IT POLICY

KHG-POL-ADM-1211

This Policy sets out the Company's policy in relation to using and accessing its company systems, including the internet and email.

This policy applies at all times, including when you are working at home, at a client's premises or at any other place.

Use of IT resources and surveillance

- Any email use, internet use or voice communication content must not be detrimental to, nor adversely affect, the reputation or operations of the Company, its employees or customers. Employees are responsible and accountable for their email use, internet use and voice communications, including the content of these.
- Any social media use in a personal capacity must also not be detrimental to, nor adversely affect, the reputation or operations of the Company, its employees or customers. You must not present or communicate on behalf of the Company on social media without the prior authorisation of the Company.
- Any social media use in a work or personal capacity must comply with this policy.
- All access to and usage of the Company's data, or any email or voice communications using company equipment or resources may be monitored or accessed by authorised employees. The Company also reserves the right to monitor, access and record internet usage and web browsing activity of all employees in the workplace or using company resources.

General Use

At all times, you must also comply with the following:

- You may use the Company's IT resources for business use and reasonable personal use, provided that such use does not bring the company or its related entities into disrepute and is not contrary to this policy or to any applicable law. Personal use must be kept to a minimum and must not prevent you from properly performing your duties;
- You must not use any of the Company's property or IT resources to deal with illegal, offensive or defamatory material including by creating, downloading, transmitting, forwarding, copying or saving illegal, offensive or defamatory material;
- You must not use of the Company's property or IT resources to act in a manner that could expose the Company, staff members, customers or other related parties to loss or liability;
- You must not use any of the Company's property or IT resources to bully, harass or discriminate against any person. This includes by sending defamatory, threatening or obscene messages to any person, distributing pornography or other offensive material and/or sending emails that denigrate or ridicule any person (whether or not member of staff). Such behaviour will be treated as serious misconduct and result in disciplinary action which may include summary termination;
- You must protect your email account including by keeping your password private and not letting other people use it or know what it is. You should log off or lock your computer when leaving your computer for an extended period;

- You must not represent your personal opinions as those of the Company; and You must not send or disclose confidential or proprietary information belonging to the Company except as strictly necessary in the proper performance of your duties.

Security

- The Company's information systems and data must be securely protected by passwords or other authentication methods. Employees with access to the Company's information systems and data are held responsible for the security and secrecy of their own passwords, or any other authentication verification data.
- Passwords are not to be written or displayed in a public area, or shared in an email, or other form of electronic communication. Passwords or any other authentication verification tools or devices must never be shared, loaned or sold.
- Employees must not act in a way that is detrimental to, or adversely affects, the safety and security of the Company's information systems.

Data Governance

- Any data generated during business operations, or created by employees for any purpose that relates to the function of the Company's operations or for the Company's benefit, is the property of the Company.
- All employees of the Company must ensure appropriate data handling procedures are followed to uphold the security and integrity of the Company's data. An employee's access to and usage of data should conform to the individual's job function and/or description.
- Any data that is considered to be reasonably sensitive, vulnerable or subject to privileges should be securely encrypted. Release of data should be subject to authorisation by the Company in compliance with any confidentiality procedures.

Company-issued IT equipment

- Company resources and equipment, including IT equipment is to be respected by employees. IT equipment includes but is not limited to company-issued phones, laptops, tablets, and any other electronic equipment issued by the Company to employees. All IT equipment belongs to the Company and must be returned by the employee as soon as reasonably possible when requested by the Company.
- All employees should take steps to secure IT equipment when such equipment is not in use, including when this is taken outside of the workplace.
- All IT equipment (Laptops, monitors, docking stations, mobile phones, tablets, etc) is to be purchased and issued by Head Office only. This is to ensure and maintain inventory of all assets, tracking their usage, maintenance, compatibility, reliability, and warranty.

Wui-Lee Tan

Wui-Lee Tan
Executive General Manager

Review Date: 08/04/2024