Annexure-I

INFORMATION TECHNOLOGY POLICY - 2018-19

The Information Technology Policy-2018-19 (IT Policy) document is meant to serve as a reference point to the officers and staff of Tourism Finance Corporation of India Ltd. (TFCI). The document provides a broad outline to IT Policy to be adopted and keeping in view the rapid changes in emerging technologies is not intended to enforce an inflexible rigidity. The IT Policy is in compliance with the directives contained in the Reserve Bank of India's Master Circular No.DNBS.PPD.No.04/66.15.001/2016-17 dated 08-06-2017.

1. INTRODUCTION

1.1 Role of Information Technology in TFCI and its History

IT plays a pivotal role in any organization due to the changing technological environment and organizational needs. In this Jet age, where the need of accurate information and timely processing of data is crucial for survival, the use of IT tools is not only providing a mechanism to gather, process and store vast amount of data, it is also helping the organization in attaining cutting edge.

TFCI is a service sector company engaged in the business of project financing. The Information needs of the organization are vast and complex.

TFCI started automation of its systems in 2002 and Systems like Loan Accounting, Financial Accounting, Payroll and Balance Sheet were computerized with the assistance of IFCI Ltd. The organization started client-server computing. The accounting packages based on Oracle8i database, development tools like Oracle Form 6 were introduced. Later on the Organization shifted its operations to a centralized computing system (CIIS) and it was in operation till March 2010. The system was taken on lease from IFCI.

In the meanwhile, in 2008 TFCI engaged Prosix Systems Pvt. Ltd., an outside agency to develop Loan Accounting and Financial Accounting packages. The independent package so prepared was in operation from April 2010 till March 2013. Thereafter, the Board of TFCI decided to adopt IT Application packages developed by IFCI viz. Financial Accounting, Loan Accounting and Payroll packages so that all group companies of IFCI operate under similar IT platform. Since April 2013 TFCI is working on IT application packages of IFCI i.e. based on Oracle 10g. TFCI has entered into Memorandum of understanding (MOU) with IFCI Ltd. for maintenance and support of the abovementioned application packages w.e.f. 01-01-2017 with rate renewal every three years.

1.2 Objective of IT Policy

- To provide IT infrastructure services and support to facilitate innovative use of technology for better decision making and for providing better service to the clients.

- Integrate IT into business operations in line with the business objectives of the organisation

- Explore and assess new and emerging technologies.

- Provide infrastructure to TFCI's users which is secure, personalised and timely access to information, services and support anytime anywhere.

- Provide users with the training, support, tools and information needed to foster innovative and effective use of technology.

2. IT STRATEGY COMMITTEE

In order to carry out review and amend the IT strategies in line with corporate strategies, Board Policy reviews, cyber security arrangements and any other matter related to IT Governance, an IT Strategy Committee is to be constituted comprising of an Independent Director as Chairman and CIO/CTO as member. The IT Strategy Committee is required to meet at frequent interval but not later than six months.

In line with the above, TFCI proposes to constitute IT Strategy Committee of comprising
(i) Independent Director (Chairman)
(ii) Managing Director
(iii) Executive Director
(iv) Chief Financial Officer

The broad roles and responsibilities of the IT Strategy Committee will encompass:

- Approve IT strategy and policy documents and ensuring that the management has put an effective strategic planning process in place.
- Ascertaining that management has implemented processes and practices that ensure that the IT delivers value to the business.
- Ensuring IT investments represents a balance of risks and benefits and that budgets are acceptable.

- Monitoring the method and management uses to determine the IT resources needed to achieve strategic goals and provide high-level direction for sources and use of IT resources.
- Ensuring Proper balance of IT investments for sustaining NBFC's growth and balancing aware about exposure towards It risks and controls.

3. IT ASSET MANAGEMENT POLICY

Overview and Purpose

IT Asset Management is an important business practice that involves maintaining an accurate inventory, licensing information, maintenance, and protection of hardware and software assets utilized by TFCI.

The Asset Management Policy focuses on the following key activities of the asset life-cycle viz. planning, acquisition, operation & maintenance and disposal.

All IT assets of the TFCI must be

- Acquired according to the needs.
- Recorded in the asset register in accordance with generally recognized accounting practices.
- Checked from the asset register to the individual asset and vice versa on a regular basis but not less than once per annum.
- Evaluated at least once per annum, to establish its condition as reflected on the asset register.
- Disposed of or scrapped, in the event that the asset
  (i) is no longer serviceable.
  (ii) has reached the end of its useful life.
- The disposal or scrapping of assets as contemplated in must be approved by the competent authority.

4. IT SECURITY POLICY

IT security is created under the following security heads:-

- Physical Security
- Security at the Network Gateway
- Security against Viruses/Spyware
- Security built into the Application Software/Database
- Data Security

4.1 Physical Security

- Restricted Access to Computer Room.
- Computer Room Environment :
  -Air-conditioning
  -Electrical distribution
  -MCBs
  -Proper earthing, etc.
- Fire Protection System
- Uninterrupted Power Supply (UPS)
- Fireproof cabinets for storing back-up HDD

4.2 Security at the Network Gateway

The Fire-wall/Router should provide the following minimum security features:-

- Intrusion Detection
- Intrusion Prevention
- Virus/Spy-ware Protection
- Access Control
- Content Filtering
- Spam Filtering
- Network Address Translation

4.3 Security against Viruses/Spyware

- Prevention/Detection of Viruses at the Network Gateway (Fire-wall)
- Selection of suitable Anti-virus solutions.
- Installation of Anti-virus Software on Servers as well as Nodes.
- Periodic/regular updation of Anti-virus software on all the machines.
- Updation of Virus definition/Spyware/Prohibited Content at Fire-wall.
- Educating the users in virus protection measures.

4.4 Security built into Application Systems

- Application systems shall have security features like:

  - User Ids
  - Passwords
  - Access Permissions
  - Login History

- User Account Log
- Audit trails
- System Modification Controls
- System Documentation

A detailed Security Policy, as per the above parameters, is as follows:

Application Systems Security Policy

4.4.1 Users and Logins

All oracle applications will be accessed through a single entry point.

4.4.2 Username and password.

- Each user should be provided with a unique username and a password. No user without a valid username and password can login to the system.
- A user should not be allowed to have multiple concurrent logins.
- Passwords should contain at least 6 alphanumeric characters and will be case sensitive. The first character must be an alphabet.
- Initially the usernames will be created without password. On first login to the system the user will be forced to enter the new password.
- The password must contain any combination of at least 6 characters and at the most 12 characters from A-Z, a-z, 0-9 and the special characters hyphen(-), underscore(_), comma(,), slash(/). The password will be case sensitive.
- The password must contain minimum numbers of alphabets and numbers as required by the system. The value of these numbers can only be set/ changed by the system administrator.
- The user should be forced to change his/her password after a specific interval in terms of days. The interval can be specified by the system administrator.
- The user should also have the privilege to change his password as and when he/she feels necessary.

4.4.3 **System Administrator**

Officer designated as System Administrator is to be provided with valid User Names and Passwords with system administration privileges. The responsibilities / privileges of a system administrator should include:

- Creation/Dropping of users (usernames).
- Activation / Deactivation of users.
- Granting / Revoking of Application Administrator privilege.
- Unlocking locked user accounts.
- Setting / Changing system parameters.
- All application administrator privileges.

DGM (Accounts) is proposed to be designated as System Administrator of TFCI.

4.4.4 **Application Administrator:**

System Administrator along with an officer from user department would be designated to act as Application Administrators. These designated officers would be provided with all the Application Administrator privileges. The responsibilities / privileges of an application administrator should include:

- Granting / Revoking access to the application system.
- Deciding Access level of the users.
- Deciding the users' reporting user / officer.
- Granting / Revoking Menu / Form level access privileges.
- Granting / Revoking of Application Administrator privilege.

4.4.5 **Application user.**

- An employee with a valid username and password and having access to any application system will be an application user for that application.

- There must exist a record with status as regular and valid office code in the employee directory of the payroll system.

- Whenever the system detects a mismatch between the office code of the user in the employee directory of the payroll system and office code as per security module, the user account should automatically get deactivated.

- Application user, on successful log in, should only be allowed access to the systems for which he has been granted permissions.

- The application user should not be allowed to have multiple logins.

- As soon as a user ceases to be an employee of TFCI, his/her user account should be de-activated immediately and he should not be able to access any of the application systems.

- Users should be able to lock their login account for any number of days. During the locking period the user accounts can not be accessed. User will be allowed to login to the system after the expiry of locking period. However, System administrator can unlock the accounts, if required.

- Maximum three login attempts should be allowed at a time. After three unsuccessful attempts login screen should be closed.

- The system should have the provision to lock the user account for those users making continuous attempts for a specified number of times (captured as system parameter) with invalid passwords.

4.4.6 **Access levels (Application System/Form/Menu)**

The following should be the broad access levels:

- Control

- Passing / Authorisation

- Preparation

- Query/View only

- No access

4.4.7 **Unsuccessful login attempts.**

The system should keep track of all unsuccessful login attempts. The details of date, time, terminal / machine id, user id and the reason for denial for login should be recorded.

4.4.8 **Current logins**

The system should keep track of all current login. The system should record the date and time of login, user id, employee code/name, terminal, session id, etc.

4.4.9 **Login history.**

The system should keep record of all past logins. The details of user id, employee code/name, terminal, session id, date and time of login, date, time nature of logout, etc. should be recorded by the system.

4.4.10 **Application-wise login history.**

The system should also keep track of all application-wise login detail. The details of user id, employee code/name, terminal, session id, date and time of login, date, time, nature of logout, etc. should be recorded by the system.

4.4.11 **Password History**

The system should preserve all old passwords.

4.4.12 **User Account Log**

The system should keep trail of the followings along with details of date and time of changes, reason and changing authority.

- Creation of user id.
- Dropping of user id.
- Deactivation of user id.
- Reactivation of user id.
- Locking of user id.
- Unlocking of user id.

- Granting system administrator privilege.

- Revoking system administrator privilege.

- Granting application administrator privilege.

- Revoking application administrator privilege.

- Changes in user profile in terms of :

  -Reporting officer
  -Access level
  -Department
  -Changes in user access to forms/reports/menu/sub-menu.

- Changes in system parameters (The old values will also be stored).

4.4.13 **Application Systems' Audit Trails:**

- Each Application System should have audit trail in respect of the fields as stipulated by the user department. Each system should also provide for generation of Audit Trail Reports.

- The Audit Trail Reports for the Systems like Financial Accounting, Loan Accounting and Payroll would be generated every month and would be perused by the user in-charge (Application Administrator) of the respective systems. These reports would be stored at least for one year till the annual audit of the office is complete.

- Audit trail data of all the Systems would remain on line for a minimum period of at least 400 days i.e. till the annual audit has been completed.

4.4.14 **Application Systems Modification**

Any new report required to be generated from any of the application systems should be provided by IT Department. However, if some major modifications required shall be undertaken by the service provider, presently IFCI Ltd.

5.4 Data Security

5.4.1 Data Backup Policy

- Full export dump of the database to be taken on an external hard disk and/or on CD/DVD.
- Full (Hot/Cold) back-up of Oracle database on daily basis along with Archival Logs.
- Copy of back-up of Oracle database on daily basis along with Archival Logs to be placed in Oracle Cloud.
- A copy of the export dump on external HDD/CD to be stored locally in a fire-proof safe.
- Daily back-up would be preserved for one month.
- The back-up created on the last day of every month should also be preserved for at least one year and should be checked periodically for readability.

6. E-MAIL AND INTERNET BROWSING POLICY

- E-mail/Internet facility for official purposes only.
- The Administrator would have the right to examine the contents of the official e-mails.
- The Administrator would also have the right to monitor the usage of internet facility by any user.
- No Spoofing.
- No unsolicited e-mail.
- All gambling/auction/pornographic sites would be blocked and not made available to users.
- The users would not be allowed to download big files which would choke the network.

7. STAFF TRAINING POLICY

- Training on operational aspects of the application systems by the System Administrator/ concerned IT service provider.
- Training to IT professionals through training programs for up-gradation of knowledge and exposure to new technologies.

- Periodic assessment of the IT training requirements should be formulated by the Human Resource Department on the recommendations of System Administrator/Chief Financial Officer to ensure sufficient, competent and capable human resources availability.

8. IT PROCUREMENT POLICY (HARDWARE/SOFTWARE)

- Preparation of specifications.
- Identification of suitable vendors
- Calling of quotations and placing the same for approval
- Approvals by Competent Authority as per delegation chart.
- Placement of orders
- Installation and Acceptance Testing.

9. ANNUAL MAINTENANCE POLICY

- Identification of suitable service providers.
- Entering into service level agreements should include:
  -Scope of work
  -Up-time warranty
  -Payment terms
  -Penalty Clauses, etc.
- Renewal of Annual Maintenance Contracts with the approval of Managing Director

10. BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY POLICY

Overview and Purpose

This document delineates the policies and procedures for technology disaster recovery, as well as process-level plans for recovering critical technology platforms.

Disaster Recovery (DR)" is the process of resuming, restoring or recovering the IT elements (computer systems, assets, and technological functionality) of a business process after an emergency, crisis, or other sudden calamitous event causing damage or loss to IT infrastructure.

Policy

- A formal risk assessment shall be undertaken to determine the requirements for the disaster recovery plan.
- The disaster recovery plan should cover all essential and critical infrastructure elements, systems and networks, in accordance with key business activities.
- The disaster recovery plan should be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
- All staff must be made aware of the disaster recovery plan and their own respective roles.
- The disaster recovery plan is to be kept up to date to take into account changing circumstances.
- All Key Personnel Contact Info must be kept handy.
- Key business processes and the agreed backup strategy must be in place.

TFCI has been taking full backup of the system/data on daily basis and keeps the same in fire proof cabinets and in Oracle Cloud space, which can be retrieved at any point of time. The responsibility of data/ disaster recovery lies with the System Administrator and the Chief Financial Officer. We propose to continue with the existing arrangement.

11. INFORMATION SYSTEMS AUDIT POLICY

The fundamental objective of the systems audit is to ensure that organization's assets are protected and suitable internal controls are in place to ensure protection against any unauthorised access to its information and information resources.

Information System (IS) audit evaluates the adequacy of the internal security controls with regards to System efficiency, standardization, Data integrity and safeguarding of information systems Assets / resources within TFCI.

Policy

<u>Protection of IT Assets</u>

- Audit Trails are designed in the system to record the activity at the system, application, and user level to support security objectives namely -
    - Detecting unauthorized access to the system.
    - Facilitating the reconstruction of events.
- Preventive controls are designed to prevent an error, omission or malicious act. Some of the actionable for preventive control includes

- Building Access control - Validation, edit checks in the application, implementing Passwords Policy.
- Authorization of transaction.
- Ensuring segregation of duties (SOD).
- Appropriate Documentation for applications, application usage and various processes followed.
- Firewalls.
- Anti-virus software

- Asset and security Classification - An inventory of assets is being maintained which includes physical, software and information assets.

IT controls regarding network security

This focuses on the various areas - like information security management, user account management, logical access security, authorization and authentication requirements, network infrastructure security.

Disaster Recovery processes

Adherence to Disaster recovery process is also reviewed from time to time.

We propose to get the IT system audit done from third party once in every two years to mend the security gap, if any, or to upgrade the security system, if needed.

Annexure-II

CHANGES IN IT POLICY FOR 2018-19 VIS-À-VIS PREVIOUS YEAR

Changes / Modification	2018-19	2017-18
IT Strategy Committee	IT Strategy Committee is proposed as per RBI direction No.RBI/DNBS/2016-17/53. DNBS.PPD.No.04/66.15.001/ 2016-17 dated 8th June, 2017.	Not provided
Asset Management	Asset Management Policy is proposed for the purpose of managing IT assets effectively.	Not provided
Data Backup Policy	Periodic full systems backup to be taken and kept locally in fire proof safe as well as in Oracle cloud.	Periodic full systems backup to be taken and kept locally in fire proof safe
Business Continuity Planning & Disaster Recovery	Specifically incorporated in current IT Policy.	Not specifically incorporated in earlier IT Policy but physically done.
IT System Audit	IT Systems Audit is proposed to evaluate the systems once in every two years to mend IT security gaps.	Not specifically provided