Davinta Financial Services Pvt. Ltd.
7-P, 93-P, Electronic City West, Bangalore - 560 100 India
Tel: 080 – 4905 4444 / 3350 4444

DAVINTA
The last mile, first

DAVINTA FINANCIAL SERVICES PRIVATE LIMITED

INFORMATION TECHNOLOGY / INFORMATION SYSTEM POLICY

As per the RBI guidelines, it is recommended for Non-Banking Financial Companies to formulate an information technology / information system policy, approved by its Board of Directors. Therefore, Davinta Financial Services Private Limited ("Davinta") is formulating this information technology / information security policy. This will ensure quick, reliable and efficient processing of business transactions. This will play a vital role by increasing the customer base by adding various new channels of banking.

In Finance Company, IT plays a crucial role as there is a need of real time data updation, payment gateway etc. Moreover it is also useful for efficient processing of internal activities and back office operations. Such information is required to be safeguarded.

Davinta want to put in place this policy to minimize the risk of security incidents involving IT usage.

BASIC SECURITY STANDARDS

Implementation of latest technology will change the way of doing business. Embracing new technology exposes the risk of unauthorized access of data. Unavailability of technology support may lead to breakdown in business. With this, users & customers must have confidence that information system will operate as without unanticipated failures or problems. This will ensure that technology is optimally utilized and IT enhances the future growth.

Company is implementing basic security standards - such as physical / logical access controls and a well-defined password policy.

Davinta is designating senior executive as the Chief Information Officer (CIO) who will be responsible to ensure implementation of IT Policy involving IT strategy, value delivery, risk management and IT resource management. To ensure technical competence periodic assessment should be formulated to ensure that sufficient, competent and capable human resources are available.

Here are the following basic creeds of the board-approved IT Policy–

a. **Confidentiality** – Ensuring access to sensitive data to authorized users only;
b. **Integrity** – Ensuring accuracy and reliability of information by ensuring that there is no modification without authorization;
c. **Availability** – Ensuring that uninterrupted data is available to users as and when required;
d. **Authenticity** – It is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine for information security.

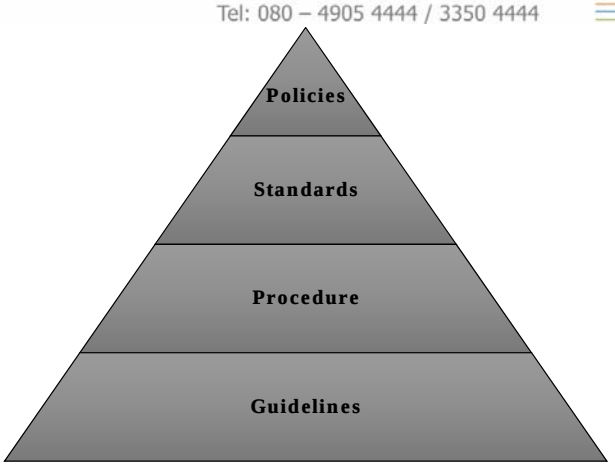
OBJECTIVE

Information Security Policy ensures that:

a. Confidentiality, Integrity and Availability of information is protected adequately and mainlined uniformly across the company.
b. All information is protected from unauthorized physical & logical access.
c. Information is protected from fraud, corruption or loss during input, processing, transmission & storage.
d. Information upon which the company depends is adequately protected to allow the continuation of day to day operations with least breakdowns.
e. The users are aware and comply with relevant legislation relating to the maintenance, protection, retention and withholding of information.
f. Security related incidents are managed appropriately.

FRAMEWORK

The framework is necessary to establish, implement, operate, monitor, review, maintain and improve security and related risks. This is important to reduce the risk of errors and to ensure reliability of information.



Policies

It consist the commitment from the senior management of the organization to meet the compliances as well as regulatory requirements, the objective and goals.

Standards

Standards as applicable to establish the benchmark for the procedures against which uniformly compliance could be measured

Procedures

Procedure to meet the objective mentioned in the information security policy .

Guidelines

These are the suggestions to carry out the activities stated in the procedures.

Information Security Policy Framework

Identification and Classification of Information Assets: Davinta will sustain detailed inventory of Information Asset with the distinct asset identification.

Segregation of functions: Duties will be segregated of the official dealing exclusively with information systems security and the Information Technology division. In terms of the number of staff, level of skill and tools or techniques like

risk assessment, security architecture, vulnerability assessment, forensic assessment, etc, the information security function should be adequately resourced. The responsibilities are clearly segregated relating to system administration, database administration and transaction processing.

Role-based Access Control: In Davinta, there will be clear delegation of authority for the right to upgrade/change user profiles and permissions and also key business parameters (eg. interest rates) which should be documented.

Personnel Security: Davinta has made proper arrangements for the appropriate check and balance in this regard. Personnel with privileged access to the system administrator, cyber security personnel, etc should be subject to rigorous background check and screening.

Physical Security: Company has created a protected environment for physical security of IS Assets such as the secure location of critical data, restricted access to sensitive areas like data center.

Maker-Checker For each transaction, there will be at least two individuals for its completion as this will reduce the risk of error and will ensure the reliability of information.

Incident Management: Davinta has developed and implement processes for preventing, detecting, analyzing and responding to information security incidents.

Trails: Davinta has ensured the existence of audit trails for IT assets satisfying its business requirements including regulatory and legal requirements, facilitating the audit, serving as forensic evidence when required and assisting in dispute resolution. If an employee, for instance, attempts to access an unauthorized section, this improper activity will be recorded in the audit trail.

Public Key Infrastructure (PKI): To ensure confidentiality of data, access control, data integrity, authentication, and non-repudiation, the usage may be increased.

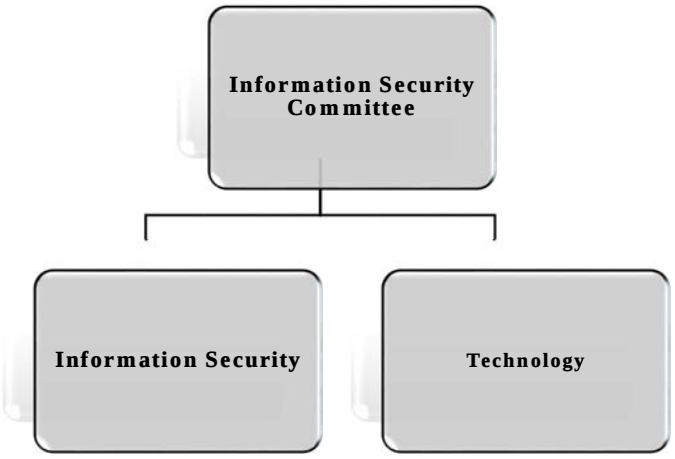
PROVISIONS PERTAINING TO INFORMATION AND CYBER SECURITY

Cyber security helps in combating cyber threats given the level of difficulty of business & acceptable levels of risk. Vulnerability management is an ongoing process to determine the process of eliminating or mitigating vulnerabilities based upon the risk & cost associated with the vulnerabilities. Company has made plan for managing and eliminating vulnerabilities.

The risk assessment should be brought to the notice of the Chief Risk Officer (CRO), CIO and the Board and should serve as an input for Information Security Auditors. The technology which is used for mobile facilities must ensure confidentiality, integrity, authenticity & must deliver for end-to-end encryption.

In case of using Social Media to market products then team should be well equipped in handling social media risks and threats. As Social Media is vulnerable to account takeovers and malware distribution, proper controls, such as encryption and secure connections, should be prevalent to mitigate such risks.

The management framework will define, implement and monitor information security for the information assets.



Information security committee consisting senior executives along with the top management participation. This committee will be responsible for security related activities in the organization.

Information will have to be suitably classified to assign the desired level of protection.

Information is categorized as:

Secret: Data concerning identity and access shall be classified as secret.

Confidential: System programmes and changes thereto shall be classified as confidential. In case of National Electronic Fund Transfer (NEFT), clearing services up to the stage of completion of clearing activities, including arriving at the settlement position, generating reports will be included under this head.

Internal: Information in relation to post completion of the clearing and settlement activities including archiving, back and other details for dispute resolution purposes shall be treated as internal.

Public: Non Sensitive information available for external release.

MANAGEMENT REPORTING SYSTEM

A management reporting system provides business information which can be in the form of reports and/or statements. The system is designed to provide timely pertinent information to assist management like creation of system generated reports for senior management, containing details regarding financial position, operating / non-operating revenues and expenses, cost benefit analysis of segments / verticals and cost of funds.

Need of effective management reporting system:

a. For decision making and analysis of trends, constant need of reports
b. At the right time reports should be available with the right stakeholders
c. Lack of awareness of the performance of the organization
d. Data redundancy leads to data management issues and quality issues
e. High value resources

REQUIREMENT TO FILE REGULATORY RETURNS TO THE RBI

Davinta will take due care of regular & strict compliance with existing and dynamically changing legal requirements. Non-Compliance will result into penalty & prosecution. Therefore due importance will be given to the legal requirements.

REVIEW OF INFORMATION SECURITY POLICY

Timely necessary steps will be taken by the board to ensure the compliance with the policy & procedures.

COMPLIANCE MONITORING

The admin must monitor the practices of the IT users to ensure the high level of compliance. The information system audit team will ensure compliance of Information Technology Act 2000, Information Technology (Amendment) Act 2008, Information Technology (Amendment) Act 2011 and other guidelines.

ARRANGEMENT FOR BACKUP OF DATA

By regular backups, data will be protected. Appropriate IT team must perform backup for responsible data. All backup data must be stored in an encrypted manner and backup copies must be stored in an environmentally protected and access controlled secure location. Stored copies must be stored with a short description that includes the following information:

a. Backup date / Resource name / type of backup method

Stored copies must be made available upon authorized request:

The request for stored data must be approved by an authorized person nominated by a Director/Manager in the appropriate department.

Requests for stored data must include:

b. Completion of a form that outlines the specifics of the request, including what copy is being requested, where and when the requester would like it delivered and why they are requesting the copy;
c. Acknowledgment that the backup copy will be returned or destroyed promptly upon completion of its use;
d. Submission of a return receipt as evidence that the backup copy has been returned.

A record of the physical and logical movements of all backup copies shall be maintained.

Physical and logical movement of backup copies shall refer to:

a. The initial backup copy and its transit to storage;
b. Any movement of backup copies from their storage location to another location;

The record of physical and logical movements of backup media shall include:

a. all identification information relating to the requested copies;
b. purpose of the request;
c. the person requesting the copy;
d. authorization for the request;
e. where the copy will be held while it is out of storage;
f. when the copy was released from storage;
g. when the copy will be returned to storage.

Media in transit and store shall be protected from unauthorized access, misuse or corruption, including sufficient protection to avoid any physical damage arising during transit and store. All personnel responsible for data backup processing shall have:

a. Relevant identification;
b. Relevant authorization.

All relevant department backups should be verified periodically and report on its ability to recover data.

On a daily basis, information generated from each backup job will be reviewed for the following purposes:

a. To check for and correct errors;
b. To monitor the duration of the backup job;
c. To optimize backup performance where possible;

IT will identify problems and take corrective action to reduce any risks associated with failed backups.

Davinta Financial Services Pvt. Ltd.
7-P, 93-P, Electronic City West, Bangalore - 560 100 India
Tel: 080 – 4905 4444 / 3350 4444

DAVINTA
The last mile, first