Synoligo BIOTECHNOLOGIES
101 Southcenter Court, Suite 800, Morrisville, NC 27560 USA
Phone +1 (919)-650-1014
www.synoligo.com | info@synoligo.com

Synoligo Incident Response Policy

Overview

Our corporate policy discourages use of personal devices for company business to safeguard both company and employee's data and devices. Use of personal computing devices is prohibited without written authorization from the CEO and CTO, and should only be done where required. This policy applies to employee owned mobile phones, tablets (i.e. iPads, Android), laptops and desktop computers.

Policy

This policy applies to all employees, vendors and partners who are granted access to corporate data and applications.

Corporate data and applications are critical assets to the company's business. Applications must be used according to their established Terms of Service, and company data must be properly stored, secured, and backed up to ensure it is not lost or stolen. The company's primary approach is to assign company owned laptop or desktop computers, and use of all personal computing devices should be avoided unless using company owned cloud hosted solutions.

Incident Definition

Incidents requiring a response under this policy include the following:

- Denial of Service
- Phishing
- Unplanned downtime*
- Loss/Theft*
- Unauthorized Access*
- Malware/Ransom Ware*
- Unauthorized Use/Disclosure*
- Inadvertent Site Security Violation*

Information Security Incident Report

With the exception of Denial of Service and Phishing attempts, employees shall report all incidents to Information Technology. The Information Security Incident Report Form outlines basic user information, time/date of incident, and a brief description of the incident. The form also documents measures taken to correct the incident. Denial of Service and Phishing attempts can be frequent and notification to Information Technology can be via simple email providing basic information.

Unplanned Downtime

Unplanned downtime can occur when a device is not functioning properly. User shall report extended periods of downtime to their supervisor and Information Technology. Information Technology shall investigate the cause and mitigate as possible.

Loss/Damage of Company Equipment

SynOligo BIOTECHNOLOGIES
101 Southcenter Court, Suite 800, Morrisville, NC 27560 USA
Phone +1 (919)-650-1014
www.synoligo.com | info@synoligo.com

In the event that company equipment is damaged, stolen, or otherwise lost, employee shall notify Information Technology of the loss immediately. If stolen, a police report may be required.

All other losses listed

Company uses advanced software to protect against Malware and/or Ransomware. Where software detects the presence of Malware/Ransomware, user shall report to Information Technology. Information Technology maintains records via software tools of attacks. In the event the attack becomes a full breach where data is either held ransom (I.e. encrypted by a 3rd party to induce the organization to pay for its release), the following process shall be followed:

Breach

In the event of a breach, the immediate priority is to block the breach. Information Technology's primary responsibility is to secure Company data. As soon as feasible, Information Technology shall notify the CEO and CTO. This should be done as quickly as possible without sacrificing the ability to respond immediately. Once the breach has been secured, a full investigation of the breach occurs. This investigation includes a full evaluation of what data, if any, has been compromised. Depending on the type or extent of data breached, department leadership will be involved to assess the potential loss.

Information Technology shall prepare a report to include the following:

- Brief description of the event, the measures taken to mitigate, user(s) involved or affected, whether systems were breached and what data or operations have been compromised.
- Relevant policies regarding data protection and system usage for additional details.
- Mitigation measures taken
- Extent of breach and data compromised
- This policy applies for breaches reported both in-house and by third parties.

Xibo Li

CEO

January 2024