ACKNOWLEDGMENT OF INFORMATION SECURITY POLICIES AND RULES

By signing below, I agree to the following:

a. I have received the information security awareness briefing and have read a copy of the:
   (i) Information Security Management Policy
   (ii) Topic-specific Policies for Information Security
   (iii) Information Security Disciplinary Process

b. I understand and agree to follow the policies and procedures contained in the above-mentioned document and the expected behaviour of me as an employee in NetGain Systems Pte Ltd.

c. I understand and agree that any company assets provided to me by the company remain the property of the company and must be returned upon my termination of employment.

d. I understand and agree I must make reasonable efforts to protect all company–provided information and associated assets from theft and physical damage, unauthorized disclosure, modification, removal, or destruction, and comply with the following rules of acceptable use:

- Use of the organisation's information and associated assets is permitted and encouraged where such use is suitable and appropriate for business purposes and complies with the relevant information security controls adopted by the organisation.
- Any person granted access must keep their password and any other forms of authentication provided private at all times and shall not by any means provide them to any other employee or any other person.
- Any person granted access must log off or lock the device they have been using on each and every occasion the device is left unattended.
- All information classified in terms of the organisation's *Information Classification Policy* shall be appropriate protectively marked to ensure that it is managed, accessed, stored, used and handled correctly. Protectively marked information should not be taken outside of the organisation unless this has been authorized by the information owner/custodian and can be protected in a manner that is consistent with the organisation's policies and procedures.
- Any person granted access to information and associated assets must be aware that levels and patterns of usage may be subject to monitoring, for security and resource management purposes, from time to time, and must also be aware that:
  - The use of information and associated assets is subject to parameters outlined in the organisation's own policies and procedures. Any issues that related to information security, or that could give rise to information, shall be reported to the Management Representative.
  - Internet usage and email usage may be electronically monitored from time to time.
  - Most IT-resource usage is directly traceable back to individual users.

A copy of this should be filed in the personnel file. The employee must receive a copy.

- Any person granted access to information and associated assets must not use any of the resource:
    - To access, download, communicate or create any offensive, defamatory, obscene, sexually threatening or intimidating, pornographic (including pedophilic), indecent, inappropriate or otherwise objectionable comments, images or materials. This shall include, but not limited to, anything that does not or may reasonably be determined to be discriminatory on the grounds of a person's racial or ethnic origin, gender, sexual orientation, marital status, disability, political beliefs or religious beliefs, or which is otherwise contrary to law.
    - To upload, download or otherwise transmit information without the necessary authorization or in contravention of the organisation's policies.
    - To corrupt, disrupt access or change any other user's data, files, records or systems, except where explicit authority to do so have been given.
    - To access, download or otherwise connect with any instant messaging, file sharing or any similar facilities, except where explicitly authorized to do so for business purposes.
    - To download or install any program or application that has not been explicitly approved within the organisation.
    - To commit an act of malicious damage to any company resources.
    - To transmit materials that infringes the copyright of another person or entity.
    - To attach and use any peripheral storage device or other removable media without explicit authority and required security protection measures.
- Any person granted access to information and associated assets are reminded that any types of behavior referred to herein are demonstrative only are not intended to form a definitive list. If any doubt exists as to any intended use of information and associated assets, this should be referred to the MR prior to use.

e. I understand and agree that any infringement of any provision set out in this document will be handled through the organisation's *Information Security Disciplinary Process*.

_____

Signature of Employee

Name: _____

Designation: _____

Date: _____

A copy of this should be filed in the personnel file. The employee must receive a copy.