Cyber Security and Data Privacy 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, Balaxi Pharmaceuticals Limited ("Balaxi") 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:

(a) protect Balaxi's data and infrastructure;
(b) outline the protocols and guidelines that govern cyber security measures;
(c) define the rules for company and personal use; and
(d) list the company's disciplinary process for policy violations.

Scope:

This policy applies to all of Balaxi's employees, contractors, volunteers, suppliers, interns, and/or any individuals with access to the company's electronic systems, information, software, and/or hardware.

Confidential Data:

Balaxi defines "confidential data" as:

(a) Unpublished and classified financial information.
(b) Customer, supplier, and shareholder information.
(c) business processes, and/or new technologies.
(d) Employees' passwords, assignments, and personal information.
(e) Company contracts and legal records.

Device Security:

Company Use:

To ensure the security of all company-issued devices and information, Balaxi's 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 the Office Manager and/or IT 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.

Personal Use:

Balaxi recognizes that employees may be required to use personal devices to access company systems. In these cases, employees must report this information to management for record-keeping purposes. To ensure company systems are protected, all employees are required to:

- Keep all devices password-protected (minimum of 8 characters).
- Ensure all personal devices used to access company-related systems Share password protected.
- Install antivirus software.
- Regularly upgrade antivirus software.
- Lock all devices if left unattended.
- Ensure all devices are protected at all times.
- Always use secure and private networks.

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, Balaxi requires 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.
- Avoid clickbait titles and links.
- Contact the IT department regarding any suspicious emails.

Transferring Data:

Balaxi recognizes the security risks of transferring confidential data internally and/or externally. To minimize the chances of data theft, we instruct all employees to:

- Refrain from transferring classified information to employees and outside parties.
- Only transfer confidential data over Balaxi's networks.
- Obtain the necessary authorization from senior management.
- Verify the recipient of the information and ensure they have the appropriate security measures in place.
- 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. Balaxi's 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.

__xx__