Information Security Policy

Purpose

The Information Security Policy aims to establish a management framework to initiate and control the implementation of information security within **PACSQUARE TECHNOLOGIES** of **PACSQUARE TECHNOLOGIES**'s environment.

Scope

This policy applies to all staff/ users that are directly or indirectly employed by **PACSQUARE TECHNOLOGIES**, subsidiaries or any entity conducting work on behalf of **PACSQUARE TECHNOLOGIES** that involves the use of information assets owned by **PACSQUARE TECHNOLOGIES**.

Information Security Policy

It is policy of PACSQUARE TECHNOLOGIES to create, maintain and continually improve the Information Security Management System and to adhere to ISMS practices and committed to protect its information assets by deploying information security controls that minimize the impact of any security incident. PACSQUARE Technologies commits compliance with best practices for Software development industry and information security needs of the customer. To achieve this objective, we ensure the following:

- All applicable legal and contractual requirements are fulfilled.
- Confidentiality, integrity and availability of information is maintained throughout a systematic process.
- Management is committed to continually improvement regarding effectiveness of ISMS.
- Appropriate access control will be maintained and information will be protected against unauthorized access. Such as but not limited to:
    - ❖ Policies, Procedures and Guidelines not limited to Information Security will be made available in online format through an intranet system to support the ISMS Policy as deemed appropriate.
    - ❖ Internal Audit Unit has direct responsibility for maintaining the ISMS Policy and involved with writing and/or managing the development of relevant policies, procedures and guidelines not limited to information security.
    - ❖ All managers are directly responsible for implementing the ISMS Policy within their units, and for adherence by their staff.
    - ❖ It is the responsibility of each member of staff to adhere to the ISMS Policy.
    - ❖ The availability of information and information systems will be met as required by the core and supporting business operations.
- Risk management framework will define Risk and its treatment to all corporate assets (tangible/intangible and human). The risk against each are assessed and against all risks appropriate controls are implemented to mitigate risk and contingency plans are defined for all Assets with unacceptable levels of Residual Risk.
- Conducive work environment have been provided to human resource, free from accidental and occupational hazards.
- All personnel are trained in information security practices, roles and responsibilities.