Cybersecurity Policy

Thai Poly Acrylic Public Company Limited ("the Company") recognizes the risks associated with cybersecurity threats, including attacks, data breaches, cyber espionage, and other evolving threats. The Company prioritizes preventive measures and risk controls to mitigate potential damages to computer and information systems, ensuring business continuity and safeguarding the Company's reputation.

This Cybersecurity Policy serves as a framework for the effective governance and management of organizational information technology to prevent, address, and reduce the risks of various cybersecurity threats. It aligns with good governance principles and international standards.

Cybersecurity Measures

Corporate and Employee Responsibilities

1. Employees and business partners must not engage in actions that compromise information systems.
2. The Company will implement measures to ensure the safety of computer equipment, telecommunications systems, and related systems, preventing damage or misuse.
3. Measures will ensure data security, reliability, and continued functionality of critical systems and information.
4. Adherence to copyright laws and regulations is mandatory.
5. Employees, contractors, or third parties must protect the information and systems they access.
6. Incidents violating this policy must be reported following Company protocols.

Security Organization

1. Designate specific personnel responsible for IT security.
2. Ensure incident reporting is conducted according to the Company’s procedures.

Asset Control

Manage IT assets with clear usage requirements and implement security measures for access.

Personnel Security

Employees are responsible for maintaining the security and privacy of computers and devices.

Physical and Environmental Security

1. Computers and network equipment must be protected from unauthorized access.
2. Critical business-related equipment must be placed in secure environments.

Computer Management

1. Establish backup systems for all computers and networks.
2. Regularly back up data and software to ensure service continuity.
3. Control and protect essential media such as tapes, disks, and other removable storage devices.

Virus Control

Implement mechanisms to prevent malicious software modifications and computer viruses.

Data Exchange

Approve and control data exchanges at critical organizational points.

System Access Control

Information systems and network services access must be authorized, with user permissions granted and approved by the IT Manager.

Third-Party Access Security

1. Third-party IT system access must comply with approval processes.
2. Risks from third-party access must be assessed and documented, with written agreements signed.
3. Server room access is restricted to authorized personnel only, controlled via fingerprint scans or Taff systems.

System Development and Maintenance

System applications must be defined, approved by the system owner, and incorporate designed security controls.

Compliance

1. All employees must comply with the Company's IT policies, relevant laws, and regulations.
2. IT equipment must only be used for approved purposes.
3. Conduct internal audits and risk assessments for cyber threats at least annually.

Announced on December 23, 2024

.....

(Mr. Surajin Tappanchai)

Managing Director