

Politique de Cybersécurité

Introduction

Le risque de vol de données, de fraudes et de failles de sécurité peut avoir un impact négatif sur les systèmes, l'infrastructure technologique et la réputation d'une entreprise. Par conséquent, GlycoNet a créé cette politique pour aider à décrire les mesures de sécurité mises en place pour garantir que les informations restent sécurisées et protégées.

Objectif

L'objectif de cette politique est de : 1) protéger les données et l'infrastructure de GlycoNet et des Services Intégrés GlycoNet (SIG), 2) décrire les protocoles et les directives qui régissent les mesures de cybersécurité, 3) définir les règles d'utilisation professionnelle et personnelle, et 4) répertorier le processus disciplinaire pour les violations de la politique.

Champ d'Application

Cette politique s'applique à tous les travailleurs à distance, employés permanents et à temps partiel, sous-traitants, bénévoles, fournisseurs, stagiaires et/ou toute personne ayant accès aux systèmes électroniques, informations, logiciels et/ou matériel informatique de GlycoNet et SIG.

Données Confidentielles

GlycoNet et SIG définissent les "données confidentielles" comme :

- Informations financières non publiées et classifiées
- Informations sur les clients, les fournisseurs et les actionnaires
- Clients prospects et données relatives aux ventes
- Brevets, processus commerciaux et/ou nouvelles technologies
- Mots de passe, affectations et informations personnelles des employés
- Contrats d'entreprise et documents juridiques

Sécurité de l'équipement

Utilisation de l'entreprise

Pour assurer la sécurité de tous les appareils et informations fournis par l'entreprise, les employés de GlycoNet et SIG sont tenus de :

- Garder tous les appareils fournis par l'entreprise, y compris les tablettes, les ordinateurs et les appareils mobiles, protégés par un mot de passe (minimum de 8 caractères)
- Sécuriser tous les appareils concernés avant de quitter leur bureau
- Obtenir l'autorisation de la direction (par exemple, le PDG de GlycoNet, le Directeur d'un nœud) avant de retirer les appareils des locaux de l'entreprise
- S'abstenir de partager des mots de passe privés avec des collègues, des connaissances personnelles, des cadres supérieurs et/ou des actionnaires
- Mettre régulièrement à jour les appareils avec le dernier logiciel de sécurité

Sécurité du Courrier Électronique

La protection des systèmes de messagerie est une priorité élevée, car les e-mails peuvent entraîner des vols de données, des fraudes et transporter des logiciels malveillants tels que des vers et des bogues informatiques. Par conséquent, GlycoNet et SIG exigent que tous les employés :

- Vérifient la légitimité de chaque e-mail, y compris l'adresse e-mail et le nom de l'expéditeur
- Évitent d'ouvrir des e-mails et des pièces jointes suspects et de cliquer sur des liens
- Cherchent pour des erreurs grammaticales importantes
- Évitent les titres et les liens de piège à clics
- Contactent le service informatique en cas d'e-mails suspects

Transfert de Données

GlycoNet et SIG reconnaissent les risques de sécurité liés au transfert de données confidentielles à l'interne et/ou externe. Pour minimiser les risques de vol de données, tous les employés doivent :

- S'abstenir de transférer des informations classifiées aux employés et à des tiers
- Ne transférer des données confidentielles que sur les réseaux GlycoNet ou SIG
- Obtenir l'autorisation nécessaire de la haute direction
- Vérifier le destinataire des informations et s'assurer qu'il a mis en place les mesures de sécurité appropriées
- Adhérer à l'accord de confidentialité de GlycoNet et SIG
- Alerter immédiatement le service informatique de toute violation, logiciel malveillant et/ou fraudes

Mesures Disciplinaires

La violation de cette politique peut entraîner des mesures disciplinaires pouvant aller jusqu'au licenciement. Les protocoles disciplinaires de GlycoNet et SIG sont basés sur la gravité de la violation. Les violations non intentionnelles ne justifient qu'un avertissement verbal, les violations fréquentes de même nature peuvent conduire à un avertissement écrit, et les violations intentionnelles peuvent entraîner une suspension et/ou licenciement, selon les circonstances du cas.