RÈGLES MÉTIER POUR LA GESTION SÉCURISÉE DES INFORMATIONS

Objet : messages clés pour le traitement des informations de Lilly, ou fournies pour le compte de cette dernière, ci-après dénommées Informations.

Pourquoi est-ce important ?

- Votre organisation et son personnel sont des contributeurs précieux à Lilly, et les actions que vous et votre personnel entreprenez font partie de la première et meilleure ligne de défense contre la mise en péril des informations.
- La protection des informations est essentielle pour Lilly et les patients que nous servons.

Les messages clés suivants, qui sont éclairés par les meilleures pratiques de l'industrie, y compris le cadre de cybersécurité du NIST, devraient être intégrés aux pratiques actuelles pour continuer à réduire les risques lors du traitement des informations.

En général :

- Évitez de faire des copies électroniques ou papier de documents contenant des informations en double, sauf en cas de nécessité absolue.

Stockage de données électroniques :

- Les fichiers électroniques contenant des informations doivent être stockés en toute sécurité. Les périphériques de stockage amovibles tels que les disques durs externes et les clés USB ne peuvent pas être utilisés sans l'approbation de Lilly.
    - Le principe du moindre privilège devrait être appliqué pour accorder l'accès aux fichiers (c'est-à-dire que l'accès à l'information ne devrait être accordé qu'à ceux qui ont besoin de savoir, dans la mesure nécessaire et seulement pour le temps requis). L'accès doit être revu en fonction du niveau de sensibilité. Cela comprend les emplacements de stockage que vous gérez ainsi que ceux gérés par vos sous-traitants.
    - La désactivation de l'accès en temps opportun doit avoir lieu après une sortie de l'entreprise ou lorsque les personnes n'ont plus besoin d'accéder aux informations.
- Les informations ne doivent PAS être stockées dans les endroits suivants sans l'approbation de Lilly :
    - Les appareils personnels des employés tels que les ordinateurs portables, iPad, etc.
    - Les services ou sites de stockage externe.

Transfert électronique de données :

- Les fichiers électroniques contenant des informations doivent être transférés en toute sécurité. Consultez votre interlocuteur Lilly pour définir la méthode préférée pour le transfert d'informations. Les périphériques de stockage amovibles tels que les disques durs externes, les CD/DVD et les clés USB ne peuvent pas être utilisés sans l'approbation de Lilly.
- Les informations ne doivent PAS être transférées par les moyens suivants :
    - E-mail non sécurisé (sauf si le niveau de sensibilité ne le justifie pas).
    - Périphériques de stockage externes tels que disque dur externe ou USB (sans l'approbation de Lilly).
    - E-mail personnel.

Téléconférences/réunions en ligne :

- Utilisez les services de réunion approuvés par Lilly pour planifier et diriger des réunions sur les affaires de l'entreprise. Consultez votre interlocuteur Lilly si vous avez des questions concernant les téléconférences/réunions en ligne.
- Soyez conscient de votre environnement et soyez prudent lorsque vous discutez des informations.

Sécurité physique :

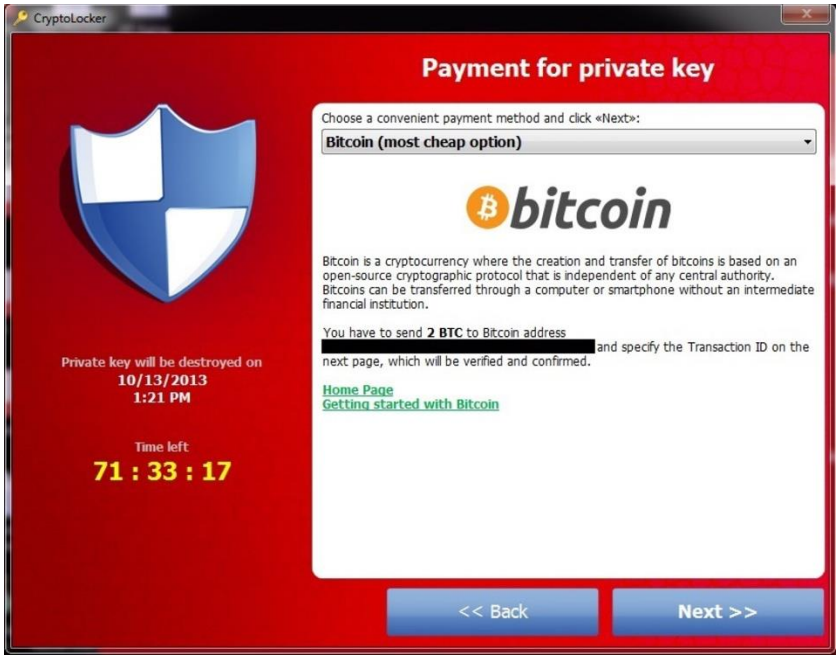
- Maintenez un espace de travail sécurisé :
    - Verrouillez l'accès à vos appareils à CHAQUE FOIS que vous vous en éloignez.
    - Les appareils doivent être placés dans une armoire verrouillable, sécurisés par un câble ou emportés avec vous lorsque vous partez pour la journée, que vous êtes en déplacement professionnel ou en vacances.
    - Verrouillez votre bureau, vos armoires et votre casier/bureau lorsque vous partez pour la journée, que vous êtes en déplacement professionnel ou en vacances.
    - Ne laissez pas de copies papier sur les imprimantes.
    - Jetez les informations de manière confidentielle (par exemple, déchiquetage).

Textes et messages instantanés :

- Utilisez un outil approuvé par Lilly pour les messages textes et messages instantanés concernant les affaires de l'entreprise. Consultez votre contact Lilly si vous avez des questions relatives à la messagerie instantanée ou la messagerie texte.

Rapport d'incident de sécurité de l'information :

- Signalez les incidents à votre contact Lilly en temps opportun. Ces incidents incluent, mais sans s'y limiter, les suivants :
    - Envoi accident d'un e-mail contenant des informations à un destinataire non souhaité.
    - Perte ou vol d'un ordinateur portable, disque dur ou périphérique de stockage amovible contenant des informations.
    - Signalement à votre entreprise d'un incident par un sous-traitant ayant accès aux informations.
    - Réception d'un ransomware, un type de logiciel malveillant conçu pour bloquer l'accès à l'appareil jusqu'à ce qu'une somme soit payée. Voir l'exemple ci-dessous. La réalisation immédiate des étapes suivantes peut aider à réduire les risques :
        - Débranchez le câble réseau ou désactivez l'adaptateur sans fil.
        - Mettez en veille prolongée.



Méfiez-vous de l'ingénierie sociale *(par exemple, Phishing, Vishing, SMiShing)* **! :**

- L'ingénierie sociale est l'utilisation de la tromperie pour manipuler des individus afin qu'ils divulguent des informations confidentielles ou personnelles qui peuvent être utilisées à des fins frauduleuses. Les fraudeurs se font passer pour une source réputée dans le but de voler des identités ou de récupérer des informations, telles que des mots de passe, des coordonnées bancaires et des numéros de carte de crédit, etc.

- **Phishing** (par e-mail)
  - Une tentative de phishing est un message inattendu et ses caractéristiques incluent les suivantes :
    - Un appel à l'action alarmant (par exemple, votre paiement par carte de crédit est en retard).
    - Un élément de temps (par exemple, quelque chose est dû dans les deux jours).
    - Une conséquence (par exemple, résolvez ce problème, ou quelque chose de mauvais va vous arriver).
    - Grammaire médiocre ou mots mal orthographiés.
    - ET a toujours un élément sur lequel « cliquer », comme un lien ou une pièce jointe
  - Si vous cliquez sur une pièce jointe ou un lien inconnu dans un e-mail, votre ordinateur et tout le réseau peuvent être mis en péril.

- **Vishing** (appels téléphoniques ou messages vocaux)
  - Une tentative de vishing est un appel téléphonique inattendu qui :
    - Cherche la confirmation d'informations ou demande des informations.
    - Peut être utilisé en combinaison avec une attaque de phishing.
- **SMiShing** (messages textes SMS)
  - Une tentative SMiShing est un texte inattendu qui :
    - Cherche la confirmation d'informations ou demande des informations.
    - Peut être utilisé en combinaison avec une attaque de phishing.
    - A généralement un élément sur lequel « cliquer », comme un lien ou une pièce jointe.

- **Si vous avez une adresse e-mail Lilly**, vous participerez au programme formel de phishing éducatif de Lilly.
  - Les personnes qui cliquent à plusieurs reprises seront signalées à la tierce partie dans l'attente d'un encadrement de suivi. Consultez votre contact Lilly si vous avez des questions sur le programme formel de phishing éducatif de Lilly.
  - Si vous utilisez un compte de messagerie Lilly o365, signalez les e-mails suspects via le bouton « Report Phishing » (Signaler un hameçonnage) dans le ruban « Home » (Accueil) d'Outlook.

  - Si vous êtes connecté au réseau interne de Lilly via VPN ou virtual.lilly.com, signalez le message suspect via cyber@lilly.com.

- **Mise en pause et inspection. Utilisez votre intuition :**
  - Si un e-mail semble suspect, prenez un moment pour l'examiner attentivement.
  - Ne cliquez pas sur les liens ou n'ouvrez pas les pièces jointes si vous ne les attendiez pas.
  - Si vous n'avez pas d'adresse e-mail Lilly et que vous cliquez sur un lien ou ouvrez une pièce jointe dans un message que vous estimez suspect, veuillez le signaler via le processus de votre employeur.

Si vous avez des questions ou des préoccupations :

- Consultez votre contact Lilly pour toute question ou préoccupation relative à l'un des éléments mentionnés ci-dessus.
- Ces informations sont également disponibles sur le Supplier Portal (Portail des fournisseurs) sous Operating Responsibility (Responsabilité d'exploitation) dans Supplier Resources (Ressources du fournisseur).