BEDRIJFSREGELS VOOR HET VEILIG OMGAAN MET INFORMATIE

Doel: Kernboodschappen voor het omgaan met informatie van of verstrekt namens Lilly, hierna Informatie genoemd.

Waarom is dit belangrijk?

- Uw organisatie en haar personeel dragen in ruime mate bij tot Lilly, en de acties die u en uw personeel ondernemen, maken deel uit van de eerste en beste verdedigingslinie tegen het compromitteren van informatie.
- Het beschermen van informatie is essentieel voor Lilly en de patiënten die we dienen.

De volgende kernboodschappen, die zijn gebaseerd op best practices uit de branche, waaronder het NIST Cybersecurity Framework, moeten worden opgenomen in de huidige praktijken om de risico's bij het omgaan met informatie te blijven verminderen.

In het algemeen:

- Maak geen duplicatieve elektronische of papieren kopieën van documenten die informatie bevatten, tenzij dit absoluut noodzakelijk is.

Elektronische gegevensopslag:

- Elektronische bestanden die informatie bevatten, moeten veilig worden opgeslagen. Verwisselbare opslagapparaten zoals externe harde schijven en USB-sticks kunnen niet worden gebruikt zonder goedkeuring van Lilly.
    - Principle of Least Privilege moet worden toegepast om toegang tot bestanden te verlenen (d.w.z. toegang tot informatie mag alleen worden verleend aan degenen die het moeten weten, niet meer dan nodig is en alleen voor de tijd die nodig is). Toegang moet worden herzien in overeenstemming met het gevoeligheidsniveau. Dit omvat zowel opslaglocaties die u beheert als die beheerd door uw onderaannemers.
    - Tijdige deactivering van de toegang dient plaats te vinden na een vertrek uit het bedrijf of wanneer individuen niet langer een zakelijke behoefte hebben om toegang te krijgen tot Informatie.
- Informatie mag NIET worden opgeslagen op de volgende locaties zonder toestemming van Lilly:
    - Persoonlijke apparaten van medewerkers zoals laptops, iPad etc.
    - Externe opslagservices of sites.

Elektronische gegevensoverdracht:

- Elektronische bestanden die informatie bevatten, moeten veilig worden overgedragen. Raadpleeg uw Lilly-contactpersoon om de voorkeursmethode voor informatieoverdracht te bepalen. Verwisselbare opslagapparaten zoals externe harde schijven, cd's/dvd's en USB-sticks kunnen niet worden gebruikt zonder goedkeuring van Lilly.
- Informatie mag NIET worden overgedragen via:
    - Onbeveiligde e-mail (tenzij het gevoeligheidsniveau dit niet rechtvaardigt).
    - Externe opslagapparaten zoals externe harde schijf of USB (zonder goedkeuring van Lilly).
    - Persoonlijke email.

Teleconferenties/onlinevergaderingen:

- Gebruik door Lilly goedgekeurde vergaderservices voor het plannen en houden van vergaderingen over zakelijke aangelegenheden. Raadpleeg uw Lilly-contactpersoon als u vragen heeft over teleconferenties/onlinevergaderingen.
- Wees u bewust van uw omgeving en wees voorzichtig bij het bespreken van informatie.

Fysieke veiligheid:

- Zorg voor een veilige werkruimte:
  - Vergrendel de toegang tot uw apparaten ELKE keer dat u ze onbewaakt laat.
  - Apparaten moeten in een afsluitbare kast worden geplaatst, met een kabel worden vergrendeld of worden meegenomen wanneer u een dag weggaat, op zakenreis of op vakantie bent.
  - Vergrendel uw bureau, kasten en locker/kantoor wanneer u voor een dag vertrekt, weg bent voor zakenreizen of op vakantie bent.
  - Laat geen papieren exemplaren achter op printers.
  - Gooi informatie vertrouwelijk weg (bijv. versnipperen).

Instant message en tekst:

- Gebruik een door Lilly goedgekeurde tool voor instant messages en sms-berichten voor bedrijfszaken. Raadpleeg uw Lilly-contactpersoon als u vragen heeft over instant messaging of sms-berichten.

Rapportage van informatiebeveiligingsincidenten:

- Meld incidenten tijdig aan uw Lilly-contactpersoon. Incidenten omvatten, maar zijn niet beperkt tot:
  - E-mail met informatie is per ongeluk verzonden naar een onbedoelde ontvanger.
  - Verloren of gestolen laptop, harde schijf of verwijderbaar opslagapparaat dat informatie bevat.
  - Een onderaannemer met toegang tot informatie waarschuwt uw bedrijf voor een incident.
  - Ontvangen van Ransomware, een type schadelijke software dat is ontworpen om de toegang tot het apparaat te blokkeren totdat een bedrag is betaald. Zie onderstaand voorbeeld. Het onmiddellijk uitvoeren van de volgende stappen kan helpen om het risico te verkleinen:
    - Koppel de netwerkkabel los of schakel de draadloze adapter uit.
    - Slaapstand.

Pas op voor social engineering *(bijv., Phishing, Vishing, SMiShing)*!:

- Social engineering is het gebruik van misleiding om individuen te manipuleren om vertrouwelijke of persoonlijke informatie bekend te maken die voor frauduleuze doeleinden kan worden gebruikt. Oplichters doen zich voor als een betrouwbare bron in een poging identiteiten te stelen of informatie op te halen, zoals wachtwoorden, bankgegevens en creditcardnummers, enz.
  - **Phishing** (e-mail)
    - Een phishingpoging is een onverwacht bericht en heeft onder meer de volgende kenmerken:
      - Een alarmerende oproep tot actie (uw creditcardbetaling is bijvoorbeeld te laat).
      - Een tijdselement (er moet bijvoorbeeld iets binnen twee dagen worden betaald).
      - Een gevolg (los dit probleem bijvoorbeeld op, anders gebeurt er iets ergs met u).
      - Slechte grammatica of verkeerd gespelde woorden.
      - EN heeft altijd iets om op te "klikken", zoals een link of bijlage.
    - Als u op een onbekende bijlage of link in een e-mail klikt, kunnen uw computer en het hele netwerk in gevaar komen.

- **Vishing** (telefoontjes of spraakberichten)
  - Een vishing-poging (voice phishing) is een onverwacht telefoontje dat:
    - bevestiging van informatie zoekt of om informatie vraagt.
    - Kan worden gebruikt in combinatie met een phishing-aanval.
- **SMiShing** (Sms-berichten)
  - Een SMiShing-poging is een onverwachte tekst die:
    - bevestiging van informatie zoekt of om informatie vraagt.
    - Kan worden gebruikt in combinatie met een phishing-aanval.
    - meestal iets heeft om op te "klikken", zoals een link of bijlage.

- **Als u een Lilly-e-mailadres hebt,** neemt u deel aan het formele educatieve phishing-programma van Lilly.
  - Individuen die herhalingsklikker zijn, worden aan de derde partij gerapporteerd met de verwachting van vervolgcoaching. Raadpleeg uw Lilly-contactpersoon als u vragen heeft over het formele educatieve phishing-programma van Lilly.
  - Als u een Lilly o365 e-mailaccount gebruikt, meldt u verdachte e-mails via de knop "Report Phishing (Phishing melden)" in het Outlook "Home"-lint.

  - Als u via VPN of virtual.lilly.com bent verbonden met het interne Lilly-netwerk, meld dan verdachte berichten via cyber@lilly.com.

- **Pauzeer en inspecteer. Gebruik uw intuïtie:**
  - Als een e-mail verdacht lijkt, neem dan even de tijd om het bericht goed te bekijken.
  - Klik niet op links en open geen bijlagen als u ze niet verwacht.
  - Als u geen Lilly-e-mailadres heeft en u klikt op een link of opent een bijlage in een bericht waarvan u denkt dat het verdacht is, meld dit dan via het proces van uw werkgever.

Als u vragen of opmerkingen heeft:

- Raadpleeg uw Lilly-contactpersoon als u vragen of opmerkingen heeft met betrekking tot een van de hierboven besproken items.
- Deze informatie is ook beschikbaar op het Supplier Portal (Leveranciersportaal) onder operationele verantwoordelijkheid in de leveranciersbronnen.