Cybersecurity Policy

Introduction

The risk of data theft, scams, and security breaches can have a detrimental impact on a company's systems, technology infrastructure, and reputation. As a result, GlycoNet has created this policy to help outline the security measures put in place to ensure information remains secure and protected.

Purpose

The purpose of this policy is to: 1) protect GlycoNet and GlycoNet Integrated Services (GIS) data and infrastructure, 2) outline the protocols and guidelines that govern cybersecurity measures, 3) define the rules for company and personal use, and 4) list the disciplinary process for policy violations.

Scope

This policy applies to all GlycoNet and GIS's remote workers, permanent, and part-time employees, contractors, volunteers, suppliers, interns, and/or any individuals with access to the company's electronic systems, information, software, and/or hardware.

Confidential Data

GlycoNet and GIS defines "confidential data" as:

- Unreleased and classified financial information
- Customer, supplier, and shareholder information
- Customer leads and sales-related data
- Patents, business processes, and/or new technologies
- Employees' passwords, assignments, and personal information
- Company contracts and legal records

Device Security

Company Use

To ensure the security of all company-issued devices and information, GlycoNet and GIS employees are required to:

- Keep all company-issued devices, including tablets, computers, and mobile devices, password-protected (minimum of 8 characters)
- Secure all relevant devices before leaving their desk
- Obtain authorization from management (e.g., GlycoNet CEO, Node Manager) before removing devices from company premises
- Refrain from sharing private passwords with coworkers, personal acquaintances, senior personnel, and/or shareholders
- Regularly update devices with the latest security software

Email Security

Protecting email systems is a high priority as emails can lead to data theft, scams, and carry malicious software like worms and bugs. Therefore, GlycoNet and GIS require all employees to:

- Verify the legitimacy of each email, including the email address and sender name
- Avoid opening suspicious emails, attachments, and clicking on links
- Look for any significant grammatical errors
- Avoid clickbait titles and links
- Contact the IT department regarding any suspicious emails

Transferring Data

GlycoNet and GIS recognizes the security risks of transferring confidential data internally and/or externally. To minimize the chances of data theft, all employees are to:

- Refrain from transferring classified information to employees and outside parties
- Only transfer confidential data over GlycoNet or GIS networks
- Obtain the necessary authorization from senior management
- Verify the recipient of the information and ensure they have the appropriate security measures in place
- Adhere to GlycoNet and GIS' confidentiality agreement
- Immediately alert the IT department of any breaches, malicious software, and/or scams

Disciplinary Action

Violation of this policy can lead to disciplinary action, up to and including termination. GlycoNet and GIS' disciplinary protocols are based on the severity of the violation. Unintentional violations only warrant a verbal warning, frequent violations of the same nature can lead to a written warning, and intentional violations can lead to suspension and/or termination, depending on the case circumstances.