INFORMATION TECHNOLOGY POLICY

Introduction:

Shri Kalyan Holdings Limited (hereafter called "the Company" or "SKHL") being a NBFC**,** its Information Technology /Information Security (IT/IS) framework, Business continuity planning (BCP), etc. must be benchmarked to best practices.

Further as per the Notification issued by the Reserve Bank of India regarding NBFC Prudential Norms vide notification no. RBI/DNBS/2016-17/53 Master Direction DNBS.PPD.No.04 / 66.15.001/ 2016-17, all Non deposit taking NBFCs are required to frame an Information Technology Policy and implement the same.

Hence, it becomes imperative for the company to have a prudent Information Technology Policy to regulate the credit system of the company to its advantage and to enhance safety, security, efficiency in processes leading to benefits for company and its customers.

Objectives of the Policy:

The policy is framed with the objectives to regulate the credit system of the company to its advantage and to enhance safety, security, efficiency in processes leading to benefits for company and its customers.

Appointment of Chief Information Officer or In-Charge of IT Operations:

Company has designated the Whole-Time Director of the company as a Chief information officer or in-charge of IT Operations whose responsibility is to ensure implementation of IT Policy to the operational level involving IT Strategy, value delivery, risk management and IT Resource Management.

Information Security

The section below describes the different levels of security, which would be implemented as part of the overall IT solution being implemented at SKHL office.

Information Security Framework

SKHL's Information security system addresses all aspects of enterprise security inclusive of but not limited to physical & environmental security, personnel security, access control, operational security, business continuity & disaster recovery, legal & compliance, system & network security, data privacy & protection, security incidence response, user awareness & training.

Physical Security

SKHL ensures adequate controls for physical security at the perimeter of the SKHL office, work are as within the facilities and sensitive areas e.g., Server rooms. The controls include the following:

- All SKHL facilities comply with environmental health and safety standards. This includes fire prevention, perimeter security, emergency evacuation processes, 24*7 CCTV coverage and monitoring, medical facilities and first aid, public address system etc.

- Certain sensitive "red zone" areas e.g. Production Control, Computer Operations, Data Centers, Server rooms, CCTV room have further entry restrictions to limited

authorized persons only and this is controlled by swipe cards plus PIN where necessary.

- Access rights to these areas are based on approval matrix and are reviewed.

- IT equipment which does not reside on an individual associate's desktop are physically located in a secured area e.g. Data Center, with adequate controls for preventing or suppressing environmental hazards like fire and other non-environmental threats and proper access controls.

System Security and Cyber security

User Access Control:

- SKHL would leverage its robust registration & de-registration procedure for granting access to all multi-user information systems and services that are owned by SKHL. Access to multi user information systems incorporates unique User IDs and multiple user levels (e.g. simple user, administrator etc.)

- All SKHL employees are instructed not to share their passwords & privileges with others, as part of the overall Information security awareness drive.

- All SKHL PCs have password-protected screen savers, which get activated automatically after 5 minutes of inactivity.

- All SKHL employees login to PC/Laptop using their Domain IDs, which are protected by SKHL password policy.

- SKHL password policy is enforced across the board on all PCs & servers, which ensure minimum length and frequent change in go passwords (30 Days).

- All SKHL desktops are periodically updated with latest OS patches and antivirus updates.

- Privileges are allocated to individuals on a need-to-have basis and if feasible on an event-by-event basis. These privileges are granted based on an authorization process and are time-bound.

- SKHL employees at any point of time should NOT attempt for any configuration changes related to software, hardware & networking.

- Any additional software\hardware required by employee (before or after taking handover) should be clearly communicated through e-mail to the Systems Admin Department. The request for installation will be reviewed if considered valuable, will be installed. System's department has the right to reject the request regarding software. It's entirely at IT discretion.

- During the period, when the owner carries the Laptop with them the same should not be misused for the purpose of transferring the data on to other storage devices. If any owner were found malpractice, he/she would be liable for disciplinary action from the organization.

- For each transaction, there must be at least two individuals (maker and checker)

necessary for its completion as this will reduce the risk of error and will ensure reliability of information.

Antivirus Management:

- Centralized Anti-virus management System wherein all the workstations & Servers are installed with Anti-Virus Client.

- The Virus Definitions are deployed from the Anti-virus Server to all the reporting clients automatically. Security/Operations team monitors the Antivirus console centrally & real time.

Security Awareness:

- All employees have to go through a course on Information Security at least once in a year.

- Employee awareness is boosted through compulsory security screensaver on PCs, large number of posters across premises along with regular e-mail communication to users.

- Frequent communication on Do's & Don'ts by Information Security Leader and business leaders along with multitude of posters are also used to reinforce security awareness

- Unless expressly authorized to do so, user is prohibited from sending, transmitting, or otherwise distributing proprietary information, data, trade secrets or other confidential.

- No external devices to be used such as DVD's, CD's, Pen Drives, network drives & other mediums to transfer/transmit data.

Data Repository Policy for Users

- User's data to be saved in specified/defined user's Home drive. Employee needs to ensure to move data on daily basis in their home drive. Incremental backup runs on the home drive at midnight and generates a report for every user, to track the changes.

Network Access Control

Network access to users is controlled and users are provided with access to services for which they have been specifically authorized to use. All network traffic is denied, unless specifically permitted. There are authorization procedures for determining who is allowed to access which networks and networked services

Internet Access Control

- To ensure security and avoid the spread of viruses, Users accessing the Internet through a computer attached to network are routed through an approved Internet firewall or other security device. Bypassing computer network security by accessing the Internet directly by modem or other means is strictly prohibited.

Security Incident Response Procedure

SKHL follows Incident Response Process. SKHL employees are required to report any security weaknesses and breaches as per the process.

- Any violation of organizational security policies and procedures by employees is subjected to a formal disciplinary process involving Human Resources (HR) and Legal departments.

- The disciplinary action would typically range from issuing CAP (Corrective Action Plan) letters upto termination of the employment depending upon the severity of the policy violation.

- A Typical incident response process followed by SKHL will include Identification of an Incident.
    - Notification to Incident Response Team
    - Incident Impact Assessment
    - Containment
    - Internal Notifications
    - External Notifications
    - Post-Incident Management

- Incidents reporting are managed by qualified & experienced professional. These professionals analyze & contain the incident depending on the threat level by:

    - Remotely running the fix tool and mitigating the vulnerabilities (if it's a vulnerability exploit),
    - Creates a RCCA (Root Cause and Corrective Action)
    - Escalate to the respective maintenance teams if hands and feet support is required.

Data Backup

In order to prevent loss of information by destruction of the magnetic means in which it is stored, a periodic backup procedure is carried out. The responsibility for backing up the information located in shared access servers is the network administrators. It must be borne in mind that not only are hard disks inclined to fail, but also magnetic tapes are quite prone to errors that destroy their contents, so we need to do the restoration testing time to time basis.

- Data Backup in File Servers: The Systems Management backs up all the information in the file servers through an automated procedure.
- Data Backup in Database Servers: The Systems Management backs up all the information in the databases through an automated procedure.
- Data Backup in Desktop PC and Notebook: This task is the responsibility of the user to whom the computer has been assigned.

Business Continuity Planning (BCP) and Disaster Recovery

BCP forms a significant part of an organisation's overall Business Continuity Management plan, which includes policies, standards and procedures to ensure continuity, resumption and recovery of critical business processes. BCP shall be designed to minimise the operational, financial, legal, reputational and other material consequences arising from a disaster. NBFC should adopt a Board approved BCP Policy. The functioning of BCP shall be monitored by the Board by way of periodic reports. The CIO shall be responsible for formulation, review and monitoring of BCP to ensure continued effectiveness. The BCP may have the following salient features:

- Business Impact Analysis- NBFCs shall first identify critical business verticals, locations and shared resources to come up with the detailed Business Impact Analysis. The process will envisage the impact of any unforeseen natural or man-made disasters on the NBFC's business. The entity shall clearly list the business impact areas in order of priority.

- Recovery strategy/ Contingency Plan- NBFCs shall try to fully understand the vulnerabilities associated with interrelationships between various systems, departments and business processes. The BCP should come up with the probabilities of various failure scenarios. Evaluation of various options should be

done for recovery and the most cost-effective, practical strategy should be selected to minimize losses in case of a disaster.

- NBFCs shall consider the need to put in place necessary backup sites for their critical business systems and Data centers.

- NBFCs shall test the BCP either annually or when significant IT or business changes take place to determine if the entity could be recovered to an acceptable level of business within the timeframe stated in the contingency plan. The test should be based on 'worst case scenarios'. The results along with the gap analysis may be placed before the CIO and the Board. The GAP Analysis along with Board's insight should form the basis for construction of the updated BCP.

Scope of Policy

This policy applies to all employees, customers, partners, vendors, stakeholders and parties associated to SKHL.

Policy Review

The Information Technology Policy shall be reviewed by the Board subject to guidelines issued by RBI and to make amendments if considered necessary.

Adoption

This policy and any changes made during the annual reviews shall be adopted by resolution of the Board of Directors.