FSS
POWERING PAYMENTS

FINANCIAL SOFTWARE & SYSTEMS (P) Ltd.

INFORMATION SYSTEMS SECURITY - UNDERTAKING

Use of the Information Systems, Intranet and Internet is provided to complete jobs assigned from time to time by employees. These facilities are provided to for business related communications only as is the use of any Company system or network. These systems are provided to further the business goals of the Company and may not be used in any manner that is deemed inappropriate. The following violations are expressly prohibited:

- Use of systems or networks in attempts (whether successful or not) to gain unauthorized access to remote systems.
- Use of Company systems or networks to connect to other systems to which you do not have authorized access.
- Decryption of system or other user passwords.
- The copying of copyrighted materials, such as third party software, without the express written permission of the owner of the proper license.
- Intentional attempts to crash network systems or programs.
- Any attempts (whether successful or not) to secure an unauthorized higher level of access on Company systems or programs.
- The willful introduction of computer viruses or other disruptive or destructive programs into Company systems or networks.
- Attempts at sending unsolicited junk mail, for profit messages or chain letters, games, jokes, or other inappropriate messages.
- Attempts (whether successful or not) at sending harassing, obscene or other threatening correspondence through the use of any systems or network including Internet or Intranet.
- Downloading and/or installing of software (whether successful or not) without the express prior approval from the respective division Head. This includes shareware, freeware, screen savers and multimedia files including videos and audios.
- Employees are also expected to adhere the Technology Infrastructure Use & Security:
- Employees are prohibited from testing or attempting to compromise the computer network security measures employed by FSS.
- Employees must be authorized by appropriate mangers and respective functional head to provide system privileges such as local administrative rights.
- Employees must not disable the virus checking software installed in the system.
- Employees must not create, compile, copy, propagate, execute or attempt to introduce any computer code that may self-replicate damage or hinder the performance of any system, data, hardware or software.
- Passwords must be changed immediately if an employee suspects or knows that it has been disclosed or discovered.
- Employees are prohibited from sharing passwords for any information system accounts.
- Employees may not acquire, possess, trade or use hardware or software tools that could be employed to evaluate or compromise FSS information systems security and compliance. From time to time, the TI Department may conduct technical audit reviews to determine whether security measures are being followed.
- Due to viruses, Trojans, and other malicious software transmitted by email, users should also use caution when opening attachments or clicking on embedded web links. If an email is received from an unknown source, the email and/or attachment should not be opened nor should the employee click on the web link if there is one. The TI Department should also be advised so that they can investigate such emails.
- When participating in Internet mailing lists and news groups' employees must take care in structuring comments and questions that they post to avoid revealing proprietary, sensitive or competitive information about FSS Products' projects, environments, systems and networks.
- Any employee, who is granted Administrator level access to FSS systems and is found to have abused those access privileges, by reviewing or copying files to which they would not normally have access, will be considered to be in violation of this undertaking.
- Electronic messages, the electronic communications systems, documentation, data, and backup copies generated by FSS employees are property information of FSS. No data or information will be given or transferred to outside individuals or organizations expect for those instances where an authorized manager approves it.
- IT Act 2000 takes cognizance of and prohibits many items and some of them are listed below:
  - ✓ Hacking with computer system.
  - ✓ Whoever with intent to cause or knowing that he/she is likely to cause wrongful loss or damage to the public or any person, destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.
  - ➢ Unauthorized access including any assistance provided to obtain unauthorized access
  - ✓ Introduction of virus or any computer contaminant
  - ✓ Publishing or transmission of any obscene material, in electronic form.
  - ✓ Disclosure of any electronic record / information, without the consent of the person concerned.
  - ✓ Understand and agreed to the policies governing the processing, storing or transmitting payment card data as per PCI DSS
- Information / Data Security roles and responsibilities also include the requirements to:
  - ✓ Implement and act in accordance with the organization's information security policies.
  - ✓ Protect assets from unauthorized access, disclosure, modification, destruction or interference.
  - ✓ Execute particular security processes or activities.
  - ✓ Report security events or potential events or other security risks to the organization

We would also like to bring to the notice of all employees that the company provides our employees with many tools that improve efficiency and allow us to better serve our customers. Such tools include telephone, fax machines, computers, e-mail and Internet access. Employees are reminded that all tools provided by the organization are considered company property and are intended to be used for business, in a manner consistent with the company's standards of conduct.

Self-Declaration:

I acknowledge / authorize that I have read and understood the Company's Information Systems Security rules and regulations including PCI DSS governing policies on Card holder data and promise to abide by

Date: 23/02/2022 **Name & Emp. Code:** K. Suresh

Place: Vasudevanallur **Signature:** K. Suresh