TAMIL NADU TRANSPORT DEVELOPMENT FINANCE CORPORATION LIMITED, CHENNAI - 600 002.

INFORMATION AND CYBER SECURITY POLICY

Information Security Policy

Information is an asset to TDFC and Information Security (IS) refers to the protection of these assets in order to achieve organized goals. The purpose of IS is to control access to sensitive information, ensuring use only by legitimate users so that data control be read or compromised without proper authorization.

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 the un interrupted data is available to user when it is needed.
d) Authenticity – For IS it is necessary to ensure that the data, transactions communications or documents (electronic or physical) are genuine.

a) Identification and Classification of Information Assets. TDFC shall maintain detailed inventory of information asset with distinct and clear identification of the asset.

b) Segregation of Functions: These should be segregation of duties of the Security Officer/Group (both physical security as well as cyber security) dealing exclusively with information system security and the information technology division which actually implements the computer systems. The information security function should be adequately resourced in terms of the number of staff, level of skills and tools or techniques like risk assessment, etc. further, there should be a clear segregation of responsibilities relating to system administration and transaction processing.

c) Role Based Access Control - Access to information should be based on well-defined user roles (system administrator, user manager, application owner, etc.) TDFC shall avoid dependence on one or few pers -ons for a particular job. There should be clear delegation of authority for right to upgrade/change user profiles and permissions and key business parameters (eg. Interest rates) which should be documented

d) Personnel Security – A few authorized application owner/users may have intimate knowledge of financial institution process and they pose potential threat to system and data. TDFC should have a process of appropriate check and balance in this regard. Personnel with privileged access like system administrator, cyber security personnel, etc should be subjected to rigorous background check and screening

e) Physical Security – The confidentiality, integrity and availability of information can be impaired through physical access and damage or destruction to physical components. TDFC needs to a secured environment for physical security of IS Asset such as secure location of critical data restricted access to sensitive areas like data center etc.

f) Maker – checker is one of the important principal of authorization in the information=n system of financial entities. For each transaction, there must be at least two individuals necessary for its completion as this will reduce the risk of error and will ensure reliability of information.

g) **Incident Management –** The IS Policy should define constitutes an incident. TDFC shall develop and implement process for preventing, detecting, analyzing,

h) **Trails –** TDFC shall ensure that audit trail exists for IT assets satisfying its business requirements including regulatory and legal requirements, facilitating audit, serving a forensic evidence when required and assisting in dispute resolution. If any employee, for instance, attempts to access an unauthorized section, this improper activity should be recorded in the audit trail.

i) **Public Key Infrastructure (PKI) –** TDFC may increase the usage of PKI to ensure confidentiality of data, access control, data integrity, authentication and nonrepudiation.

CYBER SECURITY POLICY

a) Need for Board Approved Cyber Security Policy

TDFC should put in case a cyber-security policy elucidating the strategy containing an appropriate approach to combat cyber threats given the level of complexity of business and acceptable level of risk, duly approved by their Board. TDFC should review the organizational arrangements so that the security concerns are appreciated, receive adequate attention and get escalated to appropriate levels in the hierarchy to enable quick action.

b) Vulnerability Management

A vulnerability can be defined as inherent configuration flaw in an organization's information technology base, whether hardware or software, which can be exploited by a third party to gather sensitive information regarding the organization. Vulnerability management is an ongoing process to determine the process of eliminating or mitigating vulnerabilities based upon the risk and the cost associated with the vulnerabilities. TDFC may devise a strategy for managing and eliminating vulnerabilities and such strategy may clearly be communicated in the Cyber Security Policy.

c) Cyber Security Preparedness Indicators

The adequacy of and adherence e to cyber resilience framework should be assessed and measured through development of indicators to assess the level of risk/preparedness. These indicators should be used for comprehensive testing through independence compliance checks and audits carried out by qualified and competent professionals. The awareness among the stakeholders including the employees may also form a part of this assessment.

d) Cyber Crisis Management Plan

A Cyber Crisis management Plan (CCMP) should be immediately evolved and should be a part of the overall Board approved strategy. CCMP should address the following four aspect: (i) Detection (ii) Response (iii) Recovery (iv) Containment (v). TDFC need to take effective measures to prevent cyber- attacks and promptly detect any cyber intrusions so as to respond /recover / contain the fall out. TDFC are expected to be well prepared to face emerging cyber-threats such as 'Zero-day' attacks, remote access threats, and targeted attacks. Among other things, TDFC should take necessary preventive and corrective measures in addressing various types of cyber threats including, but not limited to, denial of service, distributed denial of services (DDoS), ransom-ware / crypto ware, destructive malware, business email fraud including spam

, email phishing, spear phishing, whaling, vishing frauds, drive-by downloads, browser gateway fraud, ghost administrator exploit, identity frauds, memory update frauds, password related frauds, etc.

e) Sharing of Information Incidents with RBI

TDFC are required to report all types of unusual security incident as specified in point No. 2 of Annex I which deals with basic information including Cyber security Incidents as specified in CSIR Form of Annex I (both the successful as well as attempted incidents which did not fructify) to the DNBS Central Office, Mumbai. The other particulars of the reporting have been provided in template as per Annex I

f) Cyber-Security awareness among stakeholders / Top Management / Board

It should be realized that managing cyber risk requires the commitment entire organization to create a cyber-safe environment. This will require high level of awareness among staff at all levels. Top Management and Board should also have as fair degree of awareness of the fine nuances of the threats appropriate familiarization may be organized. TDFC should proactively promote, among their customer, vendors, service providers and other relevant stakeholders an understanding of their cyber resilience objectives, and require and ensure appropriate action to support their synchronized implementation and testing.

g) Digital Signatures

A digital signature certificate authenticates entity's identity electronically. It also provides a high level of security for online transactions by ensuring absolute privacy of the information exchanged using a digital signature certificate. TDFC may consider use of digital signatures to protect the authenticity and integrity of important electronic documents and also for high value fund transfer.

h) IT Risk Assessment

TDFC should undertake comprehensive risk assessment of their IT system at least on a yearly basis. The assessment should make an analysis on the threats and vulnerabilities on the information technology assets of the TDFC and its existing security controls and process. The outcome of the exercise should be to find out the risks present and to determine the appropriate level of control necessary for appropriate mitigation of risk. The risk assessment should be brought to the notice of the Chief Risk Officer (CRO), CIO and the Board of the TDFC and should serve as an input for information security auditors.

i) Mobile Financial Services

TDFC that are already using or intending to use Mobile Financial Services should develop a mechanism for safeguarding information assets that are used by mobile applications to provide service to customers. The technology used for mobile services should ensure confidentiality, integrity, authenticity and must provide for end-to end encryption

j) Social Media Risks

TDFC using social media to market their products 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.

k) Training

Human link is a weakest link in the information security chain. Hence, there is vital need for an initial and ongoing training and information security awareness program. The program may be periodically updated keeping in view changes in information technology system, threats/vulnerabilities and/or the information system framework. There needs to be a mechanism track the effectiveness of training programs through an assessment / testing process. At any point of time, TDFC need to maintain an update status on user training and awareness relating information security.

(V. Venkatarajan)
Joint Managing Director