Cel: Kluczowe wiadomości dotyczące postępowania z informacjami od firmy Lilly lub dostarczonymi w jej imieniu.

Informacje obejmują zarówno informacje poufne, jak i dane osobowe wykorzystywane do celów związanych z pracą. Dane osobowe to wszelkie informacje, które zarówno indywidualnie, jak i w połączeniu z innymi danymi określają tożsamość osoby. Informację poufną definiuje się jako każdą informację uznawaną za poufną lub zastrzeżoną przez stronę ujawniającą.

Proszę zapoznać się z dokumentem i przekazać go dalej osobom wewnątrz firmy, które mają obecnie dostęp do informacji od firmy Lilly lub dostarczonych w jej imieniu oraz przyszłym pracownikom.

Dlaczego jest to ważne?

- Twoja firma i jej pracownicy jesteście cennymi współpracownikami firmy Lilly, a podejmowane przez Was działania są główną i najlepszą linią obrony przed narażeniem na ujawnienie informacji.
- Ochrona informacji jest najważniejsza dla naszej firmy oraz dla pacjentów, którym służymy.

Następujące kluczowe wiadomości zawarte w najlepszych praktykach branżowych, w tym w programie NIST związanym z cyberbezpieczeństwem, powinny być włączone do obecnych praktyk w celu dalszego zmniejszania ryzyka dotyczącego postępowania z informacjami.

Uwagi ogólne:

- Nie należy wykonywać elektronicznych i papierowych kopii dokumentów zawierających informacje, jeśli nie jest to bezwzględnie konieczne.

Elektroniczne nośniki danych:

- Pliki elektroniczne zawierające określone informacje należy przechowywać w bezpieczny sposób.
    - Jeśli zewnętrzne usługi przechowywania lub usługi chmurowe, które nie zostały wcześniej określone przez firmę Lilly lub z nią uzgodnione są wykorzystywane przez Twoją firmę do przechowywania informacji firmowych lub dostarczonych w imieniu firmy Lilly, skontaktuj się z odpowiednią osobą z firmy Lilly.
    - Dostęp do plików elektronicznych zawierających informacje powinien być przyznawany wyłącznie osobom, które muszą je znać i tylko na określony czas (najniższy poziom uprawnień).
    - Dostęp powinien być przyznany współmiernie do poziomu poufności informacji. Dotyczy to zarówno miejsc przechowywania, którymi zarządzasz, jak i tych, którymi zarządzają Twoi podwykonawcy.
    - Punktualnie po opuszczeniu firmy lub gdy dane osoby nie potrzebują już dostępu do informacji należy dokonać dezaktywacji.
- Bez zgody firmy Lilly informacje NIE mogą być przechowywane w następujących lokalizacjach:
    - Jakiekolwiek zewnętrzne nośniki pamięci, takie jak zewnętrzne dyski twarde, pamięci USB itp.
    - Prywatne urządzenia pracowników, takie jak laptopy, iPady itp.

Elektroniczny transfer danych:

- Pliki elektroniczne zawierające informacje należy przekazywać w bezpieczny sposób (współmiernie do poziomu poufności informacji). Aby uzgodnić sposób przekazywania danych, skontaktuj się z odpowiednią osobą z firmy Lilly.
- Przed wysłaniem sprawdź adres odbiorcy i upewnij się, że jest to adres używany do celów biznesowych.
- Informacji NIE można przekazywać za pośrednictwem:
    - Zewnętrznych nośników pamięci, takich jak zewnętrzne dyski twarde lub pamięci USB (bez zgody firmy Lilly).
    - Prywatnej skrzynki e-mail.

Drukowanie:

- Odradza się drukowania informacji na domowych/prywatnych drukarkach lub w miejscach publicznych. Jeśli musisz wydrukować materiały w domu lub poza biurem, podłącz laptopa lub autoryzowane urządzenie (np. iPada) do drukarki za pomocą przewodu lub sieci bezprzewodowej.

Telekonferencje:

- Powinny być prowadzone za pośrednictwem usług Skype for Business, Cisco WebEx lub Citrix GoToMeeting. Jeśli nie możesz korzystać z tych usług, skontaktuj się z odpowiednią osobą z firmy Lilly.
- Spotkania online nie są nagrywane bez powiadomienia i uzyskania zgody firmy Lilly.
- Obserwuj miejsce pracy i zachowaj ostrożność podczas ujawniania informacji w rozmowie.

Bezpieczeństwo fizyczne:

- Zachowanie bezpiecznego miejsca pracy:
    - Blokuj dostęp do komputera ZA KAŻDYM RAZEM, kiedy od niego odchodzisz.
    - Pod koniec dnia pracy upewnij się, że laptopy i iPady są w zamkniętej gablocie, zabezpieczone blokadą linkową lub zabierz je ze sobą.
    - Opuszczając biuro po zakończonym dniu pracy, zamknij biurko, gabloty, szafki i biuro.
    - Nie zostawiaj papierowych kopii dokumentów w drukarce.
    - Jeśli jest to możliwe, używaj zatwierdzonych metod przekazywania informacji zamiast ich przesyłania mailem, pocztą lub faksem.
    - Pozbywaj się dokumentów w bezpieczny sposób (np. niszcz w niszczarce).

Wiadomości SMS:

- Wiadomości SMS nie zawierają informacji przekazanych przez firmę Lilly lub w jej imieniu.

Zgłaszanie incydentów dotyczących bezpieczeństwa informacji:

- W razie incydentu dotyczącego bezpieczeństwa informacji skontaktuj się z menedżerem ds. relacji lub osobą odpowiedzialną z firmy Lilly i zgłoś to za pośrednictwem infolinii ds. etyki i przestrzegania zasad, jeśli sprawa dotyczy dostępu wewnętrznego lub poprzez stronę EthicsPoint, jeśli sprawa dotyczy dostępu zewnętrznego.
  Incydenty obejmują między innymi:
    - Przypadkowe przesłanie wiadomości e-mail zawierającej informacje do niewłaściwego odbiorcy.
    - Zgubienie lub kradzież laptopa, dysku twardego albo zewnętrznego nośnika pamięci z informacjami.
    - Powiadomienia o zdarzeniu przesłane przez podwykonawcę, który posiada dostęp do informacji.
    - Ransomware (oprogramowanie wymuszające okup)
      Jeśli pojawi się okienko podobne do tego poniżej, wykonanie następujących kroków może pomóc ograniczyć ryzyko:
        - Odłącz kabel sieciowy lub wyłącz kartę sieci bezprzewodowej.
        - Przełącz urządzenie w stan hibernacji.

Uwaga na próby wyłudzania informacji!

- Phishing to próba wyłudzenia informacji przez osoby z zewnątrz poprzez, które podszywają się pod wiarygodne podmioty. W przypadku kliknięcia nieznanego załącznika lub łącza w wiadomości e-mail, komputer i cała sieć firmowa mogą być zagrożone.

- Atak typu phishing jest niespodziewaną wiadomością, która w większości przypadków zawiera:

    - Natychmiastowe wezwanie do działania (np. dotyczące zalegania z płatnością za kartę kredytową).
    - Element czasu (np. coś należy wykonać w ciągu dwóch dni).
    - Konsekwencje (np. należy rozwiązać dany problem w przeciwnym razie może się to źle skończyć).
    - Błędy gramatyczne lub ortograficzne.
    - ORAZ zawsze element, który należy kliknąć, taki jak odnośnik lub załącznik.

- **Z**atrzymaj się i **s**prawdź. Użyj swojej intuicji. Jeśli e-mail wydaje się podejrzany, poświęć chwilę na przeczytanie jego treści. Nie klikaj odnośników ani nie otwieraj załączników, jeśli się ich nie spodziewasz.

- Osoby, które mają swój firmowy adres e-mail wezmą udział w formalnym programie edukacyjnym dotyczącym wyłudzania informacji („phishingu”). Nazwiska osób, które często klikają nieodpowiednie elementy zostaną przekazane stronom trzecim, aby mogły one skierować te osoby na szkolenia. Jeśli masz pytania związane z formalnym programem edukacyjnym dotyczącym wyłudzania informacji, skontaktuj się z odpowiednią osobą z firmy Lilly. Jeśli klikniesz odnośnik lub otworzysz załącznik w podejrzanej wiadomości z adresu firmowego Lilly, zgłoś to zdarzenia za pomocą formularza Operation Screen Door.

W przypadku pytań lub wątpliwości:

- Jeśli masz pytania lub wątpliwości dotyczące omówionych powyżej zagadnień, skontaktuj się z odpowiednią osobą z firmy Lilly.
- Niniejsze informacje są dostępne również w portalu dla dostawców w części zawierającej materiały o programie Protect Lilly.

15 July 2017