TONG HERR RESOURCES BERHAD
Registration No. 199701016642(432139-W)

INFORMATION SECURITY & DATA PROTECTION POLICY

1. Introduction

This policy establishes guidelines for the secure and responsible use of Tong Herr Resource Bhd's ("THR" or "the Company"), including its subsidiaries ("the Group") Information Assets to protect the Company, its stakeholders, and business operations from information security and data protection risks. This policy supports the Group's sustainability and enterprise risk management framework.

2. Definitions

Users: Any individual granted access to the Company's Information Assets, including permanent and temporary employees, contractors, agency staff, consultants, suppliers, customers, and business partners.

Information Assets: All hardware, software, networks, applications, and data owned, managed, or used by the Company, whether on-premise or remote.

3. Scope

This policy applies to all Users and Information Assets within the Company. Where specific policies exist, the more specific policy shall prevail. However, in all other respects, both policies shall remain applicable.

This policy governs only the internal use of the Company's Information Assets and does not extend to the use of our products or services by customers or external third parties. Staff responsible for monitoring and enforcing this policy shall ensure ongoing compliance with applicable laws and regulations.

4. Use of Information Assets

All data stored, processed, or transmitted using the Company's Information Assets is the exclusive property of the Company. Users should be aware that, except where required by applicable laws and regulations, the Company cannot guarantee the confidentiality of any information stored on or transmitted through its Information Assets.

The Company's Information Assets are provided to support and enhance business operations. Limited personal use is generally permitted, provided that such use does not adversely affect the productivity of the user or their colleagues, compromise information security, or result in significant costs to the Company, other than minor, incidental expenses (e.g. a brief personal phone call).

The Company places trust in its employees to exercise sound judgment in determining what constitutes an acceptable level of personal use. In cases of uncertainty, employees should seek guidance from their manager.

Sensitive or vulnerable information must be adequately protected to prevent unauthorized access. Protection measures may include encryption, access restrictions, and secure storage, provided that such measures do not hinder access by authorized personnel.

The Company reserves the right to monitor, access, and review the use of its Information Assets and any data stored, processed, or transmitted through them at any time. Such monitoring may include, subject to applicable privacy and data protection laws, the review of user emails, data files, system logs, and access histories.

The Company also retains the right to conduct regular audits of its networks and systems to ensure ongoing compliance with this policy.

5. Data Security
If data stored, processed, or accessed using the Company's Information Assets is classified as confidential, it must be clearly identified either within the data itself or through the user interface of the relevant system or application. Users are responsible for taking appropriate measures to prevent unauthorised access, disclosure, alteration, or loss of such information.

Employees are expected to exercise sound judgment when determining what qualifies as confidential information. Where there is uncertainty, employees must treat the information as confidential and seek guidance from management or the MIS department. Confidential information, whether formally designated or reasonably considered as such, must not be sent, uploaded, transferred to portable media, or moved to non-THR Information Assets unless explicitly authorised as part of official duties or approved by management and subject to applicable security control.

Users are required to remain vigilant against malware risks, including viruses, spyware, Trojan horses, rootkits, worms, and backdoors, which may compromise the Company's Information Assets. Any actual or suspected malware infection or security incident must be reported immediately to the MIS department for investigation and remedial action.

6. Backup Storage
The Company shall implement appropriate data backup and recovery measures to ensure data integrity, availability, confidentiality, and business continuity.

7. Unacceptable Use
All employees are expected to exercise sound judgment when determining what constitutes unacceptable use of the Company's Information Assets. While the following examples illustrate behaviours that are deemed unacceptable, this list is not exhaustive. If an employee believes that deviating from these guidelines is necessary to perform their role, they must consult with and obtain prior approval from their manager before proceeding.

Unacceptable Use Includes:-

- **Illegal Activities:** Engaging in theft, computer hacking, malware distribution, violations of copyrights and patents, or using illegal services. This also encompasses activities that breach data protection regulations.
- **Detrimental Activities:** Actions that negatively impact the Company's success, such as sharing sensitive information (e.g., research and development data, customer lists) outside the Company or defaming the Company.
- **Personal Benefit Activities:** Activities that are solely for personal gain and adversely affect the business's operations, including actions that degrade network performance (e.g., streaming video, playing networked video games).
- **Reputationally Harmful Activities:** Engaging in activities that are inappropriate for association with the Company or that damage the Company's reputation, including pornography, gambling, hate speech, bullying, and harassment.
- **Security Protocol Violations:** Circumventing or undermining the security controls, safeguards, or protocols implemented to protect the Company's Information Assets.

8. Duties of the Authorized Outsourcing Information Systems Service Provider
In addition to the responsibilities outlined elsewhere in this Policy, the authorised outsourced service provider ("Service Provider") shall be responsible for the following duties in relation to the Company's Information Assets: -

- **System Maintenance:** Regularly maintain and update supported operating system resources, including servers. Where systems have reached end-of-life, suitable compensating controls shall be applied to mitigate security risks.

- **Gateway/Firewall Management:** Periodically maintain and update the gateway and firewall operating systems to protect against security threats.
- **Anti-Virus Management:** Install and renew anti-virus program packages as necessary. Configure anti-virus programs to scan for viral signatures and detect infectious agents on access. Ensure that comprehensive scans are conducted at least once a month.
- **Activity Logging:** Maintain a detailed activity log-book on a quarterly basis, documenting all performed activities to ensure accountability and traceability.
- **Incident Reporting:** Report security incidents to the Company's Management through mis_2@tong.com.my. Implement appropriate corrective actions to address and mitigate security threats.
- **System Review and Recommendations:** Conduct periodic reviews of computer system hardware and software, providing recommendations to align with the current working environment and technological advancements.
- **Technical Support:** Provide technical support for hardware, software, and system-related issues to ensure smooth operation and timely resolution of issues affecting the Company's Information Assets.
- **Database and Application Management:** Do not remove or delete any database or applications from the Company's Information Assets without prior approval from the Head of Department.

9. Enforcement

The Company has a zero-tolerance policy towards any misuse of its Information Assets. Any employee found to have violated this policy, including failing to exercise reasonable judgment regarding acceptable use, will face disciplinary action. Each case will be assessed individually; however, employees should be aware that serious violations may result in termination of employment.

The use of the Company's resources for illegal activities is strictly prohibited and will generally result in summary dismissal. The Company is committed to cooperating fully with any criminal investigations and legal proceedings that arise from such activities. Enforcement actions are undertaken in accordance with the Company's disciplinary procedures and applicable laws.

This policy was reviewed by The Management Team of the Company on 26 March 2026.