IT POLICY

1. Email

All email is the property of the Company and may be monitored and audited by appropriately authorised Company personnel. All existing Company policies apply to email usage.

Email 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 use of email, and for the format and content of messages sent by them.

At times you may receive emails which you have not solicited or encouraged and which breach Company email standards. Such emails must not be forwarded. They must be deleted, and reasonable steps must be taken to prevent a re-occurrence.

2. Voice Communication

All voice communications, including but not limited to cellular telephones, telephones, voicemail messages and radios, are the property of the Company and may be monitored and audited by appropriately authorised Company personnel. All existing Company policies apply to voice communication usage.

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 use of voice communication, and the content of messages communicated by them.

At times you may receive voice communications which you have not solicited or encouraged and which breach Company standards. Such voice communication must not be forwarded. They must be deleted if recorded, and reasonable steps must be taken to prevent a re-occurrence.

3. Internet

As a business tool, the internet represents a considerable commitment of telecommunications, networking, software and storage facilities. It therefore needs to be used primarily for business purposes. Unnecessary or unauthorised internet usage can severely compromise the Company, so the Company reserves the right to monitor and record internet usage and web browsing activity of all of its employees while at work. All existing Company policies also apply to internet usage.

Internet activity must not be detrimental to, nor adversely affect, the reputation and operations of the Company, its employees or customers.

4. Prohibited email, voice communication and internet activity

Unacceptable use of the Company's email addresses, voice communications or internet services by an employee includes, but is not limited to:

(a) harassment of any group or individual;

(b) accessing, downloading or distributing any pornographic or other offensive material;

(c) trafficking in confidential customer or client information;

(d) broadcasting information of a defamatory nature;

(e) hacking or entering into any email or voice communications that may be deemed unlawful;

(f) propagation of SPAM (unsolicited bulk email or voicemail);

(g) distribution of material or information that is defamatory, abusive, menacing, threatening, harassing or illegal under legislation where transmissions are sent from, viewed or received;

(h) transmission of unsolicited mail or voicemail, advertising material or any other material which is offensive or indecent or otherwise contrary to law or relevant Company policies;

(i) unauthorised copy or distribution of material such as copyrighted works or confidential information;

(j) commission of a crime, activity in the course of commission of a crime or for unlawful purpose;

(k) activities carried out in a manner which could expose the Company, or any entity with which it conducts business, to loss or liability;

(l) actions that may damage the network or systems or cause impairment of their quality and integrity;

(m) sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities;

(n) passing off personal views as representing those of the organisation; and

(o) activity that does not comply with the Company's operating procedures, policies or behavioural standards.

5. Social media

All employees of the Company when participating in social media in personal capacity must not impose any of the following actions:

(a) disclose the Company’s confidential information, proprietary or sensitive information;

(b) use the Company’s logo or branding on any social media platform unless approved by the Company;

(c) communicate anything that might damage the Company’s reputation, brand image, commercial interests, or the confidence of customers;

(d) present or communicate on behalf of the Company in the public domain without the approval of the Company; and

(e) post any material that would directly or indirectly defame, harass, discriminate against or bully any employees or customers of the Company.

6. 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 security and secrecy of their own passwords or any other authentication verification tools.

At no time shall a user write a password down or in any way display it for public review or in any other easily discoverable area or insert passwords in emails or other forms of electronic communication. Passwords or any other authentication verification tools or devices must never be shared, loaned or sold.

Employees must not deliberately act in any way that is detrimental to, nor adversely affect, the safety and security of the Company's information systems. All existing Company security policies also apply.

7. Data governance

Data generated during the business functions or created by employees for any purposes in relation to the functions of, or for the benefits to the Company if the property of the Company. All access to and usage of the Company's data may be monitored and audited by appropriately authorised Company personnel.

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 as reasonably sensitive, vulnerable or subject to privileges shall be securely encrypted. Release of data should be authorised by the Company and in compliance with the confidentiality policies.

8. Company-issued IT equipment

All employees should respect and protect the company's IT equipment. "IT equipment" in this IT policy includes company-issued phones, laptops, tablets and any other electronic equipment issued by the Company to employees. IT equipment belongs to the company and must be returned by the employee as soon as practicable when requested by the Company.

All employees should take steps to secure IT equipment when the IT equipment is not not in use. Employees are responsible for IT equipment whenever they are taken out of the office.

Any employee found to have breached this policy in any way shall be subject to disciplinary action, which may include termination of employment or legal action when appropriate.

If you have any questions, please contact Van Nguyen, HR Manager.