

IT POLICY

GENERAL GUIDELINES

1. Personal Account Responsibility

Users are responsible for the security of their accounts and passwords. Accounts and passwords are normally assigned to single users and are not to be shared with any other person. Users are responsible for any activity carried out under their accounts.

2. Unauthorised Use

Users must not permit or assist any unauthorised person to access the Group's system. Public users are not allowed to use any of the Group's system without appropriate authorisation.

3. Unauthorised Software

No one shall copy, install, or use any software or data files in violation of applicable of the Group's copyrights or license agreements into their computer.

4. Denial of Service (Viruses)

No one shall create, install, or knowingly distribute a computer virus, "Trojan horse," or other surreptitiously destructive program on any of the Group's computer or network facility, regardless of whether any demonstrable harm results.

5. Unauthorised Computer Equipment

Without specific authorisation by the System Administrator, users must not physically or electrically attach any foreign network device including routers, hubs, or wireless access points to the Group's system.

6. Removal of Equipment, Documents & E-mail

No one without specific authorisation shall read, alter, or delete any other person's computer files or electronic mail. This rule applies regardless of whether the operating system of the computer permits these acts. Users also must not remove any of the Group's owned or administered equipment.

7. Security

Users must not defeat or attempt to defeat any of the Group system's security, for example, by 'cracking' or guessing User identifications or passwords.

8. Unauthorised Data Access

Users must not access or attempt to access or change data on the Group's system that they are not authorised to access or change.

9. Modification of Data or Equipment

Without specific authorisation, users of the system must not cause, permit, or attempt any destruction or modification of data or computing or communications equipment, including but not limited to alteration of data, reconfiguration of control switches or parameters, or changes in firmware. This rule protects data, computing, and communications equipment owned by the Group, or any other person or entity. 'Specific authorisation' refers to permission by the Systems Administrator of the equipment or data to be destroyed or modified.

SOCIAL MEDIA GUIDELINES

The Group allows employees to access their personal accounts at work. But, we expect them to act responsibly and ensure their productivity isn't affected. Using social media excessively while at work can reduce efficiency and concentration. Whether employees are using their accounts for business or personal purposes, they may easily get sidetracked by the vast amount of available content.

i. We advise our employees to:

- **Use their common sense.** If employees neglect their job duties to spend time on social media, their decline in productivity will show on their performance reviews.
- **Ensure others know that personal account or statements don't represent our company.** Employees shouldn't state or imply that their personal opinions and content are authorised or endorsed by the Group. We advise using a disclaimer such as "opinions are my own" to avoid misunderstandings.
- **Avoid sharing company & intellectual property** like trademarks on a personal account without approval. Confidentiality policies and laws always apply.
- **Avoid any defamatory, offensive or derogatory content.** It may be considered as a violation of our Group if directed towards colleagues, clients or partners.

ii. Representing our Group

Some employees represent our Group by handling corporate social media accounts or speak on our Group's behalf. We expect them to act carefully and responsibly to protect our Group's image and reputation. Employees should:

- **Be respectful, polite and patient**, when engaging in conversations on our Group's behalf. They should be extra careful when making declarations or promises towards customers and stakeholders
- **Avoid speaking on matters outside their field of expertise** when possible. Everyone should be careful not to answer questions or make statements that fall under somebody else's responsibility
- **Avoid deleting or ignoring comments** for no reason. They should listen and reply to criticism.
- **Never post discriminatory, offensive or libelous** content and commentary
- **Correct or remove** any misleading or false content as quickly as possible

iii. **Disciplinary Consequences**

We'll monitor all social media postings on our corporate account.

We may have to take disciplinary action leading up to and including termination if employees do not follow this policy's guidelines. Examples of non-conformity with the employee social media policy include but are not limited to:

- Disregarding job responsibilities and deadlines to use social media
- Disclosing confidential information through personal or corporate accounts
- Directing offensive comments towards other members of the online community

USAGE OF INTERNET

Internet use, on company time, using Group owned devices that are connected to the Group's network, is authorised to conduct Group business only. Internet use brings the possibility of breaches of the security of confidential Group's information.

Internet use also creates the possibility of contamination to our system via viruses or spyware. Spyware allows unauthorised people, outside of the Group, potential access to Group's passwords and other confidential information.

Removing such programs from the Group's network requires IT staff to invest time and attention that is better devoted to making technological progress. For this reason, and to assure the use of work time appropriately for work, we ask staff members to limit internet usage.

Additionally, under no circumstances may Group owned computers or other electronic equipment, including devices owned by the employee, be used on company time at work to obtain, view, or reach any pornographic, or otherwise immoral, unethical, or non-business-related internet sites. Doing so can lead to disciplinary action up to and including termination of employment.


USAGE OF EMAIL

Email is also to be used for Group's business only. Group's confidential information must not be shared outside of the Group, without authorisation, at any time. You are also not to conduct personal business using any of the Group's computer or email.

Please keep this in mind, also, as you consider forwarding non-business emails to associates, family or friends. Non-business related emails waste company time and attention.

Viewing pornography, or sending pornographic jokes or stories via email, is considered sexual harassment and will be addressed according to our sexual harassment policy. Immediate termination is the most frequent disciplinary action that the Group may take in these cases.

Prepared by :-




19/09/18

AZMI BIN SABRAN

IT EXECUTIVE

Approved by :-



GERALD NG CHENG YEW

GENERAL MANAGER
(OPERATIONS)