파일은 안전하게 저장해야 합니다. 외부 하드 드라이브 및 USB 와 같은 이동식 저장 장치는 Lilly 의 승인 없이는 사용할 수 없습니다.
    - 파일에 대한 액세스 권한을 부여할 때는 최소 권한 원칙을 적용해야 합니다. 즉, 정보에 대한 액세스 권한은 알아야 할 필요가 있는 사람에게만, 필요한 내용만, 필요한 시간 동안만 부여해야 합니다. 민감도 수준에 따라 액세스 권한을 검토해야 합니다. 여기에는 귀하가 관리하는 저장 위치와 하청 업체가 관리하는 저장 위치가 포함됩니다.
    - 퇴사한 경우 또는 개인이 더 이상 정보에 액세스할 업무상 필요가 없는 경우 적시에 액세스 권한을 비활성화해야 합니다.
- Lilly 의 승인을 받은 경우를 제외하고 다음 위치에 정보를 저장해서는 안 됩니다.
    - 직원의 개인 기기(노트북, iPad 등)
    - 외부 저장 서비스 또는 사이트

전자 데이터 전송:

- 정보가 포함된 전자 파일은 안전하게 전송해야 합니다. 정보 전송에 대해 선호하는 방법을 설정하려면 Lilly 담당자에게 문의하십시오. 외부 하드 드라이브, CD/DVD 및 USB 와 같은 이동식 저장 장치는 Lilly 의 승인 없이는 사용할 수 없습니다.
- 다음을 통해 정보를 전송해서는 안 됩니다.
    - 안전하지 않은 이메일(민감도 수준이 보장되지 않는 경우 제외)
    - 외부 하드 드라이브 또는 USB 와 같은 외부 저장 장치(Lilly 의 승인을 받지 않은 경우)
    - 개인 이메일

원격 회의/온라인 회의:

- Lilly 에서 승인한 회의 서비스를 사용하여 회사 업무상 회의를 예약하고 진행하십시오. 원격 회의/온라인 회의와 관련된 질문이 있는 경우 Lilly 담당자에게 문의하십시오.
- 정보를 논의할 때는 주변 환경을 인식하고 주의하십시오.

물리적 보안:

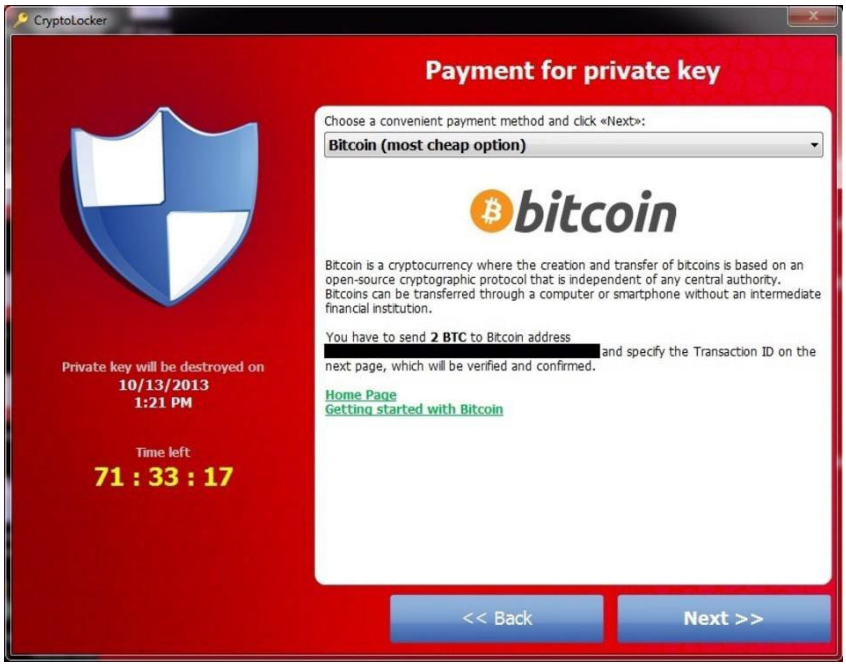
- 업무 공간의 보안을 유지하십시오.
  - 기기를 두고 자리를 비울 때는 반드시 기기 액세스를 잠그십시오.
  - 퇴근할 때나 출장 또는 휴가로 자리를 비울 때는 기기를 잠금 장치가 있는 캐비닛에 보관하거나, 케이블로 잠그거나, 직접 소지해야 합니다.
  - 퇴근할 때나 출장 또는 휴가로 자리를 비울 때는 책상, 캐비닛 및 라커/사무실을 잠그십시오.
  - 프린터에 종이 사본을 방치하지 마십시오.
  - 정보는 기밀이 유지되는 방식으로 폐기하십시오(예: 파쇄).

인스턴트 메시지 및 문자 메시지:

- 회사 업무 용도로는 Lilly 에서 승인한 인스턴트 메시지 및 문자 메시지 도구를 활용하십시오. 인스턴트 메시지 또는 문자 메시지 전송과 관련된 질문이 있는 경우 Lilly 담당자에게 문의하십시오.

정보 보안 사건 보고:

- Lilly 담당자에게 적시에 사건을 보고하십시오. 사건은 다음을 포함하나 이에 국한되지 않습니다.
  - 정보가 포함된 이메일이 의도하지 않은 수신자에게 실수로 전송되었습니다.
  - 정보가 포함된 노트북, 하드 드라이브 또는 이동식 저장 장치를 분실하거나 도난당했습니다.
  - 정보에 대한 액세스 권한이 있는 하청 업체가 회사에 사건을 알립니다.
  - 랜섬웨어(금전을 지불할 때까지 기기에 대한 액세스를 차단하도록 설계된 일종의 악성 소프트웨어)를 수신합니다. 아래 예를 참조하십시오. 다음 단계를 즉시 수행하면 위험을 줄이는 데 도움이 될 수 있습니다.
    - 네트워크 케이블을 분리하거나 무선 어댑터를 비활성화합니다.
    - 최대 절전 모드로 전환합니다.



소셜 엔지니어링에 유의할 것*(*예*:* 피싱*,* 보이스 피싱*,* 스미싱*)*:

- 소셜 엔지니어링이란 속임수로 개인을 조종하여 사기 목적으로 사용될 수 있는 기밀 또는 개인 정보를 유출하도록 유도하는 것입니다. 사기꾼은 신원을 도용하거나 암호, 은행 거래 세부 정보, 신용 카드 번호 등의 정보를 알아내기 위해 신뢰할 수 있는 주체를 가장합니다.
  - **피싱**(이메일)
    - 피싱 시도는 예상치 못한 메시지를 말하며 다음과 같은 특징이 있습니다.
      - 사람을 놀라게 만드는 문구(예: 신용 카드 결제 금액이 미납됨)
      - 시간 관련 요소(예: 기한이 2 일 남음)
      - 불이익이 되는 결과(예: 이 문제를 해결하지 않으면 피해가 발생함)

        - 문법이 엉망이거나 단어의 철자가 틀림
        - 또한 링크 또는 첨부 파일 등 "클릭"해야 하는 항목이 반드시 있음
      - 이메일에서 알 수 없는 첨부 파일 또는 링크를 클릭하면 컴퓨터 및 전체 네트워크가 손상될 수 있습니다.

  - **보이스 피싱**(전화 또는 음성 메시지)
    - 보이스 피싱 시도는 예상치 못한 전화를 말하며 다음과 같은 특징이 있습니다.
      - 정보 확인을 요청하거나 정보를 요청합니다.
      - 피싱 공격과 함께 사용될 수 있습니다.
  - **스미싱**(SMS 문자 메시지)
    - 스미싱 시도는 예상치 못한 문자 메시지를 말하며 다음과 같은 특징이 있습니다.
      - 정보 확인을 요청하거나 정보를 요청합니다.
      - 피싱 공격과 함께 사용될 수 있습니다.
      - 일반적으로 링크 또는 첨부 파일 등 "클릭"해야 하는 항목이 있습니다.

- **Lilly 이메일 주소**를 보유한 경우 Lilly 의 공식 교육용 피싱 프로그램에 참여하게 됩니다.
  - 클릭해서는 안 되는 항목을 클릭하는 상황이 반복되는 개인은 제 3 자에게 보고되며 후속 코칭을 받아야 합니다. Lilly 의 공식 교육용 피싱 프로그램에 대한 질문이 있는 경우 Lilly 담당자에게 문의하십시오.
  - Lilly o365 이메일 계정을 사용하는 경우 Outlook "Home(홈)" 리본의 "Report Phishing(피싱 신고)" 버튼을 통해 의심스러운 이메일을 신고하십시오.

  - VPN 또는 virtual.lilly.com 를 통해 Internal Lilly 네트워크에 연결되어 있는 경우 다음을 통해 의심스러운 메시지를 신고하세요.cyber@lilly.com
    .

- **잠시 멈춰 조사할 것, 직감을 이용할 것:**
  - 이메일이 의심스럽다면 잠시 시간을 내어 메시지를 자세히 살펴보십시오.
  - 예상하지 못한 링크를 클릭하거나 첨부 파일을 열지 마십시오.
  - Lilly 이메일 주소를 보유하고 있지 않으며 의심스러운 메시지의 링크를 클릭하거나 첨부 파일을 연 경우 고용주의 프로세스를 통해 신고하십시오.

질문 또는 우려 사항이 있는 경우:

- 위에서 논의한 항목과 관련된 질문 또는 우려 사항은 Lilly 담당자에게 문의하십시오.
- 이 정보는 Supplier Portal(공급자 포털)에 있는 Supplier Resources(공급자 리소스)의 Operating Responsibility(운영 책임)에서도 확인할 수 있습니다.