1 INTRODUCTION

1.1 Purpose

The purpose of this policy is to:

1. Prevent loss, damage, theft or compromise of SYBRID internal information or information handed over to SYBRID by the client.
2. Prevent unauthorized disclosure, modification, removal or destruction of information, and interruption to business activities.
3. Ensure that both logical and physical access to information and systems is controlled and procedures are in place to ensure the protection of information systems and data.

2 SCOPE

The scope of this policy includes all access to Sybrid information systems and physical access to areas and locations where information and data is located. This policy applies throughout the information lifecycle from acquisition/processing, utilization, storage and disposal.

3 POLICY

3.1 Policy Statements

- Access to information and Information processing facilities will be granted on "Need to Know" basis, and where possible will be for limited time and shall be revoked by the end of that time.
- Strict measures will be taken to identify security requirements ensuring the confidentiality and security of information access to the business applications.
- Information will be classified and must have a designated owner. An ISM Forum would be initiated by the management taking relevant departments which may include members from IT, Admin, HR, ISM and Senior Management; who will supervise the ways in which certain types of information are used and protected. The information can be classified as restricted, confidential, public etc.

- Member(s) of ISM Forum will take decisions about who will be permitted to gain access to information or information processing facilities; ISM must take steps to ensure that appropriate access are granted to the authorized user(s) and records will be maintained.
- Access to sensitive areas e.g. Server Room will have a separate process. All necessary information will be maintained regarding nature of job performed and the person who was involved. Such area's access will be given for a certain period of time and revoked after that time.
- Access control roles will be defined. Segregation of controls will be made between a regular user and privileged user.
- Every associate in SYBRID will have a unique login identity. Login identity must not be shared until and unless on need basis which will be approved and documented by the relevant authority.
- Privileged access rights will only be granted on "need to use basis" and after the completion of authorization and approval by the relevant authority.
- Regular operational activities will not be performed by the privileged user IDs.
- Passwords for generic Administrator user ID must be kept with high confidentiality. It will be changed on high frequency and will be communicated through a proper procedure to other privileged user considering the sensitivity and confidentiality.
- Access rights for privileged user will be reviewed at more frequent intervals to avoid any type of unnecessary and unauthorized access to the sensitive information or information processing facilities.
- Relevant authority will review the access rights at regular intervals and changes can be made if necessary. For e.g. if the employee is terminated, promoted or transferred, the access rights will be revised and well documented.
- If any employee is terminated, access rights will be revoked immediately. Identity cards will be taken and if the employee has any type of passwords for active applications that must be changed on immediate basis.
- All significant events and permitted access rights to information and information processing facilities will be recorded and archived.
- Access to networks and network services will be identified and documented according to the segregated access controls.

- Access to networks and network services will only be granted via authorization procedure and documented approval by the member(s) of ISMF.
- Member(s) of ISMF will put proper controls and monitor with periodic review on networks to mitigate the risk of unauthorized access.
- Member(s) of ISMF will verify the authentication and need of the user before permitting the access to networks and network services.