YES CAPITAL (INDIA) PVT LTD

DEPARTMENT NAME: INFORMATION TECHNOLOGY

POLICY: IT POLICY

Version: YCPL/FY2018-19/APR/INFORMATION TECHNOLOGY/ IT POLICY/VERSION 1.0

Effective date: 01/July/2018

INFORMATION TECHNOLOGY POLICY

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

Objective of IT Policy

- To provide IT infrastructure services and support to facilitate innovative use of technology for better decision making and for providing better service to the clients.
- Integrate IT into business operations in line with the business objectives of the organisation
- Explore and assess new and emerging technologies.
- Provide infrastructure to TFCI's users which is secure, personalised and timely access to information, services and support anytime anywhere.
- Provide users with the training, support, tools and information needed to foster innovative and effective use of technology.

IT Strategy Committee

In order to carry out review and amend the IT strategies in line with corporate strategies, Board Policy reviews, cyber security arrangements and any other matter related to IT Governance, an IT Strategy Committee is to be constituted comprising of an all Director of the company and any one as Chairman and IT head as member.

The IT Strategy Committee is required to meet at frequent interval but not later than six months. In line with the above, YCPL proposes to constitute IT Strategy Committee of comprising

- Raakhe Kapoor Tandon
- Radha Kapoor Khanna
- Roshini Kapoor

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

- Approve IT strategy and policy documents and ensuring that the management has put an effective strategic planning process in place.
- Ascertaining that management has implemented processes and practices that ensure that the IT delivers value to the business.
- Ensuring IT investments represents a balance of risks and benefits and that budgets are acceptable.
- Monitoring the method and management uses to determine the IT resources needed to achieve strategic goals and provide high-level direction for sources and use of IT resources.
- Ensuring Proper balance of IT investments for sustaining NBFC's growth and balancing aware about exposure towards It risks and controls.

IT ASSET MANAGEMENT POLICY

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

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

All IT assets of the YCPL must be

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

IT SECURITY POLICY

IT security is created under the following security heads:-

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

Physical Security

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

Security at the Network Gateway

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

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

Security against Viruses/Spyware

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

Security built into Application Systems

- Application systems shall have security features like:

- User Ids
- Passwords
- Access Permissions
- Login History
- User Account Log
- Audit trails
- System Modification Controls
- System Documentation

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

Application Systems Security Policy

1. **Users and Logins**
   All oracle applications will be accessed through a single entry point.

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

3. **System Administrator**

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

♣ Creation/Dropping of users (usernames).
♣ Activation / Deactivation of users. ♣ Granting / Revoking of Application Administrator privilege.
♣ Unlocking locked user accounts.
♣ Setting / Changing system parameters.
♣ All application administrator privileges. DGM (Accounts) is proposed to be designated as System Administrator of YCPL.

4. **Application Administrator**

System Administrator along with an officer from user department would be designated to act as Application Administrators. These designated officers would be provided with all the Application Administrator privileges. The responsibilities / privileges of an application administrator should include:
♣ Granting / Revoking access to the application system.
♣ Deciding Access level of the users.
♣ Deciding the users' reporting user / officer.
♣ Granting / Revoking Menu / Form level access privileges.
♣ Granting / Revoking of Application Administrator privilege.

5. **Application user.**

• An employee with a valid username and password and having access to any application system will be an application user for that application.
• There must exist a record with status as regular and valid office code in the employee directory of the payroll system.
• Whenever the system detects a mismatch between the office code of the user in the employee directory of the payroll system and office code as per security module, the user account should automatically get deactivated.
• Application user, on successful log in, should only be allowed access to the systems for which he has been granted permissions.
• The application user should not be allowed to have multiple logins.
• As soon as a user ceases to be an employee of YCPL, his/her user account should be de-activated immediately and he should not be able to access any of the application systems.
• Users should be able to lock their login account for any number of days. During the locking period the user accounts can not be accessed. User will be allowed to login to the system after the expiry of locking period. However, System administrator can unlock the accounts, if required.
• Maximum three login attempts should be allowed at a time. After three unsuccessful attempts login screen should be closed.
• The system should have the provision to lock the user account for those users making continuous attempts for a specified number of times (captured as system parameter) with invalid passwords.

6. **Access levels (Application System/Form/Menu)**

The following should be the broad access levels:

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

7. **Unsuccessful login attempts**

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

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.

9. **Application-wise login history**

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

10. **Password History**

The system should preserve all old passwords.

11. **User Account Log**

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

- ♣ Creation of user id.
- ♣ Dropping of user id.
- ♣ Deactivation of user id.
- ♣ Reactivation of user id.
- ♣ Locking of user id.
- ♣ Unlocking of user id. Granting system administrator privilege.
- ♣ Revoking system administrator privilege.
- ♣ Granting application administrator privilege.
- ♣ Revoking application administrator privilege.
- ♣ Changes in user profile in terms of : -Reporting officer -Access level -Department -Changes in user access to forms/reports/menu/sub-menu.

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

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 also provide for generation of Audit Trail Reports.
- The Audit Trail Reports for the Systems like Financial Accounting, Loan Accounting and Payroll would be generated every month and would be perused by the user in-charge (Application Administrator) of the respective systems. These reports would be stored at least for one year till the annual audit of the office is complete.
- Audit trail data of all the Systems would remain on line for a minimum period of at least 400 days i.e. till the annual audit has been completed.

13. Application Systems Modification

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

Backup Policy

1. Scope

The scope of the backup covers the need and rules for performing periodic backup of Servers so that data or information can be retrieved timely in the case of system malfunction, accidental deletion, intentional destruction or natural disaster, etc.
The backup procedure covers the complete backup of user's data on file servers, application and database on-premises / hosted applications.
Frequency of backup:-

- A full systems backup on monthly basis.
- A full systems backup on yearly basis.

2. Backup Retention

Type of Backup	Retention Period	Remarks
Monthly Backup	Yearly	The monthly backup is maintained on NAS Storage which is a complete backup till last day of the Month
Yearly Backup	Permanent	The data is stored Year-wise in the NAS Storage.
Specific Event Backup	As per the Business requirement	Based on the specific request from business with prior approval from respective HOD.

3. Backup Media Testing

a. The data is stored in raw format on the NAS Storage which is randomly checked for the file data integrity. This helps in resolving the following:

-To check for and correct errors.
-To monitor duration of the backup job.
-To optimize backup performance.

b. The data resides in raw format in the NAS Storage which is tested in quarterly basis.

4. Restoration Procedure

Users that need files restored must submit a request to the IT Support with information about the requested data. IT Support will provide the resorted data to the user and close the call after confirmation.

Change Management Policy

1. Introduction

Change Management policy establishes the requirements for change to be managed and auditable, and to ensure business continuity. These constitute the base requirements for change management and are not intended to define procedures or processes, but instead, provide the framework on which procedures and processes can be based.

The purpose of this policy is to create a central repository of all the changes made to IT systems supported by YCPL so that the department can have a global view of everything that is changing on the systems it manages and can use this information if problems occur to assist in tracking the issue back to a change that was made. Its purpose is also to ensure changes are communicated to customers both internal and external prior to implementation to give them a chance to have input into the schedule and scope of the change

2. Categories of Changes

There are three categories of changes:

2.1 Major Change: Change to production system that have major impact or extensive outage to the Users ability to conduct their operations.

2.2 Minor Change: Change to production system that have minor to no impact, or outage to the Users ability to conduct their operations.

2.3 Emergency Change: Change submitted in response to a problem or outage of a system. These are unplanned in nature and are submitted in response to emergencies that cause a change to happen immediately or in a shortened time frame.

3. Objectives

This Change Management Policy provides statements and definitions that are intended to enhance the continuity, stability, and reliability of business operations. Change Management Policy for any changes to an environment or system that could affect continuous business operations.

The objectives of this Change Management Policy are to:

a. Encourage advanced planning, coordination, and communication of changes.
b. Consider the consequences of an unsuccessful change, and plan for recovery, prior to implementation.
c. Communicate the change to all affected users.
d. Establish a central point and repository to coordinate changes.
e. Identify the potential impact of changes on other systems and environments.
f. Minimize the number of problems and/or conflicts that are caused by changes.
g. Review the change management process for continuous process improvement.

4. Policy Statements

In change management Information Technology has six primary components: a request, an approval, coordination, notification, implementation, and closure. These primary components establish a structure upon which policies can be founded.

4.1 Change Requests

Change Requests must be filed for changes that meet the definition of Change contained in this policy document, All Change Requests must contain the necessary information to properly describe and document the change. All requests must be submitted using the standard format.

a. All change requests must be submitted to the standard format, each change request will be associated with a category; major, minor, or emergency.

b. All Change Requests should contain the necessary information to back out a change and recover from a failed implementation.

c. All Change Requests must be traceable and auditable.

4.2 Change Approval

a. Change Requests should be approved before implementation can occur. They are approved by the HOD/Manager of the section responsible for the change.
b. If circumstances require that a change must be made immediately to satisfy an urgent requirement such as an outage/problem or a security fix, a Change Request may be filed after implementation.

4.3 Change Coordination

a. All YCPL Managers are responsible for reviewing the changes and all distributed change notices to ensure that there are no conflicts. If a Manager believes there is a possibility of conflict, that Manager should contact the Manager responsible for the section making the conflicting change and work out a schedule that will mitigate any problems.

4.4 Change Notification

a. All approved Change Requests must be formally communicated to individuals or groups that will be affected. They must be communicated using the standard format.

4.5 Change Implementation

a. All changes should occur within their scheduled change time. Significant deviations from approved Change Requests (e.g., scope of work completed, timeframe, implementer, etc.) should be recorded in standard format.

4.6 Change Closure

- The disposition of all changes must be documented. Any deviations from the approved Change Request must be documented.

Incident Management Policy

1. Introduction

The purpose of this Policy is to ensure that information security events and weaknesses associated with information systems and hard copy documentation are communicated in a way that allows timely, corrective action to be taken,

2. Policy Statement

The purpose of this Policy is to ensure that any incidents that affect the daily operations are managed through an established process. All Users have an important part to play in reporting and managing information security incidents in order to mitigate the consequences and reduce the risk of future breaches of security. This Policy provides a framework for reporting and managing:

a. Security incidents affecting the YCPL Systems
b. Losses of information
c. Near misses and information security concerns

3. Scope

This Policy applies to all Users (full-time and part-time employees, temporary employees, agency workers, contractors and consultants and third parties) working for YCPL.

4. Security Incidents and Weaknesses

An Information Security Incident can be described as an event that results in:

a. The disclosure of confidential information to an unauthorized individual.
b. The integrity of a system or information being put at risk.
c. The availability of a system or information being put at risk.

5. Security events and Weaknesses to Report

Security events and weakness that must be reported include:

a. Theft or loss of equipment, data or information (including removable media).
b. Breaches of physical security arrangements.
c. Computer infected by a virus or other malware.
d. Receiving unsolicited mail of an offensive nature or requesting personal data.
e. Unauthorized disclosure of information including information being faxed, emailed, posted or handed to an unintended recipient.
f. System malfunctions which may compromise security.
g. Inadequate disposal of confidential material.
h. Writing down passwords and leaving them on display or somewhere easy to find.
i. Non-compliance with policies or guidelines.
j. Accessing an individual's record inappropriately.

k. Receiving and forwarding chain letters - including virus warnings, scam warnings and other emails which encourage the recipient to forward into others.
l. Accessing a computer database using another User's credentials (User ID and password), either with or without their authorization.

6. IT Policy

a. The IT & YCPL Team review all incidents reported to it and advice on any further action required.
b. YCPL will action any lessons learned from reported incidents/weaknesses to prevent future incidents, this will be recorded within their minutes.
c. Where necessary, as part of the review of reported incidents/weaknesses YCPL may re-classify the event?

7. Users (Employees)

a. Users must report any security event or weakness at the earliest opportunity to the IT Support Desk.
b. All Users must cooperate fully to IT Support Team during any investigation. Users may be interviewed as part of this process.

Application Management Policy

1. Purpose

This policy establishes the Application Maintenance, for managing risks from Application maintenance and Control through respective policies.

2. Scope

The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by YCPL. Any information, not specifically identified as the property of other parties, that is transmitted or stored on YCPL IT resources (including e- mail, messages and files) is the property of YCPL. All users YCPL (employees, contractors, vendors or others) of IT resources are responsible for adhering to this policy.

3. Intent

The YCPL Application Maintenance policy serves to be consistent with best practices associated with organizational management. It is the intention of this policy to establish an Application maintenance capability throughout YCPL and its business units to help the organization implement Application best practices with regard to enterprise system maintenance and repairs.

4. Policy

Business System is then bound to this policy, and must develop or adhere to a program plan which demonstrates compliance with the policy related the standards documented.

1. **System Maintenance Policy and Procedures**: All YCPL business Systems must develop, adopt or adhere to a formal, documented system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
2. **Controlled Maintenance:** All YCPL Business Systems must Schedule, perform, document, and review records of maintenance and repairs on information asset components in accordance with manufacturer or vendor specifications and/or organizational requirements.
    a. Control all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location.
    b. Requires that a designated official explicitly approve the removal of the information asset or system components from organizational facilities for off-site maintenance or repairs.
    c. Sanitize equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs.
    d. Check all potentially impacted security controls to verify that the controls are still functioning.

3. **Maintenance Tools:** All YCPL Business Systems must approve, control, and monitor the use of information asset maintenance tools.
4. **Non-Local Maintenance:** All YCPL Business Systems must:
    a. Authorize, monitor, and control non-local maintenance and diagnostic activities.
    b. Allow the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information asset.
    c. Employee strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions.
    d. Maintain records for non-local maintenance and diagnostic activities.
    e. Terminate all sessions and network connections when non-local maintenance is completed.

5. **Maintenance Personnel:** All YCPL Business Systems must establish a process for maintenance personnel authorization and maintain a current list of authorized maintenance organizations or personnel. In addition, YCPL Business Systems must ensure that personnel performing maintenance on the information asset have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information asset maintenance when maintenance personnel do not possess the required access authorizations.

6. **Timely Maintenance:** All YCPL Business Systems must obtain maintenance support and/or spare parts for information systems/assets within defined service level agreements.

7. **Applications Use:**
    a. Microsoft Office 365
    b. Tally
    c. Adobe Reader
    d. Java Runtime
    e. Internet Browsers – IE, Chrome, Mozilla, Safari
    f. Antivirus Software
    g. HRMS

Server Security Policy

1. Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/ or operated by YCPL. Effective implementation of this policy will minimize unauthorized access to YCPL proprietary information and technology.

2. Scope

This policy applies to server equipment owned operated by YCPL and to servers registered under any YES Capital (India) Pvt Ltd owned Internal network domain. This policy is specifically for equipment on the internal YCPL network and to ensure secure configuration of equipment external to YES Capital (India) Pvt Ltd.

3. Policy

3.1 Ownership and Responsibilities

All internal servers deployed at YCPL must be owned by the IT department and it is solely responsible for System/Server administration. Approved server configuration guidelines must be established and maintained by each operational group, based on business needs and approved by management. The IT department should monitor configuration compliance and implement an exception policy specifically tailored for YCPLs environment. Additionally, IT department must establish a process for changing configuration guide which includes review and timely approval by management.

Servers must be registered accordingly to server security policy. At a minimum, the following information is required to positively identify the point of contact.

- Hardware and operating System/Version
- Main function and applications, if applicable
- Information in the corporate standard management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures.

3.2 General Configuration Guidelines

- Operating system configuration should be in accordance with approved IT department guidelines.

- Services and applications not in use must be disabled.
- Access to servers should be logged and/ or protected through access-control methods.
- The latest security patches must be installed on the system as soon as, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will suffice.
- Always use standard security principles of least required access to perform a function.
- If methodology for secure channel connection is available (i.e. technically feasible), privileged access must be performed over secure channels, (e.g. encrypted network connections using SSH or IPsec.
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from being operated from uncontrolled cubicle areas.

4. Monitoring

All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

- All security related logs will be kept online for a minimum of 1 month.
- Monthly Backups will be retained for a minimum of Six Months.
- Yearly Backup will be retained for minimum of 2 years.

Security related events will be reported to the IT Department who will review logs and report incidents to management. Corrective measure will be prescribed as needed. Security related events include but are not limited to-

5. Executive owner

The responsibility for implementing and executing the procedures applicable to this policy are:
IT Department - To monitor its effectiveness
Line Management - To monitor and ensure that team members adhere to this policy.

Network Security Policy

1. Introduction

The purpose of this policy is to establish guidelines for the use and access of YCPL Network infrastructure to preserve the security, integrity, availability and confidentiality of all information pertaining to YCPL.

2. Purpose

The purpose of this policy is to ensure the security, integrity and availability of Data and Communications Network to establish professional good working practices and procedures.

3. Scope

The scope of this policy extends to all administration, installation and configuration of the YCPL Data and Communications Network equipment and associated systems which form part of the business IT infrastructure and which falls under the responsibility of the Network Support team.

4. Policy Statement

YCPL Network equipment is maintained and installed across Data Center by YCPL IT team at HO. The Data Centre houses most of the Data and Communications Network equipment and serves as the main access area to the YCPL Infrastructure

To secure the data and communications network, the YCPL IT team must ensure:

a. All Data and Communications Network environment are issued with an authorized IT person and signed in/out using the correct procedures.
b. Any Data and Communications Network environment area must be accompanied at all times.
c. Access tags should only be used by the registered user and must not be lent out or given to other staff,
d. Personal, special access visits from relatives or acquaintances of personnel are not permitted within the secure areas. There must be a valid reason for all visits and any such visitors must go through the standard signing in/out

5. Configuration and Maintenance

The following must be considered in order to protect the security, integrity and reputation of YCPL

a. All Data and Communications Network devices must be installed and maintained according to the manufacturer's guidelines in-line with all relevant
b. All Data and Communications Network hardware and software should be purchased/obtained using approved vendors
c. Adequate levels of staffing should be provided at all times - particularly for call-out purposes or systems requiring out-of-hours support
d. Firmware updates/upgrades to Data and Communications Network hardware must only be

undertaken if there is an identified requirement or need to do so in line with the documented maintenance procedures.

e. Any visitors, contractors or vendors carrying out hardware/software installations and/or maintenance are not left unattended while Access within the building should also be limited to areas where the work is to be carried out.
f. Data and Communications Network devices must be located in physically secure areas (locked communications rooms or cabinets) to protect against unauthorized access, removal, disconnection, interference and/or damage.
g. All routing protocol exchanges must be authorized and verified.
h. Data cables should be individually identifiable through the application of a labelling scheme to ensure cables are not removed or re-patched in error.
i. Standardized cable colors should be used where practical to differentiate between cables carrying DC data and cables carrying partner data or external (service provider) connections.
j. Configuration details and any other potentially sensitive information relating to network management must not be circulated to any party outside the Network.
k. Redundancy procedures must be in place and tested for effectiveness on a regular basis. Procedural documentation must be regularly updated to include any changes or updates.
l. Network Management procedures must be in place for the administration of all critical network functions including firewall maintenance, Intrusion Detection System management and maintenance of Internet activity logs.

6. Monitoring and Event Logging

a. Network events which include the following, must be logged and recorded to a centrally secured location:
    - Security events
    - Network device access
    - Systems warnings errors or critical alerts
    - CPU and memory threshold alerts
    - Routing change events
    - Network topology changes

b. Logging events to individual network devices must be disabled
c. Log files must be routinely analyzed to ensure anomalies, failures, unexpected changes or any other significant events are reported under the YCPL IT team
d. All network device clocks must be synchronized with a central time source.
e. Network traffic profiles must be monitored and analyzed for capacity management and anomaly detection.

7. Backup Process (Switches/Firewall)

a. All network devices has to back up every Month
b. All firewall changes to be documented with proper approvals and stored for further references.
c. Firmware/OS upgrade to be conducted quarterly depending on the criticality mentioned in the revenue article published by OEM.
d. No default login to be used.
e. Password of all network device including Wi-Fi router to change every 30 days.

Remote Access Policy

Overview

Remote access to our corporate network is essential to maintain our Team's productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our corporate network. While these remote networks are beyond the control of, we must mitigate these external risks the best of our ability.

2. Purpose

The purpose of this policy is to define rules and requirements for connecting to YCPL network from any host. These rules and requirements are designed to minimize the potential exposure to YCPL from damages which may result from unauthorized use of YCPL resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical YCPL internal systems, and fines or other financial liabilities incurred as a result of those losses.

3. Scope

This policy applies to all YCPL employees, contractors, vendors and agents with an YCPL owned or personally-owned computer or workstation used to connect to the YCPL network. This policy applies to remote access connections used to do work on behalf of YCPL, including reading or sending email and viewing intranet web resources. This policy covers any and all technical implementations of remote access used to connect to YCPL networks.

4. Policy

It is the responsibility of YCPL employees, contractors, vendors and agents with remote access privileges to YCPL's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to YCPL.

General access to the Internet for recreational use through the YCPL network is strictly limited to YCPL employees, contractors, vendors and agents (hereafter referred to as "Authorized Users"). When accessing the YCPL network from a personal computer, Authorized Users are responsible for preventing access to any YCPL computer resources or data by non-Authorized Users. Performance of illegal activities through the YCPL network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access

5. Requirements

a. Secure remote access must be strictly controlled with encryption.
b. Authorized Users shall protect their login and password, even from family members.

c. While using YCPL owned computer to remotely connect to YCPL's corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or third Party.

d. Use of external resources to conduct YCPL business must be approved in advance by YCPL and the appropriate business unit manager.

e. All hosts that are connected to YCPL internal networks via remote access technologies must use the most up-to-date anti-virus software this includes personal computers. Third party connections must comply with requirements as stated in the Third Party Agreement.

f. Personal equipment used to connect to YCPL's networks must meet the requirements of YCPL owned equipment for remote access as stated in the Hardware and Software Configuration Standards for Remote Access to YCPL Networks.

Anti-Virus Policy

1. Purpose

To establish requirement which should be met by all computers connected to YCPL, computing resources and data against intrusion by virus and malwares including worms, Trojans, Adware and Spyware. This policy is intended to ensure effective virus detection and prevention.

2. Scope

This policy applies to all computers including, but not limited to, desktop workstations, laptops, handheld devices and serves that are connected to YCPL network via standard network connection, wireless connection and remote connection.

3. Policy

3.1 YCPL has standardized "SEQRITE" to secure its data network against virus and malwares.

3.2 All computers attached to YCPL network must have standard anti-virus software installed. The software must be active, automated to perform virus checks at regular intervals daily with a full disk scan once every week and have its virus definitions files kept up- to date. Team members are not authorized to de-activate, disable or uninstall antivirus software.

3.3 In addition to the above clauses, Internet Gateway and in particular, email, need to be secured against virus, spams, phishing etc.

3.4 Any activities with the intention to create and/ or distribute malicious programs (Viruses, Worms, Trojans horses, email bombs etc.) uninstallation or deactivating the anti- virus product to function/receive updates are strictly prohibited.

3.5 If any team members receives what he/she believes to be a virus, or any evidence of viruses, malwares etc. without direction from the IT department.

3.6 Any virus infected computer shall be removed from the network until it is verified as virus -free.

4. Guidelines for virus Prevention

4.1 Never open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, including from the Recycle bin.

4.2 Never download files from an unknown or suspicious source.

4.3 Always scan removal storage and/ or external media like CDs, DVDs, flash disks, pen drives for viruses before using it.

4.4 Backup critical data and system configuration on a regular basis and store this data on the backup server and media types.

5. Execution owner

The responsibility for implementing and executing the procedures applicable to this policy are-

5.1 IT department- To monitor its effectiveness.

5.2 Line Management- To monitor and ensure that team member adhere to this policy .

6. Enforcement

Any team member found to have violated this policy might be subject to disciplinary action.

Software License Policy

1. Purpose

The purpose of this policy is to define roles and responsibilities on the licensing of software within YCPL.

2. Organizational Scope

This policy applies to all users of YCPL as defined in the Information Systems Statute.

3. Policy Content and Guidelines

3.1 General Regulations

a. Users are required to all YCPL on software licensing including, but not limited to, this policy and the Information Systems constitute misconduct, and may result in disciplinary action

b. Users are required to confirm with the terms and conditions of all license agreements for software loaded on to any Information System owned by YCPL.

c. Users of YCPL licensed software are required to confirm with the terms of all license agreements between the YCPL and any third party, including company licensed software installed or used on any system, computer, or device

d. Software must not be installed or used on organization owned Information Systems in any way that is in violation of the license agreement

e. YCPL licensed Software must not be installed or used on any un -official system, computer, or device in any way that is in violation of the license agreement.

f. The user responsible for the software and user responsible for the license must ensure that they fully understand the implications of any licensing agreement before using the software.

g. Adequate records must be kept by those responsible for management of any software, to ensure licensing information is available at all times.

Third Party Connectivity Policy

1. Purpose

To maintain the security of YCPL information processing facilities and information assets accessed by third parties. Access to YCPL information processing facilities by third parties should be controlled. This document describes the policy under which third party organizations connect to the YCPL Network for the purpose of transacting business related to YCPL.

2. Scope

This Policy applies to all contractors, vendors, agents and third party organizations that are currently using, or wish to connect to the YCPL Network. This Policy also applies to all remote access connections, regardless of type of telecom circuit, used to perform business transactions on behalf of /for YCPL. This Policy is complementary to existing Policies and specifically with YCPL Remote Access Policy and Network Access Control Policy.

3. Policy

a. All connection requests need to be reviewed by YCPL IT department. The review is to ensure that all access match the business requirements in the best possible way, and that the principle of 'legitimate need basis', 'least privilege' and 'default to deny' is followed. In no case, YCPL will rely upon the third party to protect YCPL Network or resources.

b. All connection requests between third parties and YCPL require that the third parties and YCPL representatives agree to and sign the Third Party Agreement. The Agreement would imply that there is a representative from the third party who is legally empowered with detailing the terms and conditions in the Agreement and maintaining the information usage to prevent misuse.

c. Information might be at risk by access from third parties with inadequate security management.where there is a business need to connect to a third party location, a risk assessment should be Carried out to identify any requirements for specific controls. It should take into account the type of access required, value of the information the controls employed by the third party and the implications of this access to the security of the YCPL information.

d. Appropriate controls are needed to third parties that are located onsite for a period of time as defined in their contract or agreement with YCPL and who need to access YCPL Information or Information processing facilities. Third parties include but are not limited to contractors, vendors, trainees and consultants. All security requirements resulting from third Party access or

internal controls should be reflected by the third party contract. Access to information and information processing facilities by third parties should not be provided until the appropriate controls have been implemented and a contract has been signed defining the terms for the connection or access.

e. Third party connections need to be terminated if they are no longer being used to conduct business and/or work for YCPL. YCPL IT department reserves the right to suspend any third party connections if they are found to be misused or if they are subject to security risks.

f. YCPL IT department reserves the right to conduct audits on third party locations to ensure appropriate compliance to security standards.

Internet Usage Policy

1. Objective
   The Internet Usage Policy provides guidelines for acceptable use of the organization's Internet
   network so as to devote Internet usage to enhance work productivity and efficiency and ensure
   safety and security of the Internet network, organizational data and the employees.

2. General Guidelines
   a. Internet is a paid resource and therefore shall be used only for office work.
   b. The organization reserves the right to monitor, examine, block or delete any/all incoming or
      outgoing internet connections on the organization's network.
   c. The organization has systems in place to monitor and record all Internet usage on the organization's network including each website visit, and each email sent or received. The
      Management Committee can choose to analyze Internet usage and publicize the data at any time to assure Internet usage is as per the IT Policy.
   d. The organization has installed an Internet Firewall to assure safety and security of the organizational network. Any employee who attempts to disable, defeat or circumvent the
      Firewall will be subject to strict disciplinary action.

3. Internet Login Guidelines
   a. All Users are transparently login in the Internet network using their System's Static IP which is also used for monitoring their individual usage
   b. All users will be responsible for the internet usage.
   c. Sharing the Username and Password with another employee, visitor or guest user is prohibited.
   d. A visitor or guest user who wants to use the office Internet will be given a Guest Username and Password.
   e. Any password security breach must be notified to the IT Dept. immediately.
   f. Username and password allotted to an user is automatically deleted upon resignation/termination/retirement from the organization as the same system is assigned to another user.

4. Password Guidelines

a. Individual password security is the responsibility of each user.
b. Passwords are an essential component of YCPL 's computer and network security systems. To ensure that these systems perform effectively, the users must choose passwords that are difficult to guess. This means that passwords must not be related to your job or personal life. This also means passwords should not be a single word found in the dictionary or some other part of speech.
c. To make guessing more difficult, passwords should also be at least Eight characters long. To ensure that a compromised password is not misused on a long-term basis, users are encouraged to change passwords every 30 days. Password history would be maintained for previous three passwords. This applies to the Systems Logon (windows password) and Cloud Mail passwords.
d. Passwords must not be stored in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, in computers without access control systems, or in other locations where unauthorized persons might discover them. Passwords must not be written down and left in a place where unauthorized persons might discover them. Immediately upon assignment of the initial password and in all cases of password "reset" situations, the password must be immediately changed by the user to ensure confidentiality of all information.
e. Under no circumstances, Users shall use another user's account or password without proper authorization.

f. Under no circumstances, the user must share his/her password(s) with other user(s), unless the said user has obtained from the concerned Manager/IT Head the necessary approval in this regard. In cases where the password(s) is/are shared in accordance with the above, the user shall be responsible for changing the said password(s) immediately upon the completion of the task for which the password(s) was shared.
g. In cases where no prior approval had been obtained for sharing of password(s) with other user(s), such user shall be completely responsible for all consequences that shall follow in respect of breach of this Policy and YCPL shall initiate appropriate disciplinary proceedings against the said user.

Email Usage Policy

a. All authorized users of YCPL are provided with an E-mail account, which is either individual to the specific user or generic Email ID and the same is protected with a password which is provided to the individual user. The use of E-mail should be restricted only for the business purpose. In case any individual is found using e-mail service, which is objectionable by any means, the access can be terminated by IT department without any prior information, however the same may be re-instated with the approval from the Managing Director and IT Head of the corporate office.

b. Email users should be aware that exchange of information with external sites may not be secured with high risks of spam, Trojans, malicious codes etc. Hence exchange of information should be limited to reliable sites. Users are prohibited to use their names/e-mail ids/mail domain in public domain without prior authorization from IT Head.

c. Information must not be transmitted internally or externally which is beyond the bounds of generally accepted standards, values and ethics. This includes, for example, material which could be considered offensive or discriminatory; pornographic or obscene, defamatory or any other material which is otherwise abusive or contains illegal content prohibited by law or regulation of the country or which brings the organization into disrepute. Information is

understood to include text, images and is understood to include printing information and sending information via email.

d. All material contained on the email system belongs to the YCPL and users should consider messages produced/received by them on YCPL account to be secure. The confidentiality of email data should be maintained by the individual user.

e. Security regarding access to the email system is of paramount importance. User identities and personal passwords must not be shared with others. Users should be cautious of providing their email addresses to external parties, especially mailing lists.

f. Users transferring or receiving files or attachments from external sources should note that the YCPL system automatically checks downloaded material for viruses. However, in the event that a virus is suspected, the file or attachment must not be opened and the matter must be reported to the IT Department immediately for inspection and action.

g. YCPL email users are required to use this communication tool in a responsible fashion and to observe the related guidelines. YCPL provides the email system for the purposes of conducting official business and it may not be used for personal gain or business activities unrelated to YCPL's operations. Users must not use the system to promote an external cause without prior permission from the IT Head.

h. Personal use of the email system is strictly not permitted as it interferes YCPL's operations & indirectly involve cost implications for YCPL along with loss of productivity.

i. Where it is considered that there has been a breach in the use of the email system, the service of the user will be terminated without any prior information.

INFORMATION SYSTEM AUDIT (IS AUDIT)

1. Objective

The object of IS Audit to provide an insight on effectiveness of controls which are in places in Company to ensure Confidentially and Integrity. IS Audit should identify risk and method to eliminate risk arise due to use of Information Technologies.

IS Audit should form part of Internal Audit Systems of NBFCs. While designing IS Audit frame work Company should efer various guidelines issued by the professional bodies like ISACA, IIA and ICAI. Company should refer standard issued by ICAI on "Standard on Internal audit (SIA) 14: Internal Audit on information technology environment. "

2. Coverage

IS Audit should cover effectiveness of policy and oversight of IT systems evaluating adequacy of processes and internal controls and recommend corrective action. IS audit also evaluate effective business plan. During the process of audit due importance must be given to applicable compliance and regulatory requirement.

3. Personnel

IS Audit can be done by internal team of the Company having proper knowledge of Information technologies and accounting standard mentioned by ICAI. Company can also appoint outside

agency having expertise in information system audit having right skill of mix between regulatory laws, compliance and information technologies. IS auditor should act independent of Company management and provide independent and professional view.

4. Periodicity

   IS Audit looking at company size may be conducted once in a year before statutory audit of the Company. IS Audit report to be submitted to statutory auditors to incorporate the same in audit report.

5. Reporting

   IS Audit report must be presented before the information technology committee and with Board of Director for review.

6. Compliance

   Company management is responsible for the compliance under report issued by IS auditors and intimate board time to time.

7. Computer Assisted Audit Technique

   Company to adopt proper mix of audit technique which include manual and computer assisted technique for detection of revenue leakage, treasury function, assessing control on weakness, monitoring customer transaction.

OUTSOURCING

1. Before outsourcing IT service, Company to evaluate the risk attached with outsourcing vis-à-vis regulatory requirements and other legal issues.
2. Outsourcing proposal should be evaluated by the Management of the Company
3. Terms and condition between Company and third party should be reviewed by internal legal and compliance team.
4. Company should have access to all books and records which was outsourced at any point of time.
5. Internal Auditors should consider while providing audit report on outsourced contract.
6. The board of director of the company solely responsible for the outsourced operation.
7. RBI master direction on IT policy to be followed by Company before entering into outsourced contract.

Approved By	Roshini Kapoor
Reviewed By	Raakhe Kapoor Tandon
Company Name	Yes Capital (India) Private Limited