Information Technology Security Policy

Hastings Technology Metals Ltd (Hastings or the Company) is committed to being a responsible custodian of the data it holds. Hastings recognises the importance of information/data security in relation to its activities and the expectations of key stakeholders in the external environment. Regardless of the form it takes, or means by which it is shared or stored, Company information should always be kept secure and protected from data corruption and theft. This Policy sets out the basis upon which Hastings collects, uses, stores, and discloses information. This seeks to support the evolving requirements for information handling and processing by employees and approved third parties to carry out their respective Hastings roles and responsibilities.

Hastings implements the following commitments:

- Provision of guidelines for the classification and secure handling of information.
- Establish and maintain an IT incident management procedure to ensure any incidents that affect the Company's daily operations are managed effectively and efficiently at the earliest stage.
- A cyber security response team that acts quickly to mitigate the risks and damage associated with emergency cyber security incidents.
- Ensure all software applications are fully supported by the manufacturer.
- Track maintenance contracts for the software in use and under administration.
- Identify technical vulnerabilities and evaluate and mitigate risks to such vulnerabilities.
- Prevent vulnerabilities by having up-to-date, security patched operating systems and securely configured digital devices.
- Promote a workplace culture of reporting actual or potential vulnerabilities and security compromised incidents.
- Preserve confidentiality by only providing access to assets, systems, and information relevant to the position description and authorised personnel.
- Ensuring the confidentiality, security, and integrity of user's personal information in compliance with local privacy laws.
- Ensure that all Company intellectual property is protected as per guidelines.
- Provide IT and cyber security training to relevant information systems personnel in the Company.
- Identify auditable events and monitor and conduct audits of information system resource usage for identity management, ethical behaviour and threat monitoring.
- Manage all changes to IT systems and applications to prevent unscheduled disruption, data corruption, theft, or loss.
- Procure review of any new information or operation technology (IT & OT) by Hastings IT Department and, if recommended, approval by the Executive Chairman or the Board as appropriate to ensure compliance with Hastings's system integration and security requirements. Any modifications to existing technology must go through IT change management.

- Adhere to Australian Signals Directorate, Cyber Security Centre Essential Eight Model.

This policy should be read alongside all other Company policies including but not limited to, the Acceptable Use of ICT Resources Policy, Code of Conduct, and the Privacy Policy.

This Policy will be reviewed every two years or as required.

Charles Lew
Executive Chairman
Approved by the Board (20 September 2023)