PANTECH GLOBAL BERHAD

Registration No. 202401009555 (1555405-U)

CYBER RISK POLICY

10 June 2025

1. OBJECTIVE

1.1 The objectives of this Cyber Risk policy include:

a) To establish a framework for managing cyber risks;

b) To ensure confidentiality, integrity and availability of organisation's data;

c) To protect sensitive data from unauthorised access, breaches and cyber threats;

d) To define controls and responsibilities for safeguarding the organisation's digital assets;

e) To enhance organisational resilience against evolving cybersecurity threats.

2. SCOPE

2.1 Internal Users (Employees)

- This Policy applies to all employees of Pantech Global Berhad ("**Pantech Global**" or "**the Company**") and all of its respective subsidiaries (collectively referred to as "**the Group**") who have access to the Group's digital assets, systems and data spaces.
- It covers the employees' responsibilities related to the processing, storage and transmission of sensitive data, including personal, financial and operational information.
- All internal users must adhere to the guidelines (including but not limited to IT Policies and Procedures and any memo issued by IT Department) for data access, usage and protection to ensure compliance with security protocols.

2.2 External Users (Contractors, Vendors and Third Parties)

- This Policy also applies to contractors, vendors and other external parties granted access to the Group's digital assets, systems or data.
- External users must comply with the Group's data security and privacy standards, particularly when handling, storing or processing organisational data.

3. GOVERNANCE AND OVERSIGHT

The governance of this Policy is structured to ensure effective management and accountability across all organisation levels within Pantech Global, with ultimate oversight resting with the Board of Directors.

3.1 Board of Directors

The Board of Directors ("**the Board**") holds overall responsibility for overseeing the implementation and effectiveness of this Cyber Risk Policy. The Board ensures adequate resources are allocated for cybersecurity measures and that the organisation complies with relevant regulatory requirements, including data privacy and cyber risk standards.

3.2 Implementation

The Chief Financial Officer ("**CFO**") is responsible for overseeing the execution of this Policy and reports directly to the Board. The CFO coordinates with the Information Technology ("**IT**") Department to ensure that necessary technical controls and cybersecurity measures are in place to protect digital assets.

IT Managers are responsible for the day-to-day implementation of cybersecurity measures and the management of the Group's digital infrastructure. IT Managers are also tasked with maintaining and updating this Policy and other relevant internal guidelines, monitoring for threats, responding to cyber incidents, ensuring compliance with security protocols, and coordinating cybersecurity training programs.

4. CYBERSECURITY CONTROLS

Pantech Global implements a range of cybersecurity controls designed to safeguard its data and digital assets from cyber threats. These controls are aimed to prevent, detect and respond to security incidents.

4.1 Preventive Controls

- **Access Control Measures**: Strict access controls are implemented to ensure only authorised personnel can access data and critical systems. These include multi-factor authentication, password management policies, and role-based access controls.
- **Software and Patch Management:** Regular updates and patches to be applied to software, systems and applications to address vulnerabilities and protect against known cyber threats.

4.2 Detection and Monitoring

- **Intrusion Detection Systems (IDS)**: Real-time monitoring tools are in place to detect any unauthorised access attempts or anomalies in the organisation's networks and systems.
- **Threat Intelligence**: The organisation continuously gathers and analyses threat intelligence from both internal sources and external partners to identify emerging cyber threats.
- **Security Information and Event Management (SIEM)**: Automated tools are used to log security events, enabling further analysis and detection of potential security incidents.

4.3 Incident Response and Recovery Plans

- **Incident Response Procedures**: An incident response plan outlines the steps to be taken in the event of a security breach or cyber-attack. This includes roles, responsibilities, and communication protocols.
- **Data Backup and Recovery:** Regular data backups are conducted to ensure critical data can be recovered in the event of an incident. The recovery plan includes steps to restore operations quickly and minimise business disruption.

5. AWARENESS AND TRAINING

To maintain a strong cybersecurity culture, continuous training and awareness programs are essential. The IT Department will recommend suitable training programs to the Human Resources ("**HR**") Department, which is responsible for coordinating and initiating necessary trainings to equip employees with the knowledge and skills to recognise and respond to potential cyber threats.

6. INCIDENT REPORTING AND RESPONSE

6.1 Incident Reporting

Any employee, contractor, or third party who detects or suspects a cybersecurity incident (e.g. data breach, unauthorised access, malware infection) must immediately report the issue by sending email to the designated incident reporting address: cyberincident@pantechglobal.com

The report should include:

- A brief description of the incident;
- The time and date when the incident was noticed;
- The system or data involved;
- Any immediate actions taken by the reporting party.

6.2 Investigation and Immediate Action

Upon receiving the incident report, the IT Department will initiate an immediate investigation to verify and assess the scope and severity of the incident. The IT Department will gather evidence, determine the impact, and identify the root cause of the incident. Simultaneously, the IT Manager will lead the relevant team to implement immediate containment measures to prevent further damage or spread of the threat, following the organisation's Incident Response Plan, which includes:

- Eradication of the threat (e.g., removing malware, patching vulnerabilities).
- Recovery of affected systems or data (e.g., restoring from backups).
- Post-incident monitoring to ensure that the threat has been fully mitigated.

6.3 Reporting

Once the initial investigation is completed, the IT Manager will promptly report the findings to the management on the summary of the incident, actions taken, and any identified risks or vulnerabilities. Management will then determine further actions, such as notifying affected parties or seeking external consultants to assist with recovery efforts.

Critical or high-impact incidents will be reported to the Board, including the Sustainability Management Committee, during the regular updates. The report provided will include an outline of the incident, response actions, and recommended improvements. The Board will review the incident and ensure that corrective measures are taken to prevent future occurrences, including updates to policies, controls, or training programs.

7. MONITORING AND REVIEW

7.1 Audit

Audit can be conducted to assess the effectiveness of cybersecurity controls and evaluate the organisation's overall cyber risk posture, ensuring compliance with internal policies and guidelines. When necessary, independent third-party auditors may be engaged to provide an objective assessment of key risk areas, evaluating the organisation's cybersecurity practices and identifying potential vulnerabilities.

The results of audit will be reported to the Board. Any gaps or vulnerabilities identified during the audit will be addressed through corrective action plans, and follow-up audits will be conducted to ensure that issues have been resolved.

7.2 Policy Review and Updates

This Policy will be reviewed where necessary to ensure that it remains up-to-date with evolving threats, business needs, and regulatory changes. Feedback from audit assessments and incident reviews will be incorporated into updates to improve cybersecurity practices.