Tourism Finance Corporation of India Limited

INFORMATION TECHNOLOGY POLICY

FY 2025-26

INFORMATION TECHNOLOGY POLICY
FY 2025-26

The Information Technology Policy of Tourism Finance Corporation of India Ltd. (TFCI) for FY 2025-26 is based on Reserve Bank of India's Master Circular No. DoS.CO.CSITEG/SEC.7/31.01.015/2023-24 dated 07-11-2023 on Information Technology Governance, Risk, Controls and Assurance Practices.

1. OBJECTIVE OF IT POLICY:

(i) Integrate IT into business operations in line with the business objectives of the organisation.

(ii) Ensuring that IT system provides efficiency in processing and fully supports Risk Management, Cost Management, etc.

(iii) 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.

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

(v) Preventing unauthorised access/ use/ deletion/ change/ interruption of information and information services.

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

(vii) Explore and assess new and emerging technologies beneficial for the organization.

(viii) Establishing measures to monitor adherence to decisions and policies.

2. IT STRATEGY COMMITTEE OF BOARD & COMMITTEE OF EXECUTIVES

To periodically review and amend the IT strategies in line with the corporate strategies, Board Policy reviews, cyber security arrangements and any other matter related to IT Governance, an IT STRATEGY COMMITTEE of the Board has been constituted with an Independent Director as its Chairman.

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

- Approving 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 represent a balance of risks and benefits and that budgets are acceptable;
- Monitoring the method that management uses to determine the IT resources needed to achieve strategic goals and provide high-level direction for sourcing and use of IT resources;
- Ensuring proper balance of IT investments for sustaining NBFC's growth and becoming aware about exposure towards IT risks and controls.

The IT Strategy Committee in general, shall meet at frequent interval not exceeding six months. However, till the implementation of the approved IT infrastructure (hardware/software) is completed it is proposed that the Committee shall meet every quarter to monitor the progress.

Further, to ensure requisite IT compliances and updations in line with IT Strategy cum business requirements, a Committee of executives comprising of Managing Director, President, CTO/System Administrator and SVP (F&A) has been constituted. The Committee of Executives shall meet at-least once in a month or such shorter period as might be required.

3. IT ASSET MANAGEMENT GUIDELINES

3.1 Overview and Purpose

IT Asset Management is an important business practice that involves maintaining an accurate inventory of IT Hardware & Software, Software licensing information, maintenance/renewal and protection of hardware and software assets utilized by TFCI employees. The Asset Management Guidelines focuses on the following key activities of an asset life-cycle:

(A) Planning: All IT assets of TFCI must be -

- Acquired according to the needs.
- Recorded in the asset register as per the accounting practices.
- Evaluated at least once a year, to establish its condition as reflected on the asset register.
- Disposed-off or scrapped, in the event that the asset

  (i) is no longer serviceable.
  (ii) has reached the end of its useful life (About 5 years for both hardware/software).

(B) IT Procurement (Hardware/Software)

- Identification of requirement and specifications
- Identification of suitable vendors and obtaining quotations
- Approvals by Competent Authority as per delegation
- Placement of orders
- Installation and Testing

(C) Operation and Maintenance

- Identification of suitable service providers.
- Entering into service level agreements which should include scope, up-time warranty, payment terms, penalty clauses, etc.
- Renewal of Annual Maintenance Contracts (AMC) with the approval of the Competent Authority

(D) Disposal

- The disposal or scrapping of assets as contemplated should be recommended by IT Committee of Executives and approved by the Competent Authority/MD.

4. IT SECURITY GUIDELINES:

The purpose of IT Security guidelines is to control access to sensitive information, ensuring use only by legitimate users so that data cannot be read or compromised without proper authorization. The basic tenets would be:

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 when it is needed.

d) Authenticity – It is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine.

IT security would be ensured as under:-

4.1 Physical Security

- Restricted access to Server Room with CCTV surveillance
- Server Room Environment to be air conditioned, electrical distribution with MCBs installed, proper earthing, uninterrupted power supply (UPS) etc.
- Fireproof cabinets for storing back-up HDD/Tape drive

4.2 Security at the Network Gateway

The security at the Network Gateway shall be provided though Firewall/Router with Intrusion Detection & prevention, Virus/Spy-ware Protection, Access Control, Content Filtering, Spam Filtering, Network Address Translation, Denial of Service attacks (DoS), updation of Virus definition/Spyware/Prohibited Content at Firewall etc.

4.3 Security against Viruses/Spyware post Network Gateway

A second level of security shall be built-in through installation of a suitable anti-virus/anti-ransomware solution/software on servers as well as nodes which shall be updated regularly/periodically. Also the users would be educated/trained in various virus protection measures.

4.3.1 Security for Temporary Access to auditors/Application & Hardware service providers:

While providing access to eternal users the following guidelines need to be followed:

- Sanitisation of laptop/system need to be performed before providing the access and firewall VPN installation.
- The Anti-virus / Anti ransomware need to be installed on temporary basis.
- The access to be provided through secured Jump machine and no direct access will be given to the production environment.

4.4 Security built into Application Systems

Application systems should have security features as under:

4.4.1 Users and Logins

All oracle and/or other applications should be accessed through single entry point.

4.4.2 Username and Password

- Each user shall be provided with a unique username and password so that no unauthorised user can login to the system.
- A user should not be allowed to have multiple concurrent sessions.
- Passwords should be as per password guidelines given at point no. 8.

4.4.3 System Administrator

Officer designated as System Administrator shall be provided with valid user name and password with system administration and application administrator privileges. At present, the CTO/VP (IT) is designated as System Administrator.

The system administrator may create, drop, activate, deactivate a user. He may change system parameters, deciding access level of the users and their reporting officer, granting/revoking application administrator privilege to any user.

The system administrator on the recommendation of Heads of user department would provide application usage to designated employees.

4.4.4 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.
- As soon as a user ceases to be an employee of TFCI, his/her user account should be de-activated immediately and he/she should not be able to access any of the application systems. The IT-Manager/AVP and/or System Administrator would be responsible for deactivation and maintaining record of the same.
- Maximum three login attempts shall be permissible at a time. After three unsuccessful attempts login screen should be closed.

4.4.5 Access levels (Application System/Form/Menu)

The following should be the broad access levels:

- Control
- Passing / Authorization
- Preparation
- Query/View only
- No access

4.4.6 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.

4.4.7 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/machine, session id, etc.

4.4.8 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.

4.4.9 Application-wise login history

The system should also keep track of all application-wise login details. 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 Password History

The system should preserve all old passwords in an encrypted form.

4.4.11 User Account Log

The system should keep trail of all changes in the user account (creation/dropping/deactivation/reactivation of an id, granting/revoking system/application administrator privileges, changes in user profile, systems parameters etc.) along with details of date and time of changes, reason and changing authority.

4.4.12 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 be able to generate audit trail reports.
- The audit trail reports for 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.
- Complete Audit trail data of systems should be retained, wherever possible. In case retention of complete audit trail data is not possible, then data shall be retained for minimum period of 36 months.

4.4.13 Application Systems Modification

Any new report, module, functionality required to be incorporated in any of the application systems should follow the change management guidelines as described in Item no 12.

5. DATA SECURITY GUIDELINES:

5.1 Data Leak prevention:

- Any data download in external/removable drive will be restricted for the user.
- Access to external/removable drive be only used for back shifting purpose by IT department.
- Read-only access to removable drives containing the digital signature will be provided to users holding digital signature dongles.
- All different admin/super-admin passwords of IT hardware and IT applications, out of the band management network access port. i.e IIM ports, Virtualized layer, Firewalls, applications, backup encryption, mailing admin, mail archiving solution application, and database will only be used by CTO.
- Sealed envelope containing all the passwords will be available with WTD & President and the passwords should be changed/updated as and when required.
- Sub admin users with limited access & rights for maintenance activity will be provided to IT department to perform their day to day support activities.
- TFCI owned Laptop/Desktop will be provided to the auditors/vendors along with firewall VPN to login into TFCI network with view only & limited access.

5.2 Data Backup & Archive

All forms of data storage are subject to data loss (eg: disk crash) and therefore necessary steps must be taken to ensure there are copies of all important data, called backups.

Users shall be responsible for the security of data on their desktop/laptops including backups of all important data on the official google drive or on official office 365 drive installed on their desktops/ laptops. Information stored on central servers to be backed up regularly by IT Dept.

Data related to investor and regulatory filing will be available on the website for 7 years or the period as may be prescribe by RBI, SEBI or any other regulatory authority.

5.2.1 Overview

These guidelines define the backup policy for computers within the organization which are expected to have their data backed up. These systems are typically Databases, Application servers, servers, Network equipment's, San Storage, Backup application, Tape Drive, San switch etc. but are not necessarily limited to servers, Applications, Databases etc.

5.2.2 Purpose

These guidelines are designed to protect data in the organization to be sure it is not lost and can be recovered in the event of an equipment failure, disaster, destruction in data, or any force majeure situation.

5.2.3 Definition

(a) Backup - The saving of files onto magnetic tape or other offline mass storage media or on the cloud for the purpose of preventing loss of data in the event of equipment failure, disaster, destruction in data, or any force majeure.

(b) Restore - The process of bringing off-line storage data back from the offline media and putting it on an online storage system such as a file server etc

5.2.4 Timings

Differential backups to be taken at night on weekdays. If backup not performed for any reason on any weekday in the night, then same shall be done on next working day morning.
Full backups to be performed weekly at night on Sunday. If for maintenance or any reasons; backups are not performed on Sunday they shall be done on Monday morning.

5.2.5 Disk Storage

TFCI has separate backup server with capabilities to cater/bear two (2) disk failure i.e. Physical RAID5 with one hot spare is configured in Backup server.
At least one encrypted copy of each daily, weekly and monthly backup will be kept reserved on backup server at any given point in time. Transfer of backup on tap drive and cloud should be on weekdays' basis.

Glossary Note :
RAID – RAID ("Redundant Array of Inexpensive Disks" or "Redundant Array of Independent Disks") is a data storage virtualization technology that combines multiple physical disk drive components into one or more logical units for the purposes of data redundancy, performance improvement, or both.

Disk Array -A disk array, also called a storage array, is a data storage system used for block-based storage, file-based storage or object storage. The term is used to describe dedicated storage hardware that contains spinning hard disk drives (HDDs) or solid-state drives (SSDs). In more simpler words, A disk array is a disk storage system which contains multiple disk drives. It is differentiated from a disk enclosure, in that an array has cache memory and advanced functionality, like RAID, de-duplication, encryption and virtualization.

RAID5 -RAID 5 is a redundant array of independent disks configuration that uses disk striping with parity. Because data and parity are striped evenly across all of the disks, no single disk is a bottleneck. Striping also allows users to reconstruct data in case of a disk failure. RAID 5 evenly balances reads and writes, and is currently one of the most commonly used RAID methods. RAID 5 groups have a minimum of three hard disk drives (HDDs) and no maximum. Because the parity data is spread across all drives, RAID 5 is considered one of the most secure RAID configurations.

5.2.6 Tape & Cloud Storage

TFCI has separate set of tapes for each backup day including weekdays and Sunday.

- Backups performed on Weekday shall be kept for one week and used Tape drive can be reused again the following appropriate day of the week. Also, Weekday tape data backup should be upload in encrypted form to secured cloud location on same working day except Saturday.
- Backups performed on Sunday shall be kept for four(4) weeks and Tape drive shall be used again on the next applicable Sunday.
- Weekly Sunday tape data should be upload in encrypted form to secured cloud location on next working day & physical tape should be placed in fireproof vault after completing the process

5.2.7 Tape Drive Cleaning

Tape drives shall be cleaned on monthly basis and the cleaning tape to be changed after maximum 50 times of usage or earlier as per the requirement.

5.2.8 Monthly Backups

Monthly backups are performed every month on weekly backup tape on 10th of every month or on the next day (if 10th happens to be a holiday) and tape data will be upload in encrypted form to secured cloud location and history of the same is maintained in excel in below mentioned format. Also, monthly backup physical tape should be placed in fireproof vault after completing the process.

5.2.9 Age of tapes

The service start date shall be recorded on each tape itself or in the backup software. Tapes that have been used for longer than 1 year or upon showing read/write error, shall be discarded safely and replaced with new tapes.

5.2.10 Responsibility

CTO shall delegate a member of the IT department to perform regular backups. The delegated person shall share the email to business users for the availability of the latest backup in restored environment for testing.
Business users need to test the ability of the latest restored data and need to confirm by email within one (1) working day.
Delegated member of IT Department after completing the process, will publish the final result through email communication with subject line mentioning the status of Backup restore as success or failure.
If case of failure, suitable measures need to be taken for effective restoration & testing and redo the backup & testing through new tape media or after fixing the error.

5.2.11 Testing

The ability of the latest restored data from backups shall be tested at least once per month and business users need to check & confirm back over restoration email from IT department.

5.2.12 Data Backed up

Data to be backed up include the following information:

- System state data of Hyper-V virtualized hypervisor
- Guest operating file level back up on the OVM platform
- Guest operating file level back up of the any standalone physical server
- Latest Configuration file of firewall, Configuration of network switch, configuration of SAN switch, Configuration of back software
- Image copy of all used operating systems
- Image copy of all Installed - RPM & Windows Installation packages on servers

Systems to be backed up shall include but not limited to the following:

- File server
- Production Database server
- Production web/application server
- Domain controllers
- Additional Domain controllers

5.2.13 Restoration

Users needing data restoration from the backed-up data, must submit a request to the CTO/system administrator with an approval from the departmental head, including specification/details of data backed up earlier by IT team to be restored.

5.2.14 Ransom ware Prevention Guidelines in backed-up data

To prevent the attack of ransomware in already backed-up or archived data, backup should be encrypted immediately & automatically from backup software itself to prevent the any future attack on backed up data

6. E-MAIL AND INTERNET BROWSING GUIDELINES

- E-mail/Internet facility shall be for official purposes only.
- The System Administrator would have the right to examine the contents of the official e-mails and monitor the usage of internet facility by any user.
- No Spoofing and unsolicited e-mails permitted.
- All gambling/auction/pornographic/e-Commerce sites would be blocked.
- The users would not be allowed to download big files which would choke the network i.e. 25 MB threshold limit setup by Gmail for attachment

7. STAFF TRAINING GUIDELINES

- Staff Training on operational aspects of the application systems by the system Administrator/concerned IT service provider as and when required.
- Periodic assessment of the IT training requirements to be done by CTO/system administrator and training facilities to be provided by HR Department to ensure sufficient, competent and capable human resources availability.

8. PASSWORD GUIDELINES

8.1 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in a compromise of the entire network of TFCI. As such, all employees and external users having access to TFCI systems such as auditors/vendors, etc. shall be responsible for taking appropriate steps, as outlined below, to select and secure their password.

8.2 Purpose

The purpose of these guidelines is to establish a standard for the creation & use of strong passwords, protection of those passwords, and the frequency of change as required.

8.3 Scope

The scope of these guidelines includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any TFCI facility, has access to the TFCI network.

8.4 Detailed Guidelines

8.4.1 General

- All system-level passwords (e.g., root, enable, network administrator, application administration accounts, etc.) and user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days and last 1 password cannot be reused.
- All production environment system-level passwords must be part of the Information Security Document under the custody of MD/WTD/President/CTO.
- Passwords must not be inserted into email messages or other forms of electronic communication and any instance of sharing should be reported to CTO as security breach.
- All users must ensure that user-level, system-level passwords must confirm to the guidelines described below.
- Two factor authentication (2FA) should be enabled wherever it's supported and applicable like:
  - ✓ Online Email account login
  - ✓ Subscribed SaaS Cloud applications
- If two factor authentication (2FA) is not available then at-least option for the active directory (AD) integration needs to be explored.

8.4.2 Password Construction Requirements

i. Minimum length of eight (8) characters on all systems.
ii. Should not be a dictionary word or proper name.
iii. Should not be the same as the User ID.
iv. Must change on/before expiry of 90 calendar days.
v. Should not be identical to the previous password.

vi. Should not be transmitted in the clear or plaintext outside the secure location.
vii. Ensure passwords must be reset by authorized users.
viii. Should contain at least one upper case, one lower case, one numeric and a special character.

8.4.3 Password Deletion

All users which are no longer needed, must be deleted or disabled immediately. This includes, but is not limited to, the following:

- When a user retires, resigns dismissed, etc.
- Default passwords shall be changed immediately on first use.
- Contractor accounts, when no longer needed to perform their duties.

When a user id is no longer needed, the following procedures should be followed:

- HR Department should notify on an email/written request regarding user separation and send it to IT Department.
- IT Department will then delete/inactivate/suspend the user's account.

8.5 Application Development Standards

IT department to ensure that all programs by application developers must contain the following security precautions:

- Support authentication of individual users, not groups.
- Not store passwords in clear text or in any easily reversible form.

8.6 Remote Access Users

Access to TFCI's network via remote access is to be controlled by using either a Virtual Private Network (in which a password and user id are required) or a form of advanced authentication (i.e., Biometrics, Tokens, Public Key Infrastructure (PKI), Certificates, etc.).

8.7 Disciplinary Action/Penalties

All passwords are to be treated as sensitive, Confidential TFCI information. In case an employee knowingly shares the password/provides access to an unauthorized user then he/she is subject to disciplinary action from the Competent Authority.

9. BUSINESS CONTINUITY PLANNING (BCP) AND DISASTER RECOVERY (DR) GUIDELINES :

Overview and Purpose:

This document delineates the guidelines 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 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.

DR Guidelines:

- The responsibility of data/disaster recovery lies with the System Administrator/CTO.
- To minimize data loss, maximize availability of computing resources in the event of outage at primary Data Centre TFCI shall implement Disaster Recovery (DR) site for business-critical data and applications.
- Disaster Recovery (DR) site must be at a geographically different location and different seismic zone from the primary Data Centre.

- Synchronization of data between Primary and DR Site to be continuous and replication of programs must be at least once a day which shall be monitored on daily basis on all working days.
- In the event of any disaster at the primary site the DR Site shall be upgraded to primary site till the restoration of original primary site.
- The DR drills / testing shall be carried out at least on a half-yearly basis.
- In addition to above TFCI has been periodically taking full backup of the system and keeps the same in the backup server, backup tape drive in fireproof cabinets and in Oracle Cloud for different seismic zone as per data backup and archive guidelines which can be retrieved at any point of time. This will be in addition to the DR site implemented as above.
- Recovery Point Objective(s) (RPO), RPO = 15 minutes
- Recovery Time Objective(s) (RTO), RTO = 1 hour

Further, Recovery Time will be considered from the time it has been declared as disaster by the competent authority/MD.

10. INFORMATION SYSTEMS AUDIT GUIDELINES:

The fundamental objective of the systems audit is to ensure that organization's assets are protected and suitable internal controls are in place/not interfered during a particular time frame by unauthorised access to protect its information and information resources.

An approved IT Audit firm shall be appointed to carry out Information System (IS) audit once in year and it should be prior to statutory audit. Vulnerability Assessment (VA) of systems shall be conducted in every six months and Penetration Testing (PT) shall be conducted once in 12 months.

10.1 Detailed Guidelines for IT Audit

I. IT Audit shall cover the following:

- Audit Trails to detect unauthorized access to the system & facilitating the reconstruction of events.
- Preventive controls such as
  - Building Access control - Validation, edit checks in the application, implementing Password Guidelines.
  - Authorization of transaction.
  - Appropriate Documentation for applications, application usage and various processes followed.
  - Firewalls
  - Anti-virus software
- Asset and security Classification

II) IT controls regarding network security

Audit of various IT controls such as: Information security management, user account management, logical access security, authorization and authentication requirements, network infrastructure security.

III) Disaster Recovery processes

Adherence to Disaster recovery process to be reviewed from time to time.

11. ACCESS CONTROL GUIDELINES:

11.1 Overview and Purpose

Access to TFCI computing resources is granted in a manner that carefully balances restrictions designed to prevent unauthorized access against the need to provide unhindered access to informational assets. The guidelines sets forth rules for

establishing, access control - determining the allowed activities of legitimate users and mediating every attempt by a user to access a resource in the system.
The main objectives of access control guidelines are described in terms of protecting system resources against inappropriate or undesired user access. Access to IT Application systems will be limited to authorized persons whose job responsibilities require it, as determined by an appropriate approval process, and to those authorized to have access by competent approving authority.

User Access Management includes issuing, Approving, maintaining, and removing a user's access to various components of Tourism Finance Corporation of India (hereafter referred to as TFCI) like IT infrastructure such as network, specific workstations, databases, network devices and applications in a controlled manner.

11.2 Dependency/ Reference
Item No. 8.0 Password Guidelines

11.3 User Access Management Procedure

11.3.1 User Registration Procedure for TFCI Employees
For every new employee, the immediate supervisor/Department Head or HR should initiate the process by providing the details.

11.3.2 User Registration Procedure for Vendor Employees
Vendor SPOC: Vendor SPOC refers to the respective Department head/ Manager dealing with the Vendor. For every new Vendor employee, the Vendor SPOC should:

a. Review the Vendor employee roles and responsibilities, accordingly identify the different infrastructure components such as Firewall VPN and Application etc. required for the candidate;
b. Define the privilege levels to be assigned for each of the identified Infrastructure components, wherever applicable. Privilege level should be defined on the 'least privilege View' basis, i.e., the minimum privilege required for fulfilling the candidate's Department role;
c. Define the time period till which access needs to be granted;
d. Fill up the User ID Registration Form provided in Annexure I with the above details; and
e. Authorize the User ID creation and forward the same to the IT Department.
f. Dependency/ Reference: Item no. 4.4.4
    - If in any case access to the auditors needs to be given on an external system other than TFCI laptop/system then access control guidelines needs to be followed and sanitisation of laptop/system need to be performed in advance before providing the access and firewall VPN installation
    - Temporarily for limited time period antivirus & anti ransomware need to install on the auditors/vendors machine if same is not available till the time access is allowed
    - Any access to auditors/vendors need to be provided through secured Jump machine only and no direct access will be given to the production environment directly

11.3.3 Privileged Accounts Only for IT admin
Privileged account should only used by CTO /IT Manager for admin purpose and there should be no transactional activity performed; This is used to resolve the problems, password reset and system administration related activity.

11.3.4 User ID Management Procedure Guidelines

- A user requiring any changes to the assigned privilege levels for business reasons should request the same to his/ her respective Department Head/ or Vendor SPOC.
- The Department Head/ or Vendor SPOC should review and validate such requests and, accordingly, either reject or authorize, based on business requirement.
- The IT Department should perform relevant changes to privileges after receiving an approval from the concerned Department Head.
- The IT Department should maintain a record of all privilege changes performed on User IDs. The record should, at the minimum, include the following details:
    - User ID;
    - Current access and privilege levels;
    - Requested changes to access and privilege levels;

11.3.5 Removal of User Access procedure

- Whenever an employee user access is to be revoked, the Department Head should communicate the same to the HR Department.
- The HR Department should determine the last date till which the user's access is to be allowed and intimate the same to the IT Department and the Department Head.
- Whenever a Vendor employee's access is to be revoked, the Vendor SPOC should determine the last date till which the user's access is to be allowed and the same shall be intimated to the IT Department.
- On the designated last date, the IT Department should:
    - Change passwords of all access accounts that the departing user or Vendor staff had access to;
    - The User ID should be disabled/deleted but in any case safeguard the logs
    - Remove all access assigned to the respective User ID;
    - Notify the respective Department Head, HR Departments or Vendor SPOC and about the successful completion of task.

- Exceptions for revocation of access prior to designated date
    - The Department Head/or Vendor SPOC can instruct the IT Department for revocation of access rights immediately or prior to the last date for the following scenarios:
    - When the Department Head/ or Vendor SPOC determines that access to selective critical business infrastructure resources need to be revoked for a user; or
    - When a user is terminated from the job Department or the contract agreement with a Vendor is terminated prematurely;

11.4 Responsibility

All TFCI employees/Vendor Employees are instructed to protect confidentiality of company information by following all given guidelines including:

- keeping passwords confidential and changing them when directed/force by system
- logging out of workstation and/or remote connection when not in use
- not allowing any other staff or member access to workstation while logged in
- not copying company information onto other media without authorization
- having confidentiality agreements signed when any Company information is shared via disk, modem or other media to outsiders
- securing offices when not present

- Reporting lost or stolen keys/laptop/mobile etc.

Furthermore, staff is required to respect confidentiality of any data not meant for their review. This includes documents left in printers and fax machines, files open on or accessible through a computer, and similar situations. Staff is prohibited from accessing another user's files without specific authorization.

11.4.1 Before leaving:

- Employees need to clean out all personal email and archive any useful business outlook data for next user.
- Backup all data to an archive network folder.
- Employees need to organize their company data for future user's easy access When they leave.

11.4.2 After leaving:

The IT department must ensure that the employee's login, access to their PC and other information is no longer available to them. It is also a common practice to suspend or redirect & suspend the respective email.

- Disable access to the company network.
- Disable access to the Active Directory user account
- Change admin/master passwords of all the applications if employee had access to them.
- Disable/Delete user id from all applications.
- Lock/suspend & take backup of user system.
- Disable the employee's Office 365 user account.
- Suspend/Change Office 365 account access and select a new user (if any).
- As per request from reporting officer of leaving employee, IT Department will transfer Backup to the reporting officer or new joinee.

12. CHANGE MANAGEMENT (CM) GUIDELINES & PROCEDURE

12.1 Change Management

This Change Management (CM) guidelines & procedures manual defines the steps necessary to implement and maintain change management processes for TFCI and define the items needed for effective CM, establish the roles of the people involved, describe the actual steps of the CM process, and specify how they can be accomplished.

12.2 Objective of Change Management (CM)

The objective of CM is to minimize the adverse impact of required changes on system integrity, to preserve security, to enable the coordination and planning of changes in order to provide a stable production environment, and to maximize the productivity of persons involved in the planning, coordinating, and implementation of quality changes.

12.3 Scope

The intended scope of the Change Management Process is to cover all of the company's computing systems and platforms. The primary functional components covered in the Change Management process.

- Hardware – Installation, modification, removal or relocation of computing equipment.
- Software – Installation, patching, upgrade or removal of software products including Operating systems, access methods, Packages and utilities.
- Database – Changes to databases or files such as additions, reorganizations and Major Maintenance.
- Application – Application changes being carried out as well as the Integration of new application systems and the removal of Obsolete elements.
- Moves, Adds, Changes and Deletes – Changes to system configuration.

- Schedule Changes - Requests for creation, deletion, or revision to job schedules, backup schedules or other regularly scheduled jobs managed by IT Department.

12.4 Philosophy of Change Management

IT Department is responsible for servers and software applications (including related modules, services, and interfaces) that are used by end users with responsibilities encompassing all areas of organization. Technology is thoroughly ingrained in most the departments, and therefore any change has the potential to be significant. It is therefore critically important to manage change in a proactive and effective manner.

12.5 Definition

12.5.1 Change - the addition, modification or removal of anything that could have an effect on IT System's, Software's, Applications, Database and/or Services.

12.5.2 Change Advisory Committee (CAC) - The Change Advisory Committee shall oversees change procedures, validates and approves documented changes and reviews and approves all changes.

The CAC shall be responsible for reviewing the information provided in every change request in order to ensure that the changes are sufficiently researched, documented, planned, and executed.

The Committee shall comprise of Manager-IT, CTO, HOD of respective department requesting change, President and ED/WTD (Optional).

12.5.3 Change Initiator (CI) – The Change Initiator is responsible for initiating the change request, submitting Change request to CAC along with the need for change, gathering input from the cross Department and presenting the changes to the Change Advisory Team, providing information and getting approval from the Change Advisory Committee (CAC) and also serves in a communications role, and therefore takes on the responsibilities of the Department Communicator

12.5.4 Manager IT – Executing and evaluating, the Change Initiator document for the change. For most IT projects, Manager IT may be the CI and also serves in a communications role, and therefore takes on the responsibilities of the IT Department Communicator

12.5.5 Change Management (CM) – the process of documenting a change, reviewing the potential impact of that change, controlling the timing of the change and, upon completion, verifying the completeness of the change.

12.5.6 Change Manager (CMGR)- The Change Manager is a member of the IT Department, who is responsible for changes in a particular area of responsibility. In addition, based upon the information provided, the Change Manager should verify that all scheduled changes do not conflict with each other. The Change Manager has the authority to at any time defer any change which they feel to be improperly classified, lacking information or which in any way represents a potential problem that will affect Tourism Finance Corporation of India Ltd.'s systems availability or network integrity. For most IT projects, Manager IT may be the CMGR also.

12.5.7 Change Request (CR) – A broadly-defined term that describes the overall process of requesting change.

12.5.8 Emergency Change – A change to systems that requires circumvention of the specific change management process in order to meet an immediate and critical need. Such a change should still involve as much approval and management as is practical, and in all cases should be recorded appropriately.

12.5.9 Implementation – A major change to a system or systems that is typically planned in advance and requires a lengthy procedure and associated documentation. This usually applies to new software packages or major changes to existing packages that require a coordinated planning effort.

12.5.10 Modification – A minor alteration to a system that is brought on by a change in user requirements or a technical problem. Typically only affects one process or function in a system.

12.5.11 Normal Change –Normal change is a change to end-user or IT systems that requires adherence to the change management process as defined in these guidelines. Change types classified as Minor, Moderate, and Major should all be classified as Normal changes, with Emergency changes being the only exception.

12.5.12 Subject Matter Expert (SME)- The Subject Matter Expert is the person who will coordinate a change and provide information for the Change Management Process. This does not mean that the SME is necessarily the one who is implementing the change, just that they are knowledgeable about the change, can provide any information needed and will make sure that the process is followed by the actual person or persons implementing the change. In most cases the SME enters the change information to the Change Management System and attends the Change Advisory Board meetings regarding the change. SME may be third party vendor or Change Initiator (CI) or Manager IT or Change Manager (CMGR) or CTO

12.5.13 System Modification – A change to system tables, reports, configuration, system guideline etc. that represents a departure from the original version that was originally implemented.

12.5.14 Trusted Operating Procedure (TOP) - a routine change that has been proven to be performed the same way every time and should not require the same level of review each time. It should be sufficient to conduct these changes according to an agreed upon as per any annexure prepared from time to time or as per the defined process by patch/update supplying vendor

12.5.15 Update – A group of minor alterations or modifications to an existing system that is brought on by a change in user requirements or a technical problem. Typically affects multiple processes or functions within a system.

12.5.16 Upgrade – A major change to an existing system, similar to an Implementation defined above. The category of changes can be product support, enhancements, roadmap patches by vendor, others.

12.5.17 UAT – User acceptance testing

12.6 Mitigating Control:

Business users UAT testing is mandatory for system modification & application upgrade Business users UAT testing will only be done if recommended by vendor, for the change cases of Roadmap patches update, hardware firmware upgrade/ patches, operating system patches, virtual layer patches, Network equipment upgrade/patches, San Fabric & San Storage etc.

HOD/President approval is optional for support related incident/tickets raised by users while they face any issue in day to day operations. However, IT department may ask for HOD/President approval in some cases.

In case where issues identified by IT department ticket will not be raised and issue will be directly communicated to vendors for resolution in such cases Manger IT/CTO, may also recommend for any of the following case as per the requirement

1. Business UAT along with IT Department UAT
2. Only IT department UAT as the case may deemed fit.
3. Only Business UAT
4. UAT not at all required

12.7 Process Consideration:

In order to effectively accomplish the objectives defined in this section, the CM Process must incorporate the safeguards as listed below :

1. Ensure the documentation of all proposed changes prior to the modification of the production environment.
2. Confirm technical completeness: accuracy of technical impact and risk analysis plans for final test, install, back-out and recovery.
3. Identification and review of all technical dependencies including effect on concurrent changes.
4. Guarantee that the timing of change executions does not conflict with the business cycles or priorities.
5. Verify the documentation of actual change installations and/or change back-outs;
6. Enable communication of change results, to provide a history of changes, and to support the maintenance of systems documentation.
7. Service Level Agreements / Vendor Maintenance Agreements (since many changes must be coordinated with Vendors and their cooperation is critical).

12.8 Change Advisory Committee (CAC)

The objective of the CAC is to review & approve Business users purposed changes and thereafter project planning, evaluate and determine a resolution method for conflicts, and identify potential CM concerns before they become problems. The CAC if required may review current ongoing projects and determine if there are additional steps that need to be taken to ensure that the planned change is handled effectively.

The CAC for projects shall comprise of Department Heads i.e. finance, Admin, HR, Legal, Project, Monitoring & IT or who will be involved in /affected by the change. The population of the CAC will change based on the type of project/change is needed. The Change Initiator will report to CAC on discussions and proposals at the meeting(s).Meets may be monthly/weekly or as and when required

12.9 Change Management Applicability

This section provides the guidelines background for the depth of response required for various CM activities.

12.9.1 System Modification

12.9.1.1 Implementations and Upgrades

Implementations of new software and upgrades of existing software to be governed as per the request process. These are treated as Normal changes.

12.9.1.2 Modifications / Updates

Planned modifications existing in-house software are to be recorded in excel and managed accordingly. These are treated as Normal changes.

12.9.1.3 Emergency/Unplanned Modifications & Updates Changes

These changes can be treated as Emergency Changes and should be implemented according to the Emergency Change requirements found later in this document.

12.9.2 Determine the Risk & Impact:

Risk - Risk is a measure of how the proposed change will affect the actual components of the Production Environment being changed, the remainder of the Production Environment, and any resource required to complete the change or to recover from the change should a rollback be necessary.

Impact - Impact is a measure of how the proposed change will affect the users' ability to access and use the system and thereby their ability to perform their job, both directly and indirectly.

It shall be the responsibility of the CI/IT Manager/CMGR/CTO/SME to fully justify in the change request their reasoning for assigning a particular risk and impact level to their change and failure to do so may result in their change being deferred until such an explanation is provided or clarified to the Change Advisory Team's satisfaction.

Details	Risk	Impact
None	The change, communication and back-out procedures have been well documented, repeatedly tested and proven to have no impact on any production software or hardware. Work is to be performed strictly according to the Trusted Operating Procedure (TOP)	The change has been repeatedly tested, documented, and proven to have no impact on the users. The work is to be performed according to the pre-approved documented instructions .i.e. Trusted Operating procedure (TOP)
Low	The change, communication and back out procedure have been tested and proven to impact only part of a single application and/or a single piece of hardware. Work is to be performed outside of a defined maintenance window but the production software or hardware to be changed will not be significantly affected by the change and the remainder of the production environment will not be affected. The user has agreed to the change and the time. All required resources have been contacted and are confirmed to be available for the change timeframe.	The change has been tested and proven to impact only a small, well defined group of users, a single function of an application and/or a single piece of hardware. Work is to be performed outside of a defined maintenance window but the user's normal work will not be significantly impacted by any downtime the change may cause. The user has been informed of the change in advance and agreed to the change and the time
Medium	The change, communication and back out procedure have been tested and proven to impact a single application or piece of hardware. Work is to be performed in a predefined application maintenance window, the production software or hardware to be changed will not be significantly affected by the change and the remainder of the production environment will not be affected.	The change has been tested and impacts a clearly defined group of users, a single application and/or a single piece of hardware. Work is to be performed in a predefined application maintenance window when users are not normally using the application or hardware. User's normal work will not be significantly impacted by any downtime the change may cause.

	All required resources have been contacted and are confirmed to be available for the change timeframe	User is informed in advance that the maintenance window will be used
High	The change may or may not have been tested and likely impacts more than one, possibly not clearly defined application or piece of hardware. Work is to be performed in a predefined system maintenance window. The production software or hardware to be changed could be significantly affected by the change or the remainder of the production environment could be affected. All required resources have been contacted and are confirmed to be available for the change timeframe	The change has been tested; impacts clearly defined multiple groups of users, multiple applications, and/or multiple pieces of hardware. Work is to be performed in a predefined system maintenance window when users are not normally using the affected applications or hardware. User's normal work may not be significantly impacted by any downtime the change may cause. User is informed in advance of when the changes will occur
Unknown	The change could not be tested or the tests did not clearly show the risks. The users and/or hardware impacted by the change are unknown or not easily defined. The change will impact the production software or hardware to be changed and could significantly affect the production environment. The change will likely impact the production environment outside of predefined maintenance windows. All required resources have been contacted and are confirmed available for the change timeframe	The change has not been tested or tests do not clearly show the impact on the users. The users and/or hardware impacted by the change are unknown or not easily defined. Change likely to impact users outside of the predefined maintenance windows. User's normal work could be impacted by the downtime the change may cause.
Emergency	Change is to fix a problem that is, or is soon likely to, impact the production environment. The existing situation does not allow for the normal CM process to be followed	The change is to fix a problem that is, or is soon likely to, impact the users. The existing situation does not allow for the normal CM process to be followed. A full justification of the risk and impact level and the change type must to be entered by the CI on the change request for review by the Change Advisory Team. The CTO and the CAC have the right to alter the change type of a change request if they feel the justification provided does not meet the type selected.

12.9.3 Develop Test/UAT Plan

The Test Plan or Procedure is the method by which the change can be implemented in a test environment in order to determine if it will work. The change should not be implemented until it has been tested and the results are validated in the test/UAT environment.

12.9.4 Develop Rollout Plan

A Rollout plan or procedure is the method by which a change will be implemented in the Production Environment. The details of the rollout plan will be dependent on the size of the project, how many systems are affected, how many users are impacted, etc.

12.9.5 Develop Rollback Plan

A Rollback plan or procedure is the method by which a change will be undone, and the system set back to its pre-change state.

12.9.6 Implement Test Plan

Prior to submitting the change for approval, you should ensure that the change has been tested and is successful in a test/UAT environment.

12.9.7 Review Change Information

This step is simply a checklist item to indicate that all Change information has been recorded in the Project Management documents/Project Excel or the Change Management Checklist.

12.9.8 Approval/Rejection of the Change

CTO will review the request via the information in the CM document in order to confirm that all change parameters have been satisfied according to change request.

12.9.9 Record Change Status

The status of all change request needs to be recorded upon completion or back-out as soon as possible on the next business day following the change.

Details of the work performed, any problems encountered and any notes or observations on the change or something related to the change should be entered into the change request document/project excel. The Change Manager/IT Manager/CTO will review the change request the next business day and, if it is determined that the change was implemented successfully, the change request can be closed.

There are times when changes are immediately required to fix a problem that is, or is soon likely to, impact the production environment and the users. When this type of situation does not allow for the normal CM process to be used, the Emergency Change process can be followed as under:

Step I: Identify the need for a change which in emergency cases means that there is an event such as a network outage, a server problem, or a failure of an application that requires quick action to restore the usability of the technology resource.

Step II: Person who identifies the need for a change will open a request on Email with an appropriate change type. Typically, emergency will be coded as Subtype: "System Modification" and the CC will be the CAC Committee members. If someone else besides the CTO identifies the need and creates that ticket, it should be assigned to the CTO or someone else appropriate for the task like application support vendor or hardware support

Step III: If the ticket already exists then the Change Coordinator will access the ticket that initiated the need for the change. For example, if a call was made to the IT Help Desk by an end user stating that a particular error message was occurring, the IT manger/CTO/CMGR would open the ticket that serves as the record for that call. The IT manger/CTO/CMGR will change the ticket so that the subtype is "System Modification/Emergency Change request".

Step IV: The CTO will make a guideline-based judgment decision on the recommendation i.e. either to proceed, modify the plan, or do nothing pending further review. If the CTO is not available, the IT manager/CMGR will make a guideline-based judgment decision and implement the change.

12.10 Trusted Operating Process (TOP)

IT Department performs many changes that are repetitive and routine, so subjecting them to the full Change Management review process every time is inefficient and unnecessary. If a change is proven to be performed the same way every time it should not require the same level of review as a more complex item would. For these types of

routine changes it should be sufficient to conduct them according to an agreed upon, well documented, and well tested procedure. This procedure is known as a Trusted Operating Procedure (TOP).
Once the procedure has been well documented, proven to work successfully and repetitively (including the back-out procedure), and proven to not impact the production environment, a procedure can be submitted to the CTO as a TOP candidate. Once the procedure has been proven to the CTO/CAC to work as documented a minimum of 3 times then CTO /CAC can approve the procedure as a TOP.

The first step to creating a new TOP is to properly document all aspects of the change and provide clear, easy to follow instructions for others to be able to follow. Each TOP requires all of the following areas to be filled out:

12.10.1 HOW A PROCEDURE BECOMES A TRUSTED OPERATING PROCEDURE

- The procedure has been well-documented
- The documentation has been proven to work successfully and repetitively (at least 3 times) The rollback procedure has been tested
- There is no impact to the production environment

When these requirements are met, the procedure document should be submitted to the CTO /Change Advisory Committee(CAC) as a TOP candidate. The CTO/CAC will review the contents of the document to make sure that it meets the requirements of a TOP. Once satisfied, the CTO/CAC will approve the procedure document as a TOP Candidate that is ready for testing.

When the document is approved as a TOP Candidate, the procedure itself must be proven to work strictly as documented

Process/scripts/rollback plans and documents received from vendor as a part of roadmap update/upgrades/fixes to execute the same , will also be treated as TOP and will not be entitled for 3 time testing or change management process.

13. CYBER SECURITY POLICY AND CYBER CRISIS MANAGEMENT PLAN (CCMP)

This policy is distinct and separate from the broader IT Security policy and IT Policy to highlight the risks from cyber threats and the measures to address / mitigate these risks.

13.1 CYBER SECURITY POLICY (CSP)

13.1.1 Overview and Objective

Cyber security is the practice of protecting systems, networks, and programs from digital attacks. These cyber-attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes. The main objective of cyber security guidelines is to facilitate identification, prioritisation, assessment, remediation and protection of critical infrastructure and key resources based on the plan for protection of critical information infrastructure.

13.1.2 IS Framework

- Identification and Classification of Information Assets (Hardware/Software) would be maintained.
- Entry to the Data Centre should be restricted to the authorised person.
- Access to information shall be based on well-defined user roles.

- Maker-checker system will be incorporated in application system for authorisation to reduce the risk of error and reliability of information.
- The incident, if any will be reported to System Administrator who would take necessary actions to ascertain cause of incident and ascertain preventive measure.
- Systems should have audit trails to record improper activity.

13.1.3 Vulnerability Management

13.1.3.1 Purpose

The purpose of the Vulnerability Management clause is to establish the rules for the review, evaluation, application, and verification of system updates to mitigate vulnerabilities in the IT environment and the risks associated with them.

13.1.3.2 Endpoint Protection (Anti-Virus & Anti-Ransomware)

- All TFCI owned and/or managed Information Resources must use the TFCI IT management approved endpoint protection software and configuration.
- All non-TFCI owned workstations and laptops must use TFCI IT management approved endpoint protection software and configuration, prior to any connection to a TFCI Information Resource.
- The endpoint protection software must not be altered, bypassed, or disabled.
- Each email gateway must utilize TFCI IT management approved email virus protection software and must adhere to the TFCI's rules for the setup and use of this software, which includes, but is not limited to, scanning of all inbound and outbound emails.
- Controls to prevent or detect the use of known or suspected malicious websites must be implemented.
- All files received over networks or from any external storage device must be scanned for malware before use.
- All TFCI owned and/or managed Information Resources must use the proxy wherever it possible with in TFCI premises otherwise CTO need to approve the use of firewall gateway with valid reason

13.1.3.3 Logging

- Baseline configurations for Information Resources must include log settings to record actions that may affect, or are relevant to, information security.
- All servers and network equipment must retrieve time information from a single reference time source on a regular basis so that timestamps in logs are consistent.

13.1.3.4 Patch Management

- The TFCI IT team maintains overall responsibility for patch management implementation, operations, and procedures.
- All Information Resources must be scanned on a regular basis to identify missing updates.
- Software updates and configuration changes applied to Information Resources must be tested prior to widespread implementation
- Verification of successful software update deployment will be conducted within a reasonable time period.

13.1.3.5 Penetration Testing

- Penetration testing of the internal network, external network, and hosted applications must be conducted at least annually or after any significant changes to the environment.
- Any exploitable vulnerabilities found during a penetration test will be corrected and re-tested to verify the vulnerability was corrected.

13.1.3.6 Vulnerability Scanning

- Vulnerability scans of the internal and external network must be conducted once in six months or after any significant change to the network.
- Failed vulnerability scan results rated at Critical or High will be remediated and re-scanned until all Critical and High risks are resolved.
- Any evidence of a compromised or exploited Information Resource found during vulnerability scanning must be reported to the CTO and CTO needs to reports the same to the IT Committee.
- Upon identification of new vulnerability issues, configuration standards will be updated accordingly.

13.1.4 Reporting a security incident

Ref. Incident Management Guidelines

13.2 CYBER CRISIS MANAGEMENT PLAN (CCMP)

The purpose of Cyber Crisis Management plan (CCMP) is to establish the strategic framework and guide actions to prepare for, respond to, and begin to coordinate recovery from a cyber incident and to ensure that interruption or manipulations of critical functions/services are brief, infrequent, and manageable and cause least possible damage. It covers different types of cyber crises, possible targets and related impact, actions and responsibilities of concerned stakeholders and coordination of cyber incident response. The objective is to make the organisation Cyber Resilient. Cyber Resilience is defined as ability of organization or business process to

- Anticipate: Maintain a state of informed preparedness in order to forestall compromises of mission/business functions from adversary attacks
- Withstand: Continue essential mission/business functions despite successful execution of an attack by an adversary
- Contain: Localize containment of crisis and isolate trusted systems from untrusted systems to continue essential business operations in the event of cyber attacks
- Recover: Restore mission/business functions to the maximum extent possible subsequent to successful execution of an attack by an adversary
- Evolve: To change missions/business functions and/or the supporting cyber capabilities, so as to minimize adverse impacts from actual or predicted adversary attacks

CCMP will address the following four aspects of Cyber crisis:

- Detection
- Response
- Recovery
- Containment

Detection: Timely detection of cyber incidence is crucial for early recovery and containment. The Cyber Crisis Management Team needs to be trained to respond to

cyber crises. The Employees may be educated in cyber security and IT Team may be trained in handling Cyber incidence.

Response: The response during cyber crisis is critical, coordinated response to incident limits lost time, money and damage to reputation and cost of recovery. The identified team members from Senior Management, Legal, IT, Accounts will coordinate and respond to the situation. All evidence of the incident may be preserved and help from third parties may be taken for analysis. Response to stakeholders may be done by the Competent Authority.

Recovery: Based on the type of incidence, the process of recovery will be initiated.

Containment: The impact of cyber-attack needs to be contained, root cause analysis of the attack needs to be analyzed and the remedial action to be taken for preventing future attacks.

13.2.1 Nature of Cyber Crisis

Cyber attacks can trigger on

- Individual systems
- Multiple systems and networks in a single or multiple organizations
- States and entire Nation

The attack primarily involves but not limited to

- Targeted Scanning, Probing and Reconnaissance of Networks and IT Infrastructure
- Large scale defacement of websites
- Malicious Code attacks (virus/worm/ /Trojans/Botnets)
- Malware affecting Mobile devices
- Large scale SPAM attacks
- Identity Theft Attacks
- Denial of Service(DoS) attacks and Distributed Denial of Service(DDoS) attacks
- Domain Name Server (DNS) attacks
- Application level Attacks
- Cyber Espionage and Advanced Persistent Threats

13.2.2 Cyber Security threat landscape

- Attack Targets
    - Critical infrastructure
    - Business intelligence
    - Personally identifiable information
- Attack Motives
    - Disruption of Services
    - Cyber espionage
    - Financial frauds
- Attack Actors/elements
    - Nation states
    - Cyber criminals
    - Hacker groups
    - Malicious Insiders
- Attack vectors and medium

- Botnets
- Vulnerabilities and Exploit tool kits
- Social engineering
- Ignorant users

13.2.4 Cyber Security Crisis, Possible Targets, and Impacts

- Targeted Scanning and Probing of IT infrastructure
  - Possible Targets
    - Sensitive and Critical Information infrastructure
  - Related Impact
    - Pre-cursor to hacking and focused attack leading to cyber crisis

- Large scale defacement and semantic attacks on websites
  - Possible Targets
    - Web Portals
    - Websites
  - Related Impact
    - Reputation Risk
    - Total/partial disruption of service, monetary loss

- Malicious Code attacks (i.e. Virus, Worm, Trojans, Botnets etc)
  - Possible Targets
    - Database systems
    - Application systems
  - Related Impact
    - Partial or no response from Computer system
    - Total/partial corruption of databases
    - Monetary loss, damage to reputation, loss of image etc.

- Identity Theft Attacks Large scale spoofing
  - Possible Targets
    - Websites
    - Web Portals
  - Related Impact
    - Increased possibility of identity theft leading to penetration into sensitive IT systems and Databases, loss of sensitive data, monetary loss, and loss of image.

- Denial of Service (DoS) attacks and Distributed Denial of Service (DDoS) attacks
  - Possible Targets
    - Network
    - Critical Systems
  - Related Impact
    - Total/partial disruption of services for prolonged periods

13.2.4 Prevention and Precautionary Measures

To minimize occurrence of cyber incidences the following preventive measures shall be followed:

- Implementation of Information Security Policy & implementation of best practices

- Business Continuity Plan (BCP)
- Disaster Recovery Plan (DRP)
- Security of Information infrastructure and network
- Network traffic scanning for malicious traffic
- Isolation of critical networks
- Implementation of Security guidelines issued by concerned authorities
- Background checks of data managers, information systems manager and IT infrastructure managers
- Audit & Assurance involving Information Systems, IT Security, Vulnerability Assessment and Penetration Testing
- Security training & awareness of internal end-users, Information System and Infrastructure managers
- Sharing of information pertaining to incidents with all stakeholders

13.2.5 Incident Response and Mitigation

- Notify incidents to IT Security team & Management
- Monitor and detect anomalous behaviour and degradation of services
- Take all logs of affected systems for forensics analysis
- Notify and share relevant information to CERT-In and RBI
- Implement appropriate eradication process and recovery of systems as prescribed against each type of attack

13.2.6 Crisis management & Emergency response

Crisis management & Emergency response is a set of actions aimed at rapid response & Remedial measures and recovery & restoration of normalcy in the event of a build-up or Emergence of a crisis.

These actions include:

- Containment of crisis
- Communication to all concerned and coordination of efforts that can facilitate adequate & swift response in a timely manner
- Business continuity to maintain availability of minimum essential services / activities in accordance with best practices and industry accepted standards
- Detailed analysis of the crisis event, initiation of appropriate disaster recovery measures and return to normalcy at the earliest
- Learning from the crisis

Crisis management and emergency response involves actions at two levels:

- Actions within the organization: The point of action where the crisis has occurred (as part of due diligence and fulfilment of its business objectives, legal and commercial obligations)
- Actions beyond the organization: The point of coordination between multiple agencies & stake holders

14. INCIDENT MANAGEMENT GUIDELINES

14.1 Introduction

Information Security threats and incidents have become not only numerous and diverse, but also damaging and disruptive. An incident response and management capability is therefore necessary for detecting information security incidents, minimizing loss and damage to information / data, mitigating the weaknesses that

were exploited, and restoring information assets in a timely manner. To that end, this document describes the procedure for incident management, particularly for reporting, response, analysis, investigation and recovery from an information security incident reported/detected within Tourism Finance Corporation of India.

14.2 Responsibility

(a) User Responsibility: An employee should report any observed or suspected deviations from the organization's IT policy, procedures and associated documents, and/or weaknesses to IT team.
Employees shall not attempt to prove any suspected security weakness. Testing weaknesses could cause damage to the information system or service; it would be interpreted as a potential misuse of information system and may result in disciplinary action for the individual performing the testing.

(b) IT Team Responsibility: IT team shall

- Perform Initial diagnosis and categorization of the reported problem / Incident in accordance with the available detail reported /captured/ identified information as per "Problem Report Form", Ref. Annexure III
- In case, problem categorized as Information Security Incident (SI) as mentioned in item no 14.3 (a), (c) and (d) then same shall be referred to the management, IT Committee and Statutory Bodies/ RBI as per the guidelines at 14.2(c).
- Notify respective team members from IRT in a timely manner
- Work closely with departments, vendors etc. to ensure availability of IT Infrastructure as required during the course of problem / incident response, investigation or recovery;
- Wherever required, arrange support of Vendors;
- Ensure that data and information found during investigation is not tampered with, deliberately or unknowingly by anyone during maintenance or other activities; and
- Notify and update the user of status of the problem / incident via email / call.

(c) Guidelines on Reporting of unusual cyber incidents

- Unusual cyber incidents shall be reported to RBI within six hours of detection
- Reporting shall be done on the DAKSH portal
- Queries raised by Cyber Security and IT Risk Group (CSITEG) shall be responded within five working days, unless specific timelines for submitting the inputs sought.
- Root Cause Analysis (RCA) report shall be submitted within 10 working days from the initial detection of the incident where no external audit or forensic investigation is necessitated
- In case of requirement of additional time for submission of RCA, a timeline must be provided to RBI within 10 working days from the date of initial detection of incident.
- On resolution of the incident the status in the DAKSH portal must be updated.
- TFCI mandatorily report any unusual cyber incident at Vendor / Partner / Third-Party Service Providers' (TPSPs') infrastructure which impact its operation within

6 hours of detection.

Cyber Incident types that are required to be reported

a. Unusual Cyber Incidents: This could be, for illustrative purpose, one/ more of the following types of incidents but not necessarily limited to:

- Malware, Ransomware attack;
- Data/ customer information/ business information breach;
- Malicious traffic observed from TFCI's information system to a suspicious IP/ Command & Control terminal (or) any other internal/ external information system;
- Denial of Service (DoS) / Distributed Denial of Service (DDoS) attacks exceeding 30 minutes;
- Exploitation of vulnerabilities resulting into compromise of integrity of the system/ application. (e.g., Parameter manipulation/man-in-the-middle type of incidents)
- Email phishing, spoofing attacks leading to execution of fraudulent transactions
- Website defacement
- Any other type of cyber incident not necessarily falling into one of the above

b. A major near-miss cyber-attack with the potential to escalate into an unusual cyber incident, as per TFCI's risk assessment.

Reporting Authority: The incidents should be reported by the CTO/CISO, or any other competent authority(ies) designated for this purpose by TFCI.

14.3 Definitions

(a) **Incident** is something that needs to be resolved immediately. This can either be through a permanent fix, a workaround or a temporary fix. If an incident requires changes the emergency change process is normally followed, especially if the service level is critical. An incident is where an error occurs. i.e. something doesn't work the way it is expected and causes a disruption/outage in the business process. In nutshell, an incident is an event that disrupts normal operation.

(b) **Problems** are not incidents. A problem may or may not raise an incident, A problem may be raised because of an incident and a problem may cause one or more incident. The root cause of the problem may be known or not known. Some examples of problem are as follows:

- the occurrence of the same incident many times
- an incident that affects many users
- the result of network diagnostics revealing that some systems are not operating in the expected way
- Server crash after business hours & does not disrupt the business

In any case, the following actions may be taken for problems:

- Do nothing - if the problem does not affect the business, or if the cost of fixing the problem exceeds its benefits
- Deploy work around if the determination of root cause exceeds the benefits.
- Determine root cause and fix the problem if the benefit is worth it.
- Categorized the problem as Information Security Incident

(c) Incident management is a process designed to return services to normal as quickly as possible after an incident, in a way that has little to no negative impact on the business. In practice, incident management often relies upon temporary workarounds to ensure services are up and running while the incident is investigated, the root problem identified and a permanent fix put in place. In this context, an incident is an event that disrupts normal operation. A problem is an underlying issue that could lead to an incident;

- An incident is an unplanned disruption or degradation of service.
- A problem is a cause of one or more incidents.

(d) Information Security Incident is defined as the act of (or the threat of) occurrence of non-compliance with the Tourism Finance Corporation of India ltd. Information Technology guidelines, procedure, or a core security requirement that may result in:

- Loss of confidentiality of information assets;
- Compromise of integrity of information assets;
- Denial of service;
- Misuse of service, systems or information assets; and
- Damage to information assets.

Some examples of Information Security incidents are, but not limited to:

- Successful unauthorized access, use, disclosure, modification or destruction of information;
- Interference with information technology operation;
- Violation of explicit or implied acceptable usage;
- Unauthorized usage/disclosure of information;
- Compromised user account;
- Loss or theft of information assets;
- Unwanted service disruption or Successful denial of service attack;
- Changes to information assets without the asset owner's knowledge, consent, or instruction;
- Accidental mis-categorization of information that releases it inappropriately; and
- Copyright infringement.

14.3.4.1 Categories of Information Security Incident, but not limited to:

1. Outage of Critical IT system(s) : Like. LMS, GFA, ALM, etc.
2. Cyber Security Incident (s) (if Successful) : Like DOS, Ransom ware/crypto ware, data breach, data destruction, web defacement, etc
3. Theft or Loss of Information : Like sensitive customer or business information stolen or missing or destroyed or corrupted
4. Outage of Infrastructure: In DC / Central Processing Units, HO, branch, etc. in regard to power / utilities supply, telecommunications supply
5. Others : e.g. outsourced service providers, business partners, breach of IT Act / any other law and RBI/SEBI regulations. etc.

14.3.5 Incident Response Team (IRT) is a team responsible for responding to a security incident reported or detected in the organization. IRT's role is to provide prompt and correct response to an information security incident, so that the incident can be

contained, investigated and recovered in a timely manner thereby reducing loss to the organization.

Team Member	In-house Applications	Third Party Applications
IT support Executive / AM	L1	L1
Manager / AVP	L2	L2
DVP / VP / CTO	L3	L2 , L3
Vendor (Application Software/Hardware/ Both)		L2, L3

14.3.6 Turn Around Time (TAT) : TAT cannot be defined in vendor dependent cases and will be governed as per the signed agreement/contract with the related vendor. TFCI's current operation timing is 9:30 AM to 5:30 PM Monday to Friday excluding TFCI declared holidays, hence incident/ticket received after 4:30 PM will be considered for next working day.

14.4 Procedure/Guidelines Applicability

This procedure is applicable to all information security problems /incidents reported / detected by employees of TFCI as well as vendors associated with TFCI who are using TFCI information facilities.

14.5 Problem Handling

14.5.1 Entry Criteria

- Problem is reported by the user/ Self-identified by IT team/ Vendor; and

14.5.2 Problem Management Process Narration

- It is the responsibility of the user to raise the ticket or IT team may also create a problem ticket and assign a unique identifiable number to the ticket for the users to track the problem;
- The IT team shall categorize the problem as per the detailed reported /captured/ identified as mentioned in Annexure III "PROBLEM REPORT FORM"
- If problem reported calorized as Incident than Item no 14.5.3 & Item no 14.6 will be invoked
- The IT team shall check whether the problem is a known error and can be resolved, the IT team shall provide the resolution and close the process;
- The IT team shall perform the investigation and diagnosis of the problem and validate if a solution can be achieved;
- In cases where a solution is not available, the team shall provide a workaround and escalate the problem to the vendor (as applicable);
- In cases where a solution has been identified, it is the responsibility of the IT team to check if the resolution requires a change to be undertaken to fix the problem;
- If a change is required to resolve the problem, the change management procedure shall be followed and the ticket be closed;
- If a change is not required, as part of the problem resolution the IT team shall obtain approvals as specified in the project plan and implement the problem resolution;
- Upon providing the resolution, the IT team shall perform a root cause analysis to determine what triggered the problem and what preventive measures can be adopted;
- Once the problem has been analysed and evidence has been collected, IT team shall notify the respective stakeholders within the organization;

- Once the incident has been resolved or contained, eradication of incident components shall be done by IT team (solely or jointly with relevant stakeholder(s) for e.g., product/service vendor or application developer) to contain the incident;

14.5.3 Exit Criteria

- Problem categorized as Information Security incident or problem is resolved

14.6 Incident Handling

14.6.1 Entry Criteria

- Information Security Incident is reported; and
- Information Security Incident is detected;

14.6.2 Incident / Problem Priority Matrix

Business Impact		Urgency (U)	Ticket rating
Damage Scale (D)	Customer Service (C)		
Significant damage, fraud, or loss (compromise) of confidential, strategic and/ or critical customer information or result in liability to the organization and to its public image	Total loss of production service to entire customer (both internal and external) set	Critical	Emergency
Damage, corruption, or loss of information without compromise OR may have a moderate financial impact on the organization / or its normal functioning	Potential critical loss of production service to a partial customer (both internal and external) set	High	High
Causes inconvenience, aggravation, and/or minor costs associated with recovery and the event will have moderate to minor financial impact on the organization	Minor loss of production service OR degrades customer (both internal and external) service but do not prevent delivery of service	Medium	Medium
No considerable damage in organization normal functioning	Customer service unaffected	Low	Low

14.6.3 Incident Escalation

Priority	Time Limit before Escalation	
3 - Low	3 Working days	IT Department
2 - Medium	2 Working Days	IT Department
3 - High	1 Working Day	IT Department

14.6.4 Incident Handling - IRT

- On receiving notification about the incident, IRT will perform initial diagnosis and provide preliminary support, if possible to contain the incident;
- IRT shall perform an impact analysis to determine the impact of the information security incident on the business processes and users;
- IRT shall undertake investigation and diagnosis of the information security incident and shall send out an incident alert to users and relevant Departments who could be possibly impacted by the incident. The incident alert shall contain incident symptoms and actions to be taken by the user (if any);
- If the incident involves proprietary software or hardware, IRT shall contact the product vendor for support and work jointly to resolve the issue;
- IRT shall work towards providing resolution and support to resolve the incident;
- IRT shall collect and maintain relevant evidence, associated with the incident
- Upon providing the resolution IRT shall perform a root cause analysis to determine what triggered the incident and what preventive measures to be adopted going further;
- Once the incident has been analysed and supported evidence has been collected, IRT shall notify the stakeholders within the organization. In cases where notification of the incident is vital for the continuity of business, IRT may inform the stakeholders at any time during incident-handling;
- Once the incident has been resolved or contained, eradication of the incident components shall be done by IRT (solely or jointly with relevant stakeholder(s) for e.g., product/service vendor or application developer) to contain the incident;
- IRT shall suggest through appropriate communication mechanisms (such as system notifications, e-mails or oral warnings) to the relevant stakeholders, methodologies for recovering from the incident. Such methodologies shall include restoring systems to their normal operations, cleaning up of residual incident components and suggestions for strengthening the systems;
- As part of post-incident analysis and activities, IRT shall analyse incident reports and determine corrective and preventive actions to prevent similar incidents in future.

15 CUSTOMER DATA PRIVACY GUIDELINES

TFCI recognizes that one of its fundamental responsibilities is to ensure that the TFCI protects personal information entrusted to the TFCI by its customers. This is critical for the maintenance of the TFCI's reputation and for complying with its legal and regulatory obligations to protect the TFCI's customer information. TFCI also follows a transparent guideline to handle personal information of its customers.

In these guidelines, personal information/information means any information that relates to a natural person/corporate, which either directly or indirectly, in combination with other information available or likely to be available with the TFCI, is capable of identifying such person (e.g., telephone number, name, address, transaction history etc.).

These Guidelines are in compliance with the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011 (the "IT Rules") contained in the Information Technology Act 2000.

15.1 Objective The purpose of these guidelines is to maintain the Customer Data privacy of and protect the personal information of customers of TFCI and ensure compliance with laws and regulations applicable.

15.2 Scope & Applicability TFCI collects three types of information: personal, sensitive personal data and non- personal data.

These guidelines are applicable to personal data & information (including sensitive personal data & information) collected by TFCI directly from the customer or through TFCI's online portals, electronic communications as also any information collected by TFCI's server from the customer's browser or through mobile application.

These guidelines are applicable to all TFCI employees, auditors, contractors, vendors, interns, associates, customers and business partners who receive personal information from TFCI, who have access to personal information collected or processed by TFCI, or who provide information to TFCI, regardless of geographic location. All employees of TFCI are expected to support the privacy guidelines and principles when they collect and / or handle personal information or are involved in the process of maintaining or disposing of personal information. These guidelines provide information to successfully meet the organization's commitment towards customer data privacy.

All Subsidiary firms and any Third-Party working with or for TFCI, and who have or may have access to personal information, will be expected to have read, understand and comply with these guidelines. No Third Party may access personal information held by the organization without having first entered into a confidentiality agreement/Non-Disclosure Agreement (NDA).

15.3 Definition

15.3.1 Data Subject A data subject who is the subject of personal, sensitive personal data and non- personal information

15.3.2 Personal data means any information that relates to a natural person/corporate (the data subject), which either directly or indirectly, in combination with other information available or likely to be available with TFCI, is capable of identifying such person / corporate (e.g., telephone number, name, address, transaction history etc.).

15.3.3 Personally Identifiable Information PII is any information about an individual/corporate (the data subject) which can be used to distinguish or trace an individual's/corporate identity; any other information that is linked or linkable to an individual/corporate. Examples included but not limited to: Name, Address, Date of birth, DIN, PAN, etc.

15.3.4 Sensitive Personal Information (SPI) Sensitive personal information means personal/corporate data (the data subject) consisting of information but not limited to the following attributes of the data subject:

- password;
- financial information such as bank account or other payment instrument details ;
- physical, physiological and mental health condition;
- sexual orientation;
- medical records and history;
- genetic or biometric information;
- racial and ethical origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership & other membership;
- any detail relating to the above clauses as provided to body corporate for providing service; and
- any of the information received under above clauses by body

corporate for processing, stored or processed under lawful contract or otherwise:

Provided that any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

15.3.5 Non-personal Data: Non-personal information includes the IP address of the device used to connect to TFCI's network, TFCI's VPN, TFCI's website or any other TFCI application/ infra/database along with other information such as browser details, operating system used, the name of the website/application that redirected the visitor to TFCI's website, etc. Also, when user browse TFCI site or receive one of TFCI emails, TFCI and our affiliated companies use cookies and/or pixel tags to collect information and store the online preferences.

15.3.6 Third Party All external parties including contractors, interns, summer trainees, vendors, auditors, and business partners, etc. or who has access to TFCI information assets or information systems.

15.4 Purpose of collection and Usage of Personal Information TFCI shall use the information collected to manage its business and offer an enhanced, personalized online/offline experience or experience on its website/mobile application. Further, it shall enable TFCI to:

1. Process applications, requests and transactions
2. Maintain internal records as per regulatory guidelines
3. Provide services to customers, including responding to customer requests
4. Comply with all applicable laws and regulations
5. Recognize the customer when he Connect online or offline or to conducts online transaction
6. Understand the needs and provide relevant products and service offers

If a customer does not wish to provide consent for usage of its sensitive personal data or information or later withdraws the consent, TFCI shall have the right not to provide services or to withdraw the services for which the information was sought from the customer.

15.5 Disclosure/ Sharing of Information

TFCI shall not disclose personal information of its customers without their prior consent unless such disclosure has been agreed to in a contract between the body corporate and customer, or where the disclosure is necessary for compliance of a legal obligation. In- case TFCI discloses the personal information to Third Parties, such Third Parties shall be bound contractually to ensure that they protect customer personal information in accordance with applicable laws.

The above obligations relating to sharing of personal data or information shall not apply to information shared with the government, mandated under the law to obtain such information or by an order under law for the time being in force. Further, if any personal data or information is freely available or accessible in the public domain, TFCI shall not have any obligations regarding the same.

No specific information about customer accounts or other personally identifiable data shall be shared with third parties unless any of the following conditions is met:

1. To help complete a transaction initiated by the customer
2. To perform support services through an outsourced entity provided it conforms to the Privacy Guidelines of TFCI

3. The customer/ applicant has specifically authorized it
4. To conform to legal requirements or comply with legal process
5. The information is shared with Government agencies mandated under law
6. The information is shared with any third party by an order under the law
7. Enforce the terms and conditions of the products or services
8. Act to protect the rights, interests or property of TFCI, or its members, constituents or of other person
9. Entered into a confidentiality agreement/Non-Disclosure Agreement (NDA).

15.6 Data Protection and Security

The security of personal information is a priority and shall be ensured by maintaining physical, electronic, and procedural safeguards that meet applicable laws to protect DATA SET information against loss, misuse, damage and unauthorized access, modifications or disclosures.

Anyone collecting personal and customer information must fairly and lawfully process it, process it only for limited, specifically stated purposes, use the information in a way that is adequate, relevant and not excessive, use the information accurately, keep the information on file no longer than absolutely necessary, process the information in accordance with the legal rights, and keep the information secure.

TFCI shall continuously review and enhance its security policies and security measures to consistently maintain a high level of security.

Annexure II

CHANGES IN IT POLICY FOR 2025-26 VIS-À-VIS PREVIOUS YEAR

Modification Item Refence	IT Policy FY 2024-25	IT Policy FY 2025-26
9. DR Guidelines (Page. 12)	• Recovery Point Objective(s) (RPO), RPO = 24 hours • Recovery Time Objective(s) (RTO), RTO = 34 hour	• Recovery Point Objective(s) (RPO), RPO = 15 minutes • Recovery Time Objective(s) (RTO), RTO = 1 hour Further, Recovery Time will be considered from the time it has been declared as disaster by the competent authority.

***