



INFORMATION SECURITY

Impulse Embedded Limited handle customer and cardholder information on a regular basis. It is the policy of the Directors that the Company handles sensitive data with extreme care and ensures that adequate safeguards are in place to protect all data and information, to protect the data subject's privacy and to ensure compliance with laws and regulations.

To this end, the Directors and Management are committed to maintaining a secure environment in which to process, store and manage all data and information. In addition, all Company practices, processes and operational activities have data security, integrity and privacy designed in.

The Directors and management acknowledge their responsibility for ensuring our Company systems and data are protected from unauthorised access and improper use with the use of hardware and software protection methods and regular system updates and reviews.

The Directors and Management require all employees handling information and data to ensure the following:

- Comply with the company GDPR statement and practices
- Ensure strong passwords are used at all times and keep passwords and user accounts secure
- Request approval from management prior to installing any new software or hardware on any company equipment
- Report information security incidents or concerns without delay, to the Directors and Senior Technical Manager responsible
- Attend regular training on information security

All staff authorised to handle sensitive card holder data will also comply with the following:

- Handle card holder information in a manner that fits with the sensitivity of the data
- Ensure credit card details are not recorded in written or digital formats
- Use only authorised platforms to process credit card payments (Worldpay)