Masteel

MALAYSIA STEEL WORKS (KL) BHD

197101000213 (7878-V)

INFORMATION TECHNOLOGY POLICY

INFORMATION TECHNOLOGY POLICY

1. Introduction

This policy establishes guidelines for the responsible and secure use of Malaysia Steel Works (KL) Bhd's ("Masteel") IT systems, safeguarding the company, its employees, customers, and partners from the risks associated with misuse. Whether intentional or accidental, misuse can result in serious consequences, such as malware infections, legal and financial liabilities due to data breaches, and operational disruptions caused by system failures.

All Masteel employees are responsible for ensuring the security and appropriate use of IT systems and data. Should there be any uncertainty about the policy or its relevance to their duties, employees are encouraged to seek guidance from their manager or the Risk Management Officer

2. Definitions

Users : Any individual granted access to Masteel's IT systems, including permanent and temporary employees, contractors, agency staff, consultants, suppliers, customers, and business partners.

Systems: Encompasses all IT equipment connected to Masteel's corporate network or accessing its applications. This includes, but is not limited to, desktop computers, laptops, smartphones, tablets, printers, network infrastructure, software, and data storage devices.

3. Scope

This policy applies universally to all Users and Systems within Masteel. In certain cases, specific policies may exist for particular Users or Systems; where conflicts arise, the more specific policy will take precedence. However, in all other respects, both policies shall remain applicable.

This policy governs only the internal use of Masteel's systems 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 are required to ensure compliance with all relevant local laws and regulations at all times

4. Use of IT Systems

All data stored on Masteel's systems is the exclusive property of the company. Users should be aware that Masteel cannot guarantee the confidentiality of any information stored on its systems, except where local laws require such protection.

Masteel's IT systems are provided to support and enhance business operations. While limited personal use is generally permitted, it must not negatively impact the productivity

of the user or their colleagues, nor should it result in any significant costs to the company, apart from minor, incidental expenses (e.g., a brief personal phone call).

Masteel 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 encrypted and securely stored to prevent unauthorized access, or at the very least, to make such access extremely difficult. However, these security measures must not obstruct legitimate access by properly authorized individuals.

Masteel reserves the right to monitor the use of its IT systems and the data stored within them at any time. This may include (subject to local privacy laws) reviewing the content of user emails, data files, 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 on Masteel's systems is classified as confidential, it must be clearly marked either within the data itself or in the user interface of the system used to access it. Users are responsible for taking all necessary precautions to prevent unauthorized access to such information.

Employees are expected to use sound personal judgment when determining what qualifies as confidential. Information that is designated as confidential, or which could reasonably be considered as such, must not be sent, uploaded, transferred to portable media, or moved to non-Masteel systems unless explicitly authorized in the course of regular duties.

Users are required to keep their passwords secure and must not share their account access with others. Passwords must adhere to Masteel's secure password policy, which mandates the following:-

- Must be a minimum of six characters in length, combining letters and numbers;
- Must not contain more than two identical consecutive characters; and
- Must not include the user ID as part of the password.

Users are required to diligently safeguard against the risk of malware—such as viruses, spyware, Trojan horses, rootkits, worms, and backdoors—that could potentially infiltrate Masteel's systems. It is imperative that users exercise caution to prevent malware from being imported through any means. Any actual or suspected malware infection must be reported immediately to the IT department for prompt action.

6. Backup Storage

All portable storage media must be distinctly labeled as "Property of Masteel" and may contain proprietary information that must be protected from unauthorised use or access. These hard disks must not be removed from the company's control without proper authorisation. Backup data should be systematically stored at a designated, secure location separate from the primary data sources to mitigate the risk of data loss. Each department is accountable for conducting and documenting weekly backups in accordance with established protocols. This ensures both the integrity and availability of critical data, facilitating prompt recovery in case of system failures or data loss incidents.

7. Unacceptable Use

All employees are expected to exercise sound judgment when determining what constitutes unacceptable use of Masteel's systems. While the following examples illustrate behaviors 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 approval from their manager prior to proceeding.

Unacceptable Use Includes:-

- **Illegal Activities:** Engaging in theft, computer hacking, malware distribution, violations of copyrights and patents, or using illegal or unlicensed software or services. This also encompasses activities that breach data protection regulations.
- **Detrimental Activities:** Actions that negatively impact Masteel'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 Masteel's association or that damage the company's reputation, including pornography, gambling, hate speech, bullying, and harassment.
- **Security Protocol Violations:** Circumventing or undermining the IT security systems and protocols established by Masteel.

8. Duties of the Authorized Outsourcing IT Partner

In addition to the aforementioned responsibilities, the authorized outsourcing IT Partner is tasked with the following duties:-

- **System Maintenance:** Regularly maintain and update all operating system resources, including servers, to ensure optimal performance and security.
- **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 cybercrime@masteel.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 both hardware and software issues to ensure smooth operation and resolve any IT-related problems.
- **Database and Application Management:** Do not remove or delete any database or applications from the computer system without prior approval from the Head of Department.

9. Enforcement

Masteel has a zero-tolerance policy towards any misuse of its systems and resources. 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 Masteel's resources for illegal activities is strictly prohibited and will generally result in summary dismissal. Masteel is committed to cooperating fully with any criminal investigations and legal proceedings that arise from such activities.

This policy was reviewed and approved by The Management Team of Masteel on **28 November 2016**. Subsequently, this policy was revised and improvised on **8 January 2024**.