SABINA

IT Security Policy

Sabina Public Company Limited and Its Subsidiaries

1. Objective

To protect the organization's data, systems, and resources from unauthorized access, cyberattacks, and security breaches, as well as to safeguard the privacy of customers' and employees' personal information.

2. Scope

This policy applies to all employees, contractors, temporary staff, and any individuals authorized to access the organization's systems or information.

3. User Account Management Policy

- All user accounts must be approved by the department manager.
- Access rights for each account must be assigned based on job responsibilities and must be revoked immediately when the individual leaves the position or resigns.
- Passwords must be at least 8 characters in length, containing uppercase letters, lowercase letters, numbers, and special characters, and must be changed every 90 days.

4. Access Control Policy

- Access to the organization's network from external sources must be through a VPN and require authentication.
- Access rights to the organization's systems and applications must be assigned based on job responsibilities (Role-Based Access Control).

5. Acceptable Use Policy

- Employees may use the organization's equipment and resources for business purposes only. Use for personal purposes or for activities that may pose a risk to the security system is strictly prohibited.
- The installation of software or applications not authorized by the IT department is strictly prohibited.

SABINA PUBLIC COMPANY LIMITED
บริษัท ซาบีน่า จำกัด (มหาชน)
12 ARUN-AMARIN RD., ARUN-AMARIN, BANGKOKNOI, BANGKOK 10700, THAILAND.
12 ถนนอรุณอมรินทร์ แขวงอรุณอมรินทร์ เขตบางกอกน้อย กรุงเทพฯ 10700
(02) 422-9400
WWW.SABINA.CO.TH

6. Backup Policy

- All critical data must be backed up automatically on a daily basis, and the backup must be stored in a secure location separate from the primary system.
- Data recovery tests must be conducted regularly, at least every six months, to ensure that the backup can be used effectively in case of an emergency.

7. System Update Policy

- All software and operating systems must be updated regularly, with priority given to security patches.
- The IT department must regularly inspect software to ensure that the systems are secure and free from vulnerabilities.

SABINA PUBLIC COMPANY LIMITED
บริษัท ซาบีน่า จำกัด (มหาชน)
12 ARUN-AMARIN RD., ARUN-AMARIN, BANGKOKNOI, BANGKOK 10700, THAILAND.
12 ถนนอรุณอมรินทร์ แขวงอรุณอมรินทร์ เขตบางกอกน้อย กรุงเทพฯ 10700
(02) 422-9400
WWW.SABINA.CO.TH