Information Security Policy

1 INTRODUCTION

1.1 Purpose

The purpose of this policy is to provide a framework for defining and regulating Information Security Management System in Sybrid so that its core and supporting business operations continue to operate with minimal disruptions. This policy will be provided to and made available to all employees of Sybrid (and external interested parties where appropriate) in order to ensure that information is appropriately secured against loss of confidentiality, integrity, availability (CIA).

1.2 Goals & Objectives

The objective of the information security is to ensure business continuity and minimize business damage by reducing the impact of security incidents and where possible preventing their occurrence. The following goals in support of this to:

- Establish safeguards to protect the SYBRID's information assets and resources from theft, abuse, misuse and any form of damage by improving physical access controls and surveillance systems.
- Establish a paperless work environment and to improve security, accessibility, efficiency, reduce processing time by automating Operational processes.
- Protect business systems, all information within its custody by safeguarding its Confidentiality, Integrity and Availability, through Optimization of Network & Infrastructure as per updated Technology Systems practiced across the globe, and through improving IT services and security through implementing the ITIL V3 Framework.
- Reduce receivable turnover by improving receivable management process. And improve profitability of Sybrid by placing effective financial controls, exploring new markets and resource optimization.
- Encourage management and staff to maintain an appropriate level of awareness, knowledge and skill in order to minimize Information Security incidents and to improve productivity and deliver high quality of service to the customers.
- Minimize non-conformities, incidents, frauds, errors and security breaches by reporting and investigating all suspected breaches of the information security and by placing effective process controls.
- Improve productivity, quality and market image by providing a positive working environment to employees and reducing employee turnover.
- Ensure that SYBRID is able to continue its business activities in the event of significant Information Security incidents.

Further details of these goals are mentioned in RISM – 909 Departmental Goals and Objectives

1.3 Scope of Applicability

Information Security policy is intended to support the protection, control and management of the SYBRID's information assets. These policies are required to cover all information within the organization which could include data and information that is:

- Stored on databases and on computers
- Transmitted across internal and public networks
- Stored on removable media such as CD-ROMs, flash drives, hard disks, tapes and other similar media
- Stored on fixed media such as hard disks and disk sub-systems
- Held on film
- Presented on slides, overhead projectors, using visual and audio media
- Spoken during telephone calls and meetings or conveyed by any other method

2 POLICY

2.1 Policy Statements

SYBRID is committed to facilitate business improvement through the adoption of secure business practice and business management. It is the policy of SYBRID that the information assets it manages shall be protected from all threats, whether internal or external, deliberate or accidental. SYBRID shall ensure that:

- Information should be made available with minimal disruptions to staff and the public as required by the business process. The integrity of information will be maintained and confidentiality of information will be assured. Hence, non-public Information should be secured against disclosure, modification, and access by unauthorized individuals.
- All suspected breaches of information security having impact on confidentiality; integrity and availability of information will be reported to, and investigated by relevant HOD with consent of ISM.
- Appropriate access control will be maintained and information will be protected against unauthorized access.
- Business continuity management framework shall be made to minimize disruption to business functions by preventing and minimizing the impact of security incidents.
- Information security awareness and trainings will be made available to staff.
- The goals and objectives defined by the company will be supported by ISMS policies and procedures.
- Policies, procedures and guidelines not limited to information security will be made available for all staff.

All staff, management and suppliers are responsible for implementing, complying and reporting improvements in relation to this policy and supporting information security management system policies and documentation.

SYBRID's internal audit department has the responsibility for facilitating the implementation of this policy and supporting information security management system, providing advice and guidance to all personnel.

All managers and HODs are directly responsible for implementing the ISMS policy and its requirements within their Business Units / departments and for adherence by their staff.

Risk Assessment for all the information assets within the defined scope of Information Security Management will be carried out periodically and all the identified risks will be managed to an acceptable level that complies with all stakeholders, business and legal or regulatory requirements and contractual security obligations.

This information security policy is approved by the Chief Executive Officer and has the full support of management and shall be reviewed by the management annually.