IH Digital Group - IT Policies & Procedures

1. **Introduction**
   IH Digital Group ("Company") provides information technology (IT) resources for the shared and responsible use by employees to perform their work. Employees are in turn, expected to use them in an efficient, ethical, professional, secure, and legal manner.

   This policy applies to all IH Digital employees. You must read and sign this Policy as a pre-condition for employment.

2. **General Provisions**
   a. You shall use Company IT resources for authorised business purposes only. Prohibited use includes, but is not limited to political campaigning, solicitation, unauthorised financial gain, or conducting business that has no official relationship with the Company.
   b. Files that are used in the cause of official business are the property of the Company. Under no circumstances may you alter a file that does not belong to you without prior permission from the file's owner or from the Company.
   c. You must not store personal confidential information such as credit / debit card details or passwords on Company IT Resources.
   d. You are not permitted to allow third parties access to Company IT Resources.

3. **IT Security Policy**
   a. All employees are required to sign an IT Security Policy form, agreeing to comply to all IT Security measures outlined by the Company. Employees are allowed to use Company's computers only for authorized work purposes and are not allowed to install any software without permission. Employees are also prohibited from allowing non-employees to have access to Company's computers.
   b. Firewall, antivirus and restricted admin access are activated for all Company's computers to safeguard against hacking. Employees are required to comply by IT Department's instructions to update anti-virus software or safeguard against computer viruses from time to time.
   c. Only the IT Department has access to Company's server. All data is encrypted and with secure transfer.

4. **Right of Company Access**. The Company reserves the right for authorised personnel to access employees' stored information to investigate cases of computing abuse and for systems maintenance purposes.

5. **Disclaimer**. The Company accepts no responsibility for any damage to or loss of data, hardware or software arising directly or indirectly from use of the Company's IT resources or for any consequential loss or damage.

6. **Specific Prohibitions on Use**
   a. Use that attempts to damage the integrity of Company or other IT Resources.
   b. Company IT Resources may not be used for making unauthorised connection to, monitoring of, breaking into, or adversely affecting the performance of IT systems
   c. Access, transmit, store, display or request for inappropriate content such as obscene, pornographic, erotic, profane, racist, sexist, defamatory or offensive materials.
   d. Develop and/or use programmes that may/will harass or harm other users of the system

7. **Unauthorised Access or Use**
    a. **I**t is a violation to use another person's account, with or without that person's permission. You should use only the computer accounts you are authorised to use.
    b. All employees are to use Company-issued laptops or computers only.
    c. You should not attempt to crack, guess and/or capture another person's computer password.
    d. To save/share all office documents and access cloud under the corporate profiles:
        i. Google Drive using Company email profile;
        ii. One Drive using Company email profile.

8. **Use in Violation of Laws.** You must not use your company account in any way that violates the laws of any country. The Company expects its employees to be cognisant with and abide by the provisions stipulated in the Computer Misuse Act (Chapter 50A) and Cybersecurity Act 2018 and the Sedition Act (Chapter 290).

9. **Copyright**.
    a. You are responsible for ensuring that no copyrighted material (including music, film, podcasts, books, games and/or software) is downloaded using, published on, or distributed from company network without the copyright holder's permission.
    b. Civil and criminal penalties apply for violations of the Copyright Act. In addition, unauthorized copying or downloading of software or data from the Company's computers may attract criminal penalties (fines and imprisonment) under the Computer Misuse Act.

10. **Personal Data Protection Laws**. You are responsible for ensuring that the collection, use and disclosure of Personal Data are in compliance with Singapore's Personal Data Protection Act 2012 (PDPA) or the employment country's privacy law. Generally, you should obtain valid consent before they collect, use or disclose Personal Data, unless any exception applies.

11. **Company Licenced Software**. The Company provides one Company Licensed Software license per employee regardless of the number of PCs, desktops, laptops and/or computing devices purchased.

12. **Email and Web Policies. -** the following conduct / actions are prohibited:
    a. harassing, sending pornographic or defamatory materials / messages;
    b. massive or unsolicited emailing;
    c. sending or forwarding of confidential company information via email.
    d. Do not use Company e-mail addresses to send or receive e-mail that does not pertain directly to company business.
    e. Profanity, ethnic slurs, name-calling, sexual harassment or antagonistic / unprofessional communication of any kind will not be tolerated.
    f. Hackers routinely use e-mail and e-mail attachments to distribute destructive programs throughout the Internet and to commit identity theft by tricking e-mail recipients into divulging personal information. Do not open any e-mail attachment unless:
        i. You are certain of the sender's identity;
        ii. It is an attachment you specifically requested the sender mail to you;
        iii. You are familiar with the file format and know that it cannot possibly contain any destructive programming. Microsoft Word (*.doc) and Excel (*.xls) file can contain harmful programs called macros.
        iv. Under no circumstances open files with the extension *.zip or *.exe. These are almost always viruses.
    g. Be suspicious of any e-mail that appears to be from a bank or credit company asking you to go online to confirm personal account information. These counterfeit messages are

designed to trick you into divulging credit card numbers, user names, passwords, etc. Legitimate companies do not ask for this information via e-mail.

13. **Company WIFI** connection strictly for company laptop only. Employee is not allowed to use Company WIFI connect for their own personal mobile or tablet usage.

14. **Loss/Stolen/Damage of IT/Video Equipment**
    a. You are expected to take precautions to ensure that IT Equipment are not stolen, lost, or damaged.
    b. You are not allowed to send your Personal Computer or Video Equipment for repair without written approval.
    c. In case of theft or loss, you must file a police report and submitting to IT on the same day after filing the police report.
    d. If IT/Video Equipment assigned to you are lost, stolen, or otherwise damaged due to negligence and such that they cannot be restored to normal working order, you agreed to pay for the prorated cost of replacement
    Payment Schedule
        - 1 year and below: 100% of purchasing cost
        - 1 year to 2 year: 75% of purchasing cost
        - 2 year to 3 year: 50% of purchasing cost
        - More than 3 years: 25% of purchasing cost

15. **Mobile synchronize with Exchange email**
    a. You are allowed to synchronize Company email to your mobile devices but please ensure that they are password protected.
    b. A FULL wipe of your mobile device [Factory default] in the case of loss of mobile and on the employee's last day of work. Instead of synchronizing email to mobile, you can also access email online through Microsoft 365.

16. **Installation of illegal software.** You should not copy any program installed on your company assigned computer for any purpose without permission from the Company. Any employee found copying software illegally is subject to employment termination by the Company.

17. **Disciplinary measures.** Employees who violate IT policies may be subject to penalties and disciplinary actions by the Company. The Company may restrict or deny access to information technology resources prior to the initiation or completion of disciplinary procedures when it appears necessary to protect the integrity, security, or functionality of the Company's IT resources.

18. **Company's right to Indemnity.** Failure by employees to comply with Company IT policies may result in company being involved in claims and/or suffering damages. You shall indemnify IH Digital and its officers from such claims and damages resulting from your intentional failure to comply with the policies.

19. **Waiver of Privacy.** The Company reserves the right to intercept and monitor the computer, internet and e-mail activities of employees.

20. **Confidentiality & Non-Disclosure**
    a. All employees are required to sign a Confidentiality & Non-Disclosure (CNDA) form, agreeing to comply to all CNDA guidelines outlined by the company. Employees are required to keep all Company's and Clients' proprietary or trade information confidential.

b. Access to Client's database involving personal data will be restricted to only relevant personnel within the Company, up to 3 employees. Employees are allowed to use the database strictly only for work purposes outlined by Client.
c. Files containing personal data will be password-protected.
d. When Company needs to pass database to 3rd party Vendor such as in the case of SMS/Email blast, only limited and relevant data will be forwarded instead of the full database.
e. Database will be deleted immediately when it is no longer required for work purpose or as instructed by client.

21. **Policy Review**
The Company reserves the right to amend this Policy and/or implement additional policies periodically.

By signing this page, I indicate that I have read, understood and accepted the Acceptable Use Policy set out above, including any revisions, and agree to abide by the terms stated.

_____
Full Name:
Date: