MANAPPURAM ASSET FINANCE LIMITED(MAAFIN)

INFORMATION TECHNOLOGY POLICY

Version Control		
Version No.	Description	Date
Version 1.0	IT Policy	29-06-2022
Version 2.0	IT Policy	04-12-2024

Effective Date	04-12-2024
Next Review Date	04-12-2025
Policy Owner	Head of Information Technology
Prepared By	Risk Management Department
Reviewed By	Policy Review Committee
Approved By	Board

MANAPPURAM
ASSET FINANCE LIMITED

Contents

1.INTRODUCTION

Purpose and Objectives

Information Technology (IT) Policy governs the procedures to be followed by the individuals accessing and using an organisation's IT assets and resources. The document provides organisation wide strategies and responsibilities for protecting the confidentiality, integrity and availability of IT assets and resources that are accessed, created, managed and/ or controlled by the Company. Additionally, the document helps the management align its policies in line with the relevant laws and regulations. This document provides a framework to ensure protection and adequate use of the Company's IT assets and resources.

Applicability of IT Policy

This Policy applies to the Company employees and third parties (vendors, contractors, consultants, and auditors), information technology infrastructure, physical facilities and equipment owned by the Company.

Distribution of the Policy document

This is a confidential document and is meant for restricted distribution only. Any unauthorized copying or distribution of this document is strictly prohibited. Individuals in custody of this document are responsible for ensuring the confidentiality of the document. It is the responsibility of the IT Department to ensure that the document is updated with changes as and when required.

IT Department shall ensure that the Policy standards and requirements are communicated to all users including the Company employees and third parties (vendors, contractors, consultants, and auditors). Acknowledgement forms shall be obtained from all users on the acceptable usage policy awareness.

Maintenance Procedures

The following numbering scheme has been adopted for the Standard Operating Procedure documents references used in this document:

Number position	Acronym/ Number	Description
First Part	the Company_SOP	Document Type
Second Part	CM	Change Management Procedure
Third Part	v	Version
Digit	1.0	Version number

2.POLICY GOVERANCE

IT Policy Implementation

All employees of the Company (including branch employees) and third parties (vendors, contractors, consultants, and auditors), who require access to the information processing resources, are responsible for ensuring that IT policies are adhered to and they operate systems in such a manner as to ensure its security. The IT department is responsible for ensuring that staff are aware of, and adhere to, this Policy and the standards there under.

Policy Compliance

The IT Department shall ensure that:

- All users including the Company employees and third parties (vendors, contractors, consultants, and auditors) adhere to the Policy standards.
- Continuous compliance monitoring and measurement processes shall be adopted.
- Reports pertaining to continuous compliance monitoring and measurement processes shall be shared with the Information Security Team on a periodic basis.

Review of IT Policy

The document shall be reviewed at least annually by the IT Head. The IT policy and standard operating procedure documents shall be updated in-line with any major or minor changes in the operating environment. This Policy shall also be reviewed and updated in-line with recommendations provided by internal/ external auditors and legal counsel.

Exceptions to the Policy

The IT Department shall identify instances where exceptions to the Policy requirement shall be allowed for process, procedure, systems and specifications. Such requests shall be approved by the Managing Director. Exceptions allowed shall be reviewed periodically by the IT Department

Non- compliance/Violation of the Policy

Violation of standards defined in this document may include, but not limited to:

- Users do not comply with the Policy standards
- Use of the Company owned information processing resources for unauthorized or illicit purposes
- Violation of guidelines provided by the regulators
- Disclosure of confidential information

Non-compliance of users to the IT Policy would result in disciplinary actions including, but not limited to:

- Suspension
- Termination
- Other disciplinary action
- Civil and/or criminal prosecution

Training and Awareness

1. All employees of the Company should be provided with awareness on the IT policies and procedures to enable them to ensure that IT policies are adhered to and they operate systems in such a manner as to ensure its security.
2. The Company should arrange and coordinate periodic training and awareness programs through the training systems of the organization to ensure that the sufficient, competent and capable human resources are available. These programs should be targeted at all levels of employees including end users of IT resources in the organization, top management personnel and personnel managing the IT infrastructure of the organization.
3. The respective departments should monitor the work performance of their staff and should hold periodic assessments to identify IT training needs and to discover any

problem areas, particularly where staff deal with sensitive information, or work on sensitive computer applications.

4. All management and staff should be briefed on their own role in ensuring the protection of the organization's information assets and complying with the relevant policies and procedures.
5. The Company should make use of posters, newsletters, booklets, films and training courses so that all employees can better understand and carry out their responsibilities.
6. All the Company employees should receive prompt notice of changes in the Company's IT policies and procedures, including how these changes may affect them and how to obtain additional information.
7. Users should be made aware of the correct use of IT facilities including logon procedures, use of software packages, etc. prior to being given access, so as to reduce likelihood of errors.

   Designated employees should receive training in emergency procedures, first aid treatment and the use of fire fighting and other emergency equipment.

3. RISK ASSESSMENT FRAMEWORK

Introduction

A risk assessment is an important part of any information security process that is used to understand the scale of a threat to the security of information and the probability for the threat to be realized. The results of a risk assessment can then be used to prioritize efforts to counteract the threats.

The process of risk assessment is not a one-time activity but an on-going project, which is dynamic in nature and responds to changes in the internal and external environment facing an organization during a point of time. Therefore, while risk assessment may be classified as a point in time exercise, an organization's ability to assess and manage its risk continuously (in response to an ever-changing environment) is a key challenge .

MANAPPURAM
ASSET FINANCE LIMITED

Risk Assessment Methodology

1. The risk assessment process shall involve the following steps:

a. Identifying the in scope business processes and supporting information assets
b. Analyzing the threats that information assets are subject to
c. Identifying the vulnerabilities of the information assets
d. Understanding the controls in place and finding any gaps in the controls
e. Determining the impact that the loss of confidentiality, availability and integrity will have on the business

The following phased approach shall be adopted for performing the risk assessment:

a) Preparation: The risk assessment objectives shall be confirmed with all concerned stakeholders. An understanding of the scope and functions of the business and the key information assets that support the business processes shall be obtained. This involves, but is not limited to:

i. Understanding existing Information Security Framework: Applicable information security standards to the the Company environment shall be evaluated and assessed. Relevant global security standards and industry best practices shall be considered while performing the risk assessment.
ii. Identifying Controls: A work program based on the above mentioned information security standards shall be created and used by personnel during the risk assessment exercise. The associated controls that are in place to address the threat and vulnerability scenarios shall be covered. It can incorporate domains mapped to the Company processes and can include the controls, test procedures followed and observations noted.
iii. Identifying business functions and processes: Business functions critical to business delivery shall be identified and focused upon. Interviews with concerned stakeholders shall be scheduled to understand the business functions and priorities of the organization.

b) Assessment: The risks related to the various the Company IT processes shall be identified. This involves, but is not limited to Conducting Control Owner Interviews: Interviews shall be conducted with the control owners to understand the processes at the ground level and identify possible gaps in the definition of processes.

i. Performing Process Walk throughs: Process walk throughs shall be performed to understand the operation of business processes and to identify possible issues in the working of such processes. iii. Verifying

evidence of control design and implementation: Evidence of control design and implementation shall be verified to validate the efficacy of the control in mitigating risks.

c) Reporting: The identified gaps and issues shall be documented in a structured manner and reported to Risk Department. This involves, but is not limited to:

i. Documenting the Risk Assessment Report: The business process description and findings observed during the exercise shall be documented as part of the work program and a risk rating assigned to each observation. Additionally a consolidated observation log shall be created that will cover the identified gaps across locations and business domains.

ii. Review by Concerned Stakeholders: A review shall be conducted by concerned stakeholders to identify any inaccuracies in the observations identified by the risk assessment team.

iii. Release of Final Report: Once the observations have been finalized, the final report shall be released to the senior management within the Company for their perusal.

d) Treatment: The identified risks shall be assessed to determine the mitigation strategy. This involves, but is not limited to:

i. Identifying treatment options and mitigation measures: If the residual risk of the observations identified by the Risk Assessment Team is at an acceptable level, mitigation of risks may not be required. Otherwise, further controls need to be identified to mitigate the risk. These actions can be any one of the following along with a justification for the option:

- Accept the risk
- Transfer the risk
- Mitigate the risk
- Control the risk

ii. Preparing Risk Treatment Plan: A consolidated risk treatment plan shall contain the risk treatment decision taken for each observation and will contain implementation tasks recorded against each threat that requires the implementation of controls to mitigate, avoid or transfer the risk.

MANAPPURAM
ASSET FINANCE LIMITED

Criticality Assessment Criteria

The objective of providing a criticality rating for each risk is to understand the impact on business and rate it accordingly for the control. The methodology for rating the identified risks shall be as follows:

1. High: The controls are not in place to prevent the risk from materializing; the outcome of which may include but are not limited to severe business loss, frequent recurrence of the incident, class action lawsuit, costly legal or regulatory penalties, or an organization wide impact to employee safety, morale and well-being.

   Typically, such HIGH risks may result in, among other things:

   a) High financial losses.
   b) May significantly violate, harm, or impede an organization's mission to comply with regulations.
   c) May result in significant harm to the organizations reputation and employee morale.

2. Medium: The controls are in place to reduce the risk from materializing but are seen inadequate or are not being implemented properly; the outcome of which may include but are not limited to significant business loss, individual occurrence of the incident, potential lawsuit, significant legal or regulatory penalties or localized impact to employee safety, morale and well-being.

   Typically such MEDIUM risks may result in:

   a. Costly financial losses;
   b. May violate, harm an organization's mission to comply with regulations;
   c. May moderately harm the organizations reputation and employee morale;

Audit Observations on inadequate or non-compliance with the existing controls.

3. Low: The controls are in place to prevent, or at least significantly impede the risk from materializing; the outcome of which may be limited to minor business loss, potential legal or regulatory penalties or isolated impact to employee safety, moral and well being.

   Typically, such LOW risks will almost always be a part of audit observations (where self-assessments are not prevalent) and may also result in, among other things:

   a. Some financial losses.
   b. May noticeably violate, harm an organization's mission to comply with regulations.

c. May harm the organizations reputation and employee morale.

4.ACCEPTABLE USAGE POLICY

Introduction

The objective of This Policy is to create awareness among end users on the acceptable usage of company information and information processing resources. the Company shall ensure that all the Company employees and third parties (vendors, contractors, consultants, and auditors) use the Company's information processing resources as defined by the policies, procedures and guidelines and only for business purposes.

This section shall be read in conjunction with the following:

- Acceptable Use Of Information Processing Resources in Information Security Policy document

Computer Systems Usage

Computer systems provided by the Company shall be used only for business purposes.

Password Policy

1. Passwords shall be created in accordance with the Password security policy Sharing of passwords is strictly prohibited.
2. Passwords are to be treated as confidential information. Under no circumstances is an employee to give, tell, or hint at their password to another person, including IT staff, administrators, superiors, other co-workers, friends, and family members.
3. Under no circumstances will any member of the organization request a password without the request coming from both a representative of the IT department and the user's direct manager. Should a request be made that does not conform to this standard, immediately inform both the IT department and your direct manager.
4. Passwords are not to be transmitted electronically over the unprotected Internet, such as via e-mail. However, passwords may be used to gain remote access to company resources via the company's Virtual Private Network or SSL-protected Web site.
5. No employee is to keep an unsecured written record of his or her passwords, either on paper or in an electronic file. If it proves necessary to keep a record of a password, then it must be kept in a controlled access in case of hardcopy or in encrypted file in

case of electronic form. Also, the “Remember Password" feature of applications shall not be used.

6. Passwords used to gain access to company systems are not to be used as passwords to access non-company accounts or information. Similarly, passwords used to access personal, non-work related accounts are not to be used to access company accounts.
7. Each application, system and data point should be protected by a different password where possible. The use of the same password to protect all access is strongly discouraged.
8. If an employee either knows or suspects that his/her password has been compromised, it must be reported to the IT Department and the password will be changed immediately.
9. The IT Department may attempt to crack or guess users' passwords as part of its ongoing security vulnerability auditing process. If a password is cracked or guessed during one of these audits, the user will be required to change his or her password immediately.

E-mail Usage and Internet Usage

Email and Internet services provided by the Company to users are to be used only for business purposes and as per guidelines provided in the:

- Email Usage Policy
- Internet Usage Policy

Mobile Device Usage

Employees shall not use their own devices for accessing/ storing or exchanging company information. However, if hand held devices are used by employees for accessing/ storing or exchanging company information like data/ e-mail/ SMS, then users shall take prior approval from the MD.

Such users shall take due care to protect such devices and the data stored therein from loss, theft and misuse through use of appropriate protection measures such as secure handling, passwords, PINs, encryption etc. For details on mobile device security refer to the Bring Your Own Device (BYOD) Policy in Information Security Policy.

Clean Desk and Clear Screen Policy

- Users shall abide by the Clear Desk and Clear Screen policy in the Information Security Policy, on paper documents.

- Users shall keep information assets such as printouts, notepads etc. in a secured place when not in use
- Users are responsible for protecting any information used and/ or stored on the Company workstations
- Users shall ensure that their terminals are adequately protected by locking the same when not in use and shutting the terminal down when leaving the premises
- Users shall ensure that any material printed on network printers is supervised and not left unattended

Social Media Policy

Users shall abide by the social media Policy in Information Security Policy, when using social media platforms and blogging sites from the Company.

the Company shall monitor any Internet activity occurring on company equipment or accounts. the Company employs filtering software to limit access to sites on the Internet. If the Company discovers activities which do not comply with applicable laws or departmental policies, relevant information which can serve as evidence shall be retrieved.

Reporting of Incidents

In case users come across weaknesses in computer security or any incidents of possible misuse or violation of This Policy, the user shall report the same to his or her Manager or Head of Information Security.

5.E-MAIL USAGE POLICY

Introduction

This section shall be read in conjunction with the following:

- E-mail Security Policy of the Information Security Policy document.

Standards

10. Users using the Company's e-mail system shall avoid performing activities such as:

    - Sending or storing offensive content
    - Sending the Company's proprietary or confidential information to external parties
    - Sharing e-mail accounts and passwords with other users
    - Using the Company's e-mail system for unsolicited mass mailing, non-company commercial activity, political campaigning, dissemination of chain letters, and use by non-employees
    - Using the Company's e-mail system for creating, sending or storing material that infringe the copyright or intellectual property right of any third parties
    - Opening e-mails from unknown or unsigned sources
    - Sending e-mails with unreasonably large attachments
    - Sending e-mails using other users' e-mail accounts

11. Users shall be responsible for managing their individual mailboxes. Users shall be responsible for all outbound emails sent from their mailbox.

12. All branches/departments/eligible employees of the Company shall receive an e-mail account.

13. All email IDs shall be tagged to a single user. However, in the event of creating shared email IDs and distribution lists, approval has to be obtained from the CTO.

14. All branches shall be provided with a single mailbox, which shall be owned by the Branch Head.

15. An automatic standard footer disclaimer shall be included in all e-mail communications. Employees shall not add, modify or delete the disclaimer of the Company, at any time of use of the email systems. The disclaimer shall include the following (but not limited to):

    - The e-mail is intended for the use of the recipient to whom it is addressed
    - If received by an unintended user, the e-mail shall not be acted upon and shall be immediately deleted

16. the Company reserves the right to monitor all e-mails sent and/ or received through its e-mail system. Such monitoring shall be for the purpose of legal requirements and as per extant provisions of relevant regulations from time to time.

17. Users shall be notified before the IT Department reviews the users' e-mail records. The IT Department shall disclose the contents of e-mails to law and regulatory agencies, if required by law enforcement or regulatory agencies.
18. Archival and backup copies of e-mail messages shall be taken, despite end-user deletion, in compliance with the Company's Records Retention policy. The goal of these backup and archival procedures is to ensure system reliability, prevent business data loss, meet regulatory and litigation needs, and to provide business intelligence.
19. All employees shall be required to sign the email acceptable use policy acknowledgement.

6. INFORMATION ASSET MANAGEMENT

Introduction

Policies and standard operating procedures shall be established to protect information, documents, computer media, input/ output data and system documentation in order to prevent damage to assets and interruption to business activities. This section shall be read in conjunction with the following documents:

- Asset Management Policy of the Information Security Policy document

Standards

1. The Asset Management Team shall maintain an inventory of all assets owned by the Company. Assets include the Company's applications, information and information processing resources.
2. the Company shall use an appropriate tool for asset management and identify an asset owner and asset custodian for all the assets.
3. The Asset Management Team shall be responsible for recording and updating the asset details in the inventory and classifying the assets based on the internal risk assessment performed.
4. Periodic review of the assets against the inventory details shall be performed in order to ensure that the assets details are up to date in the register.
5. All physical assets shall be labelled with a unique asset number.

6. All types of assets including, but not limited to, the following shall be identified and inventoried:
    - Software Assets: Application software, system software, software utilities, OS, databases, version control systems like SVN etc.
    - Physical Assets: Storage media, servers, network devices, computers and other input devices, printers and other output devices etc.
    - Information Assets: Critical electronic/ physical forms of data (such as, but not limited to, Legal documents, Service Level Agreements, Standard Operating Procedures etc.)
7. The asset register shall include at a minimum:
    - Asset Number
    - Asset Status
    - Serial Number
    - Device Type
    - Asset Description
    - Asset Custodian
    - Asset Owner
8. The respective user departments shall issue physical assets to the end users after obtaining approval from respective Heads of Departments.
9. If an asset needs to be moved out of the Company's premises for repair/ servicing/ maintenance it shall be done based on approval from Asset Owner/ respective user departments. The Asset Owner/ respective user departments shall ensure that the assets are returned to the Company's premises after the repair/ servicing/ maintenance activities.
10. The Asset Management Team shall maintain a 'Hardware Movement Register' to record the movement of the Company's assets outside its premises.
11. All computer media (such as tapes disks, CDs) shall be stored in a safe, secure environment, in accordance with the manufacturer's specifications.
12. Procurement, distribution and use of the Company's media shall be controlled by Purchase Department and Asset Management Team.
13. A physical asset audit must be conducted on a periodic basis to confirm location of assets for its security, insurance, depreciation, efficiency, and maintenance purposes.

14. All software deployed in the Company shall be available in a common software pool and licenses and documentations for each software title and version shall be documented and reviewed. All identified gaps/ issues, if any, shall be addressed and rectified on a half-yearly basis.
15. All software keys and installation disks shall be kept in safe place.
16. Adequate backups of all software shall be maintained.
17. Only licensed software must be deployed in the Company's environment and all software deployed in the Company shall be purchased with the technical recommendation from the IT Department.
18. Annual Maintenance Contract (AMC) and other details shall be updated regularly.
19. 'Media Disposal Register' shall be maintained to track and record the status of media that needs to be disposed.
20. The hardware/ media that was disposed must be removed from the Information Assets Inventory, under due authorizations.
21. The Asset Owner shall be responsible for overseeing all media disposal activities. Proof of disposal records shall be maintained.
22. The CTO/ IT Head shall review the Media Disposal Register periodically.

7.Desktop Install-Move-Add-Change (IMAC) Policy

1. The goal of this policy is to outline guidelines for end-users to request a move, add, or change to their desktop computing environments.
2. The Install-Move-Add-Change request form must be used for the completion of any of the following;
    - Install desktop system (e.g. PC, telephone) or peripheral (e.g. printer)
    - Move desktop system (e.g. PC, telephone) or peripheral (e.g. printer) to another location.
    - Add/disable an employee account (e.g. network, e-mail, voicemail).
    - Add/remove a service to/from an existing employee account.
    - Add a new employee desktop system.
    - Add/remove/change software or hardware to/from an existing desktop system.

- Change an employee's name or other personally identifiable information in the system.

3. Although any employee may submit an IMAC request for their desktop environment, all requests shall be approved by the Department Head before submission to the IT Support Desk.

4. All install, move, add, or change requests shall be sent before the requested action date. However, to ensure that the preferred action date can be met, it is recommended to submit the request as early as possible. In order to minimize disruptions and maintain efficiency, all regular IMAC services shall be scheduled to take place within the agreed timelines.

5. While all approved IMAC services shall be carried out in a timely manner, there may be delays in the event of any unforeseen IT -related problems or emergencies.

6. In the event of an emergency request, advance notification is not required. These requests shall be handled on a case-by case basis. Details of the actual execution of the request shall be forwarded to the requester in a timely manner on receipt of the request.

7. Most IMAC services involve system downtime for the user. Outage windows shall be minimized whenever possible. However, the requester must be aware of the implications of such downtimes.

Software Installation Policy

1. The Software Installation Policy articulates what software is permitted on enterprise end-user devices, the approving authority and who shall carry out the installation task.

2. The following table contains list of fully supported, that may be installed on Company owned end-user devices:

No.	Company's Standard Software (Licensed)
1	Microsoft Windows 10 ,11
2	Adobe Reader
3	Office 365
4	Dot Net framework 2
5	Open Office (Versions)
6	Report Setup

7	Antivirus
8	Report viewer
9	All drivers & Manappuram modules required for user
10	Java 6. Update 7
11	.Net Applications
12	Adobe /Flash Player 10

3. All software installations and de-installations shall be thoroughly documented so that appropriate licensing fees can be paid or amended.
4. If a user requires installation of a particular software, approval shall be obtained from the IT Head after taking due recommendation from the user's Department Head. The IT Department reserves the right to reject any software installation request. This includes all software titles listed above, currently unlisted titles, and privately owned and licensed titles.
5. Software titles are to be installed on company-owned end-user devices by IT Helpdesk under direct supervision of department senior official. The IT helpdesk reserves the right to uninstall any unapproved software from a company owned machine.
6. Unannounced, random spot audits shall be conducted. During such audits, scanning and elimination of computer viruses shall be performed. Other unsanctioned software shall also be uninstalled at this time.
7. The IT helpdesk reserves the right to monitor software installation and usage on the Company's end-user devices. The IT Department shall conduct periodic audits to ensure compliance with the Software Installation Policy.

8.LOGICAL ACCESS MANAGEMENT

Introduction

This section shall be read in conjunction with the following:

- Logical Access Policy of the Information Security Policy document

Standards

1. Users shall be granted access to the Company's applications, systems and information processing resources on a 'need to-know-basis'. Users shall be granted Read/ Write/ Execute/ Delete access on the basis of 'least privilege' to perform desired job function.
2. Access to applications or other information processing resources in the Company are provided to employees based on their job profile by the HR Department. For any additional access, the user shall submit an 'Access Request Form' or 'Software Request Form'. This request form shall be approved by respective Head of Department subsequent to which the access shall be provided by the System Administrator (IT Department).
3. For third parties (vendors, contractors, consultants, and auditors), the process for providing access to the Company's applications, systems and information processing resources is the same as the process documented for the Company employees.
4. Users shall be granted unique user IDs to ensure accountability wherever applicable. Duplicate user IDs shall not be created on the applications, systems and information processing resources.
5. Use of group or shared IDs shall not be permitted, unless a valid business justification is provided. Shared IDs shall be permitted to a group of individuals sharing a common job role.
6. The Human Resource (HR) Department shall notify the IT Department of all changes (the roles and access that need to be added, and the roles and access that need to be removed) to a user's access rights. For transferred and promoted employees, the HR Department shall also communicate the effective date of change in position to the IT Department.
7. For resigned and terminated employees, the HR Department shall notify the last working day of these employees to the IT Department, so that their access to the Company's applications, systems and information processing resources is revoked on the last working day.
8. The IT Department shall be responsible for maintaining the user access listings of all applications in the Company. The respective Heads of Departments shall be responsible to communicate the changes that need to be made to these user access listings.
9. A standard naming convention shall be used for all user accounts in the Company's applications, systems and other information processing resources to facilitate user identification. Naming conventions shall cover all end users, vendors, contractors, consultants, and auditors.

10. User access and activity logs shall be captured and monitored for all applications, systems and information processing resources in the Company.
11. Users shall not be granted access to edit or delete the logs.
12. The access logs shall be retained for a period as determined by respective regulatory authorities.
13. User IDs with special system privileges shall be controlled and restricted to a limited number of authorised users. These will include user IDs, which are used to administer modifications to the operating system, security functions and audit logs.
14. System IDs with privileges in support of the operating system (service machines, started tasks, agents, installed system user IDs, etc.) shall be assigned to the system owner unless otherwise assigned to an authorised individual.
15. Privileged access shall be provided to authorised users based on their job role, along with the recommendation and approval from users' Head of Department. Privileged user access shall be granted based on a valid business need or reason.
16. Privileged access shall be granted to a group of users only when all the users in the group have a valid business justification.
17. Administrator accounts shall not be shared under any circumstances.
18. Each administrator shall be assigned his or her own unique administrator ID (domain/ server/ application/ database/ network device) to ensure accountability. Administrator IDs shall be assigned the necessary administrative capabilities so that the user may carry out his or her assigned job functions.
19. Revalidation of privileged IDs shall be performed quarterly.
20. Privileged IDs shall be revoked within three days from the date of notification from the HR Department.
21. Passwords shall contain all four (4) following character classes wherever applicable:
    - Lower case characters
    - Upper case characters
    - Numbers
    - Special characters
22. Two types of password are allowed which are, the punching password and transaction password. Punching password shall be used for all general purposes and transaction password shall be used for financial impacting transactions.
23. User ID shall not be part of the password.

24. Users will be notified five days in advance of password expiration. At that point, and at every subsequent login until a change is made, users will be prompted to select a new password.
25. The minimum length of passwords shall be set as eight (8) alphanumeric characters, wherever practical.
26. Password expiry shall be set to 90 days, wherever practical.
27. The practice of 'recycling' of re-using the same password shall be prevented. Password history shall be set to eight (8), wherever practical.
28. User IDs shall be disabled after incorrect passwords have been entered for five (5) consecutive times, wherever practical.
29. Default passwords, provided in the software upon installation of the software or receipt of a system with preloaded software, shall be immediately changed.
30. Temporary passwords shall be conveyed to the users in a secure manner. The initial passwords created shall adhere to the Password Policy, be difficult to guess, and be unique to each user.
31. Users shall be limited to a single login session on all networked computers, wherever applicable.
32. No user in the Company shall use another user's ID to gain access to computer resources.
33. Users shall be held accountable for all activities performed using their user IDs.
34. While provisioning user IDs, System Administrator shall bind the user IDs to the MAC address of the devices that they are authorised to use.
35. All users shall terminate their active sessions, when finished, unless they could be secured by an appropriate locking mechanism (e.g. re-authentication of user).

9.BACKUP AND RESTORATION

Introduction

This section shall be read in conjunction with the following:

- Backup and Restoration Policy of the Information Security Policy document

Standards

1. Backup of data residing in critical applications and other information processing resources shall be taken regularly to ensure that the data is available in the event of a system failure or to recover past transactions.
2. The responsibility of the backup operations shall be assigned to Backup Administrator, who is part of the Server Systems Operations Team. The Backup Administrator shall ensure that the Backup procedures are aligned with the RTO (Recovery Time Objective)/ RPO (Recovery Point Objective) of the BCP (Business Continuity Policy) of the company.
3. the Company shall perform periodic risk assessments to identify the critical applications and other information processing resources that need to be backed up. The Server Systems Operations Team (SSO), in consultation with the respective Heads of Departments, shall identify the critical data relevant to each business process that is under the purview of the respective user department.
4. The Company Infra Team shall identify the essential components that need to be backed up for each critical application, including the following (but not limited to):
    - Operating system files
    - Application files
    - Data files
    - Configuration files
    - Database
    - Log files, including operating system logs, application logs and security logs
5. The backup operations shall be in line with the defined Business Continuity Plan and Disaster Recovery Plan for all information processing resources.
6. the Company shall use a centralised tool to backup critical applications and other information processing resources. The permission to edit the job schedules configured in the tool shall be restricted to the Backup Administrator.
7. The Server Systems Operations Team shall track the backup status for the critical applications and information processing resources in the tool.
8. The backup tool shall be configured to trigger automated alerts for all backup failures. These alerts shall be monitored and managed by the Backup Administrator, with the aid of the IT Department.
9. On a daily basis, the the Company Infra Team shall send a report capturing the status of all backup jobs to the IT Department. The backup jobs that are not completed in the

defined backup window shall be highlighted as an exception and through an incident ticket.

10. Failed backup jobs shall be re-initiated and completed either the same day or the next day. The decision to reinitiate the job the same day or the next day shall be made by the Backup Administrator based on the following:

    - Criticality of the failed backup job
    - Recommendation from the concerned user department

11. All critical backups shall be scheduled during non-peak usage hours.
12. Backup shall be taken before and soon after the execution of a critical process.
13. The retention period is required to determine the rotation cycle of the backup media and to decide whether it is necessary to erase past data for creating free disk space. The Server Systems Operations team, in consultation with the Compliance Team, shall define a standard retention period for the backup of all critical applications and other information processing resources. The retention period shall be determined based on the data retention mandates issued by regulatory bodies including Reserve Bank of India (RBI).
14. All tape/ offsite backup media shall be uniquely labelled and stored in a fireproof cabinet.
15. For critical applications, a copy of the backup media shall be stored at an offsite location. The backup shall be moved to the offsite location on a weekly basis. Backup media shall be properly packaged to prevent damage and tampering while transferring to offsite location.
16. the Company shall revalidate its Backup Policy and corresponding configuration in the backup tool every six months.
17. Access to the data stored in the backup media placed in the datacentre and offsite location shall be secured from unauthorised access.
18. The backup logs shall be maintained by the Backup Administrator. The log shall be reviewed on a weekly basis by the the Company Infra Team/ CTO.
19. Following adequate security measures shall be taken before disposing the backup media:

    - Essential data shall be copied to another media
    - Data on the backup media shall be erased before disposing the media

20. The the Company Infra Team shall perform restoration test for a sample backup media of critical applications and information processing resources at least every quarter, in order to ensure that data is available and retrievable in case of any adverse events (e.g. system failure, loss of data).

10.END USER COMPUTING (EUC) MANAGEMENT

Introduction

End-user computing (EUC) tools refers to systems & applications, which are created by end-users outside a recognized formal IT area. Such tools can be spreadsheets, databases, report writers etc. Given the importance related to integrity and reliability of the information generated by EUC tools, appropriate measures must be adopted for ensuring that appropriate controls exist.

Development of EUC application

1. The Company shall discourage users from developing EUC applications. However, in case of projects involving huge resources and usage of critical data, the users will route the request for authorisation through departmental heads for initiating the project. The following documentation will be required for approvals of such EUC application:
    a. need and objective of the EUC application;
    b. assessment of the cost, time and efforts involved in the project;
    c. need for special hardware, software or storage requirements; etc.;
2. Users shall route the request for approval through IT team and CISO. The IT team may route the request to CTO for security considerations.
3. Users shall conform to the policies and procedures laid down by the the Company related to system development and maintenance while developing any EUC application.
4. EUC applications shall not be allowed to upload any data directly into the organization's production system.
5. Users shall evaluate the criticality of the EUC application and design adequate controls to ensure secure computing. If required, they may seek help from CTO/CISO on any technical area.
6. Users shall test the EUC application with the help of independent personnel to ensure accurate computing and adequate exception handling mechanism is in place.

7. Version controls shall be implemented for the EUC application to ensure that the same data is used by all concerned users of such data and for audit purposes. This shall be reiterated through frequent communications so that all EUC data are governed by Version control disciplines.

8. Users will maintain adequate system documentation for the EUC which will include:

    a. name of the EUC application;
    b. details of the author of the EUC application;
    c. need and objective of the EUC application;
    d. approval for the EUC application, if any;
    e. sources of input and the format in which it is to be made available;
    f. computations performed and its logic;
    g. tests results;
    h. operating instructions for users; etc.
    i. current version in use.

Inventory of EUC applications

1. Users will be responsible to inform the IT team about the EUC applications implemented by them.

2. The IT team shall periodically review the EUC applications running on user machines to ensure that all of these applications are reported to the IT department along with adequate system documentations. This exercise is essential to ensure that the Company can continue using and maintaining the EUC applications in absence of the authors.

Change management

1. Users have complete access to the EUC applications making them vulnerable to risk of accidental and/or malicious modifications. In order to protect the integrity of these applications, adequate controls shall be implemented to ensure continuity, confidentiality, and integrity.

2. Users shall maintain a record of all changes made to the EUC application.

3. All changes introduced into the EUC application shall be tested with the help of independent personnel.

4. System documentation shall be updated to reflect the current status of the EUC application.

Back-up of EUC applications and data

1. EUC back-up procedures shall follow the same pattern as defined for the core applications.
2. Users shall ensure that control copy of the EUC application is furnished to the IT team, which will then be responsible for maintaining adequate back up.
3. Users shall maintain EUC data in a suitable space allotted to them on file servers so that it is backed up by the IT team as a part of normal back up process.
4. If a file server is not available at a particular location, the users shall backup the data as per the standard backup procedures and store it securely.

11.CHANGE MANAGEMENT

Introduction

This section shall be read in conjunction with the following:

- Change Management Policy of the Information Security Policy document.

Standards

1. Changes to an information processing resource including programs, system software, hardware or any other aspect of the information-processing environment shall be governed by a formal change control process.
2. The change management team shall ensure that all changes to the Company's operational environment are:
    - Identified and recorded
    - Assessed for potential risks
    - Formally approved
    - Communicated to all relevant stakeholders
    - Rolled out with minimum disruption to the production environment and that roll back plans are ready
3. The testing environment shall be segregated from the development environment. The quality assurance and user acceptance testing shall be conducted in the testing environment.

4. If a separate testing environment is not feasible, then the test environment shall be logically separated from the development environment.
5. The production environment must be segregated from development and testing environments.
6. The business team shall prepare a 'Business Requirement Specifications (BRS)' document, along with a 'Change Request Form (CRF)', detailing the requirements of the new software or application.
7. The BRS and CRF shall be assigned a risk rating and classification based on an internal assessment. Once this activity is completed, the estimated cost and working hours are identified and recorded in the document.
8. The BRS and CRF shall be approved by the respective Head of Department (whose department is requesting for the new software or application), approval from CTO/ IT Head and Managing Director along with the impacting department should be in place.
9. In case the risk rating is 'High', an additional approval shall be obtained from the Head of Risk.
10. For minor customizations, where additional cost is not involved, the BRS and CRF require an approval from the CTO/ IT Head only.
11. The Management shall decide whether to develop the change requirements in-house at the Company or to outsource the change development to an approved support vendor, after internal discussions.
12. For changes developed in- house at the Company, a change ticket shall be raised in the centralized change management tool.
13. Once the change is developed and tested, the change shall be pushed to the production environment only once the approval from the CTO/ IT Head is obtained.
14. An emergency change is a critical change required to resolve a 'Severity 1/2' incident to ensure that information processing resources are available for critical business operations.
15. Emergency changes shall be recorded and documented retrospectively after actual implementation.
16. Approval shall be obtained for implementation of emergency changes from Chief Technology Officer (CTO) or Managing Director (ED). In cases where only verbal approvals from CTO/ ED were obtained, electronic approvals must be obtained retrospectively prior to closing the ticket.

17. Emergency changes shall be logged and approved in the tool within a business day from the date of implementation.
18. A Change Implementation Plan shall be prepared for 'High' impact changes.
19. The Change Implementation Plan document may contain the following details:
    - Time and resource requirements
    - Change impact description
    - Pre-requisites
    - Test plan
    - Implementation plan
    - Back out/ roll back plan
    - Technical group accountable for the change
    - Change Type
20. All changes developed shall be submitted to the Change Regulatory Board (CRB) for review.
21. The Change Regulatory Board shall conduct review meetings on a Monthly basis. The meetings shall be attended by the CEO,CTO,CRO ,CISO/Head IT,CCO and CFO.
22. All the emergency and expedited changes shall be reviewed during the monthly meetings.
23. The Change Regulatory Board shall review the effectiveness of changes based on the following parameters:
    - Changes achieving desired objective
    - Adherence to implementation plan

The Change Regulatory Board shall ensure that ineffective changes are rolled back.

12.ANTIVIRUS MANAGEMENT

Introduction

Antivirus software is a computer program that attempts to identify, neutralize or eliminate malicious software. Most modern antivirus software is designed to combat a wide range of threats, including worms, virus hoax, Trojans, often described collectively

as malware. Antivirus software has been implemented to protect information-processing systems at the organization against virus attacks.

Guidelines

1. The Company shall ensure that all work stations (desktops and laptops) and servers be adequately protected against viruses, worms, malware and trojans.
2. All machines shall be installed with the latest version of an antivirus client and definitions updated daily. Periodic reconciliation shall be performed to ensure that all machines have the latest anti-virus signatures/definitions installed. End users shall not have the ability to change configuration settings of the Anti-virus.
3. The workstations (laptops/desktops) and servers shall be configured to contact antivirus server every 24 hours to request for updates and download the same locally, if available.
4. The antivirus software shall be configured to scan all data from the desktops and laptops hard drive and servers. If any file is infected with a virus, it shall be cleaned by the antivirus software. In case the virus is not cleaned by the antivirus software, the infected file shall be quarantined.
5. All virus incidents shall be reported to the the Company Infra Team. Further, users shall have the provision of reporting virus issues to the service desk for suspected virus infections to their machines.
6. Full scans of all workstations (desktops/laptops) shall be scheduled daily at non-business hours.
7. If any new patch for antivirus software is released, it shall be updated on all servers and workstations through a formal change management process.
8. IS Operations team shall have the authority to change the Scan settings, Update pull settings to enable them to effectively manage the operations through an approved change management process.

Periodic Review

1. Daily review of the AV console shall be conducted to ensure that the latest pattern file have been pulled from the live update server and have been updated on all machines, servers and workstations.
2. Tickets shall be logged for recurring failures for AV updates.

3. Monthly review of the quarantined virus items shall be performed to determine whether any particular virus has been recurring.
4. Monthly reviews of 10% machines shall be performed to ensure all machines have AV/update installed and have had at least one full scan of all disks

13.NETWORK MANAGEMENT

Introduction

This section shall be read in conjunction with the following:

- Network Management Policy of the Information Security Policy document

Standards

1. The Infrastructure Team shall document the hardware configuration of all servers in the Company and shall review these configurations annually.
2. Unauthorized software shall not be installed in the Company's servers. The Infrastructure Team shall maintain an inventory of network service software and other application or utility software that shall be installed in the Company's servers.
3. the Company shall adopt hardware redundancy for all critical applications and network servers to ensure that its operations continue even in the event of a disaster.
4. Fail over mechanism shall be adopted for all critical servers in the Company.
5. Based on the periodic risk assessment performed, the Network Operations Team shall deploy two separate power supplies for critical network devices and servers.
6. Public facing servers shall be deployed in a Demilitarised Zone (DMZ). The IP address for public facing servers shall be translated using Network Address Translation (NAT).
7. For decommissioned servers, the Network Operations Team shall ensure that relevant data is removed or migrated to another server without leakages.
8. Operational manuals shall be prepared by the Network Operations team for each server.
9. the Company shall adopt the process of server hardening to mitigate the risk of weakness in the operating systems.

10. The following techniques may be considered during the process of server hardening:
    - Block unused ports
    - Disable unused or unwanted network services
    - Apply hot fixes
    - Configure security policies for authentication and access control • Setup encryption
    - Enable auditing on application and security logs
    - Removing unauthorized software
    - Disabling of default permissions and accounts
    - Changing default passwords
11. The Network Operations Team shall enable network services such as, but not limited to, FTP, SFTP, SSH or HTTPS on the Company servers based on valid business reason.
12. All network systems, servers and devices on premises shall be synchronised to an accurate time source.
13. Only licensed version of operating systems shall be installed in the Company servers.
14. Default parameters such as passwords shall be changed as part of the installation process.
15. The default settings in the operating system shall be reviewed prior to installing the operating system. Default settings that could potentially cause security vulnerabilities shall be disabled during the installation process.
16. Users shall be provided a unique user ID and password. Shared/ group IDs shall only be allowed in case of a valid justification from the respective Head of department.
17. All user accounts shall be provided a name and description.
18. The Network Operations Team shall delete/ disable all 'Guest' accounts.
19. Users shall be granted access to the operating system on a 'need-to-know' basis by restricting access permissions to operating system files and directories.
20. The Network Operations Team shall be responsible for installing security related updates in a timely manner.
21. All unsuccessful login attempts shall be recorded.
22. The Network Operations Team shall identify the type of log information that needs to be retained and monitored.

23. Only the Network Operations Team shall have the access to edit/ reconfigure the logging mechanisms.
24. The access control mechanisms, retention period and disposal of log files shall be defined based on the Backup and Restoration Policy.
25. Inactive terminals shall be locked after a defined period of inactivity. The lock out duration shall be determined by the Network Operations Team.
26. All the Company's wireless infrastructure/ network devices, which include access points, servers and laptops, shall adhere to the following:
27. User access to wireless infrastructure (excluding public Wi-Fi) must be authorised and approved by CTO/ IT Head.
28. the Company shall use Wi-Fi Protected Access (WPA 2.0) compliant protocols and not Wired Equivalent Privacy (WEP) protocol.
29. Strong authentication mechanism shall be implemented for users connecting to the Company's corporate wireless networks.
30. User access to the Company's wireless network shall be restricted using MAC binding.
31. The use of guest wireless networks provided to personnel visiting the Company premises shall be granted based on an authentication mechanism. The guest network shall be independently segregated from the Company's corporate network, and adequate controls shall be placed to restrict the inbound and outbound connectivity.
32. Visitors requiring access to the Company's guest Wi-Fi network shall be provided time bound access. The CTO/ IT Head shall approve the guest's access to the Company's guest Wi-Fi
33. The guest Wi-Fi access shall be revoked automatically after the approved time period.
34. The Network Operations team shall ensure that Wireless LAN (WLAN) is logically separated from Wired LAN.
35. Administrator access to wireless access points shall be limited to authorised personnel from the IT Department.
36. On a regular basis, Network Operations Team shall monitor for any rogue wireless networks and disable such networks on priority. 'Rogue' refers to any new unregistered access point.
37. Broadcast of Service Set Identifier (SSID) of the Company's corporate wireless networks shall be disabled.

38. The Network Operations Team shall periodically monitor the status of wireless access points and connectivity, and shall submit a consolidated report to the CTO/ IT Head for review.

39. Employees may request access from the Internet for services located on the internal network. Typically, this remote access is handled via a secure, encrypted virtual private network (VPN) connection. VPN sessions will have an absolute timeout length. An inactivity timeout will be set. At the end of these timeout periods, users must reauthenticate to continue or re-establish their VPN connection. A VPN connectivity request form, with full justification, must be submitted to the IT department for approval.

14.INCIDENT MANAGEMENT

Introduction

The Company shall establish Incident Management Policy and reporting responsibilities and procedures to ensure a quick, efficient and orderly response to incidents. This section shall be read in conjunction with the following documents:

- Incident Management Policy of the Information Security Policy document.

Standards

1. The Company shall establish incident management policies and procedures to ensure quick, efficient and orderly response to incidents.
2. the Company shall define service level agreements (SLAs) and classify incidents based on the priorities and severities of business impact and urgency.
3. the Company shall have an adequate governance structure for incident management and this shall be defined and documented.
4. the Company shall establish procedures to conduct periodic review of reported incidents and the minutes of the review meeting shall be documented.
5. the Company shall establish policies and procedures to manage security incidents.
6. the Company shall use a centralized tool for managing service requests and security incidents.

7. the Company shall establish procedures to ensure that security incidents are reported to the regulators as mandated in the prescribed format.
8. The Information Security Team shall monitor the security incidents reported and appropriate actions taken shall be recorded.

15.ENCRYPTION KEY MANAGEMENT

Introduction

The purpose of encryption key management is to manage keys, which provide the required protection level to maintain the confidentiality, integrity and authenticity of confidential information assets and sensitive application systems of the organization.

Guidelines

1. The Company shall ensure that both symmetric and asymmetric key encryption algorithms are supported. Public Key Infrastructure (PKI) shall be the preferred method for deploying asymmetric key encryption techniques.
2. Use of a particular encryption algorithm to ensure privacy and integrity of information, assets, and/or resources shall be decided by the IT/Network functions in consultation with CTO/CISO.
3. The Company shall ensure that strong encryption protocols like SSLv3/ TLSv1 in strong encryption mode (a minimum of 256 bit or higher symmetric/bulk encryption, 1024 bit or higher public key encryption or one that provides an equivalent strength) is used in all Internet commerce servers.
4. The Company shall ensure that all non-console administrative access are encrypted using SSH v2, or TLS/ SSLv3.
5. The Company shall ensure that standard encryption technologies like WPA2, IPsec VPN or SSL/ TLS are used if information labelled as “Confidential” or “Restricted” is being sent over wireless network.
6. The Company shall ensure that sensitive data is protected by using Strong One-way hashes (e.g. MD5), Triple DES (128bit), AES (256-bit).
7. The Company shall ensure that confidentiality of the shared secret key is protected.

8. The Company shall ensure that a one-time shared secret key is generated only by authorized personnel.
9. The Company shall ensure that the shared secret key is protected against intrusion by logically and physically securing the device on which the key is stored.
10. The Company shall ensure that the shared secret key is accessible only by authorized personnel on a need-to- know basis.
11. The Company shall ensure that pre-shared secret key is of minimum 16 characters in length and includes alpha numeric and special characters.
12. The Company shall ensure that keys are generated afresh in case of suspected compromise.
13. The Company shall ensure that audit trails of key management activities are stored and protected.
14. The Company may, choose to setup its own internal certifying authority (CA) or avail the services of an external provider.
15. The Company shall ensure that internal certifying authority systems are installed and managed securely with appropriate physical and logical controls.
    - the Company as the internal CA shall keep a secure backup of its private keys. The backed-up keys shall be stored in encrypted format and protected from environmental and physical threats. A copy of the backups shall be stored in an off-site location for protection against major failure and/ or disaster.
    - A well-defined and documented procedure shall be established for the issuance of the certificates including user request, user credential verification, certificate approval and user undertaking.
    - The user key pair may be generated by the user or by the Company internal CA.
    - In order to reduce the likelihood of compromise, the certificates shall have a defined activation and deactivation date, so that they are used only for a limited period.
16. the Company shall ensure that secure backup of internal CA private keys is maintained on an independent secure media, which provides a source for key recovery.
17. the Company as an internal CA should decide the validity period of the user certificate.
18. the Company shall ensure that a copy of the backed -up keys is stored at an off-site location for protection against major failure and / or disaster.
19. the Company shall ensure that cryptographic keys are destroyed in a secure manner when they are no longer required.

20. the Company shall ensure that adequate provision is made for different cryptographic keys for different uses and data.
21. the Company shall ensure that split knowledge / dual control (two persons know their parts of the key, to reconstruct the whole key) is required for a cryptographic key to be used, when appropriate.
22. the Company shall ensure that no copy of user's private key is retained by the internal CA to avoid risk of repudiation.
23. the Company shall ensure that that import, export and use of encryption techniques comply with the applicable laws and regulations

PKI - End-user Responsibilities

1. The users shall ensure that their private keys are kept strictly confidential and not available to anyone else including the certifying authority.
2. The users possessing the private keys (in case of public key cryptographic technique) shall be responsible for the safety of the keys.
3. The users shall be accountable and responsible for the transactions and safe maintenance of the digital certificates assigned to them for use.
4. The user shall safeguard the private key by locking with password and/ or by storing on media like smart card that is always under the custody of the user.
5. If there is compromise of private key or if the key is unavailable (because of damage to key storage media), it shall be immediately reported to the registration authority/ CA.
6. The user shall ensure that certificate is renewed before its expiry.
7. The user shall maintain an updated copy of the certificate revocation list to ensure that expired or compromised certificates are not used in transactions.

16.CLOCK SYNCHRONISATION

Introduction

Over time, a computer's clock is prone to drift. The Network Time Protocol (NTP) is one way to ensure system's clock stays accurate. Many services rely on, or greatly benefit from, computers clocks being accurate.

Guidelines

1. The Company Infra Team shall implement hierarchy of Network Time Protocol [here after referred as NTP] Servers for the Company Network.
2. The primary NTP servers shall be synchronized from external authentic NTP servers. Communication between the client and Server shall be authenticated.
3. The correct interpretation of the date/ time format shall be ensured. The format shall be identical across all servers and network devices.
4. Acceptable time slippage at different stratums shall be defined.
5. Laptops shall be configured with NTP client to get the time synchronization on a continuous basis with locations specific NTP Servers.
6. Time Synchronization failure events of primary & secondary servers shall be monitored on a continuous basis.

17.IT BUDGETING AND PROCUREMENT

Introduction

The objective of the IT Budgeting and Procurement Policy is to provide the Company with an efficient and consistent way of budget allocation, procurement and purchasing of assets needed to support its business needs. This procedure establishes the criteria for budgeting, requesting, approving, ordering and receiving assets, as well as tracking orders throughout the entire procurement cycle.

IT Budgeting and Procurement

1. All expenditures at the Company shall be strictly controlled as per planned annual budgets that are allocated under CAPEX and OPEX.
2. The budgets allocated shall be approved and signed off by the Management.
3. Procurement costs shall be tracked and monitored regularly on a quarterly basis for OPEX and CAPEX respectively by the Finance Team, Procurement Team and IT Head/CTO.

Project Cost Tracking

1. Every IT initiative shall be tracked as a project except for items such as production support costs, annual maintenance contracts, printing costs, license renewal costs etc. Cost incurred for various IT projects shall be assessed.
2. A unique project code shall be allocated (arising out of budget guidelines), and the costs invested on hardware, software, application development and services rendered shall be tracked throughout the system.
3. The responsibility for Project cost tracking shall lie with the Budget Controller and Budget tracking team. The Budget Controller shall guide the Budget tracking team.
4. The Budget tracking team shall send a MIS on a quarterly basis to the Budget Controller for review of the project status.

Vendor Management

1. Vendors shall meet the Company requirements and the Company shall take adequate measures to monitor the performance of vendors on a regular basis.
2. Vendors can be classified as One Time vendors (refers to vendors from whom purchases are made only once) and Regular Vendors (vendors with whom purchases are carried out on a regular basis)
3. The Vendor Management Process shall consist of the following sub processes:
    a. Vendor Identification, Selection and Registration: Vendor Identification shall be carried out when the items requested are of a new type and the same cannot be procured from an existing Registered Vendor. Once potential vendors are identified, Vendor Selection shall be carried out by the Procurement Team. The selected vendors shall be further covered under the Vendor Empanelment process defined in the the Company Procurement Policy.
    b. Overall Risk Evaluation: An overall IT risk review process shall be conducted to identify IT relevant security, recovery and operating risks. All new service provider arrangements shall undergo and complete an IT review prior to any contract signing with the vendor. For existing service provider arrangements, the IT review shall be completed on an annual basis for High Risk arrangements and every two years for Medium and Low risk arrangements. For the purposes of this standard, "service provider arrangement" refers to an arrangement with a third-party to supply the Company with systems, software and/or services, which may operate within Company locations or at locations not within the Company premises.

Service Level Agreements

1. For all Company IT requirements, Service Level Agreements shall be included wherever applicable as part of the requirements.
2. Service Level Agreements shall cover the scope of the deliverables and the commitments from various vendors. Necessary penalty clauses shall also be included in the SLAs.
3. The SLA clauses shall be included at the time of floating the Request for Proposal (RFP).
4. In the event that services are offered by vendors for the IT Support and Application Development functions, necessary Non-Disclosure Agreements (NDAs) shall be included as part of the SLAs.
5. All SLAs shall be scrutinized by the respective User Department Heads, IT Heads and vetted and signed by the Legal Head.
6. Inter-departmental IT services shall be covered under Operational Level Agreements (OLAs) which includes
   various services provided by functional groups, and roles and responsibilities.

18.CAPACITY PLANNING MANAGEMENT

Introduction

Capacity Management is the discipline that ensures IT infrastructure is provided at the right time, in the right capacity, at the right price, and used in the most efficient manner. This calls for inputs from many functions of a business to identify what services would be required, the kind of IT infrastructure needed to support these services, the level of contingency and the cost of this infrastructure. Planning is an activity that can be applied to all Capacity Management activities to predict the future utilization of IT Services and Resources.

Planning

1. Management shall ensure than an 'availability plan' is established to achieve, monitor and control the availability of information services. For creating the availability plan, the following steps shall be undertaken, but not limited to:

   a. Identify critical IT resources related to each of the business processes, which need to provide maximum
      availability;
   b. Assess the availability requirement matrix for each resource that should be mandatorily covered.

Demand Management

1. The urgency of the proposed demand modification shall be determined, in response to a demand of IT services.

   a. If there is a direct impact in the delivery of IT services, the urgency would be high and only a short-term action shall be required. This would result in a physical constraint. The implementation of the physical constraint would eventually result in a threshold or alarm, because the short -term physical constraint would have to be solved permanently. When the constraint is implemented, the SLA shall be modified.
   b. When urgency is low, no immediate action is required, thus resulting in advice based on modelling techniques rather than direct action.

Capacity Plan

1. The Capacity Plan shall be analysed and drafted based on information from appropriate sources such as business strategy and plans that provide information on future business growth, IT strategy and plans that provide information on growth required in the IT infrastructure and capacity, SLAs, request from Problem Management or Change Management etc.
2. The information in the Capacity Plan shall be verified and updated on a quarterly basis to take into account changes in business plans, to report on the accuracy of forecasts and to make or refine recommendations.
3. Every year a 'Final' Capacity Plan shall be published in line with the business budget life cycle, and completed before the start of negotiations on future budgets.

4. Services and systems shall be identified to define appropriate monitors and threshold. After the monitors and thresholds are defined, they shall be implemented or modifications shall be made to existing monitors/thresholds. Implementing monitors and thresholds is part of adjusting systems and shall therefore always follow Change Management procedures.
5. After monitoring, thresholds are defined, they shall be monitored against future requirements. The requirements for monitoring shall be matched against the actual monitors and thresholds on a regular basis to accommodate for changes based on business requirements.
6. Management shall ensure that the performance of information technology resources is continuously analysed and exceptions are reported in a timely and comprehensive manner.
7. Based on ongoing monitoring of thresholds/monitors, the management shall continuously tune and implement the monitors/threshold. Tuning activities are activities that result in zero downtime for the users during the agreed service hours; a list shall be maintained by the Change Management process of pre -approved tuning activities.

19.AUDIT LOGGING POLICY

Introduction

A log is a record of the events occurring within an organization's systems and networks. Logs are composed of log entries; each entry contains information related to a specific event that has occurred within a system or network. Logging can give detailed information about any access or change for any of the network resources. Protecting the logs from unauthorized access is extremely important and therefore, it becomes essential to implement necessary controls and ensure that all logs are provided with adequate level of protection.

Guidelines

1. Audit logging shall be enabled on all applicable information systems to track the activities of the user.
2. Log information shall be protected from all unauthorized access and preserved for future reference.

3. IT and Networks functions shall ensure that the audit logs recording the user -activities, exceptions and security events are enabled and stored for reasonable period to assist in future investigations and access control monitoring.
4. Audit trails must be enabled on all servers and network devices for recording exceptions and other security related events. Audit logs recording exceptions and other security -relevant events shall be reviewed and kept for an agreed period to assist in future investigations and access control monitoring.
5. Wherever possible, all audit records should be sent to the central server for monitoring and correlation. If technology of the product does not allow logs to be transferred on real time basis, periodicity for the logs to be transferred from local device to central server shall be defined. Logs shall be monitored and analyzed for any possible unauthorized use of information systems.
6. All audit records shall be maintained as per the requirements provided by relevant regulatory bodies from time to time and archived to assist in future investigations and access control monitoring. A record of successful system access, in addition to rejected attempts, shall be created. At a minimum, audit trails must include the following:
    - User ID's;
    - Dates and times for logon and logoff ;
    - Terminal identity or location if possible ; and
    - Activity Performed
7. Logs should be analyzed on a real time basis or on a defined interval where real time analysis is not possible.
8. In the event of any reported or observed security incident, the person analyzing the logs should support in the investigation by noting and reporting relevant information to the appropriate function .

Categories of Logs

This section describes the categories of logs of particular interest that should be monitored within the Company:

1. Routers- Routers shall be configured to permit or block certain types of network traffic based on an approved policy. Routers that block traffic shall be configured to log only the most basic characteristics of blocked activity.

2. Firewalls- Firewalls shall be configured to track the state of network traffic and perform content inspection. Detailed logs of activity generated from firewalls shall be monitored.
3. Intrusion Detection and Intrusion Prevention Systems- Intrusion detection and intrusion prevention systems record detailed information on suspicious behavior and detected attacks, as well as any actions intrusion prevention systems performed to stop malicious activity.
4. Virtual Private Network- VPN systems shall be configured to log successful and failed login attempts, as well as the dates and times, each user connected and disconnected, and the amount of data sent and received in each user session.
5. Proxy server- Proxies being intermediate hosts through which Web sites, FTP sites etc. are accessed, make requests on behalf of users, and they cache copies of retrieved pages to make additional accesses to those pages more efficient. Proxies shall be configured to restrict user's Web access and to add a layer of protection between Web clients and Web servers. A record of all URLs accessed through proxies shall be maintained and monitored.
6. Anti-Malware Software- The most common form of Anti -malware software is antivirus software, which typically records all instances of detected malware, file and systemdisinfection attempts, and file quarantines. Additionally, antivirus software might also record when malware scans were performed and when antivirus signature or software updates occurred. Anti spyware software and other types of anti malware software (e.g., rootkit detectors) are also common sources of security information. Relevant logs from such anti-malware software shall be decided and monitored
7. Vulnerability Management Software- Vulnerability management software, which includes patch management software and network vulnerability assessment software shall be configured to log the patch installation history and vulnerability status of each host, which includes known vulnerabilities and missing software updates. Vulnerability management software may also record additional information about hosts' configurations.
8. Authentication Servers- Authentication servers, shall be configured to log each authentication attempt, including its origin, username, success or failure, and date and time.

Log management

1. Backup of logs shall be taken on a removable media and shall be maintained for 6 months to assist in future investigations and access control monitoring. Monthly full Backup tape shall be rotated offsite by the Company Infra Team.
2. Random checks shall be carried out on the backup of logs taken to verify the integrity of the logs.
3. Unneeded sensitive information (e.g. Passwords, E -mails etc.) shall not be captured in logs. If such information becomes a part of logs then, it shall be filtered out.
4. Access to Log server shall be controlled by strict password controls. (Refer Password Management, Logical Access Management, Information Security Policy)
5. Log server shall be placed in a secure location with physical and logical access limited to only authorized users.
6. Secure mediums shall be used for remote management of Log server. Secure technology like VPN shall be used for transmission of logs over less secure medium, like Internet

Administrator and Operator Logs

1. Information systems shall be configured in such a way so that the system administrator and system operator activities are logged.
2. CTO shall ensure that system administrator/operator do not edit /delete their logs. The CTO shall review System administrator and operator logs at least once in a week.
3. Logs should include:
    a. The time at which an event (success or failure) occurred;
    b. Information about the event or failure;
    c. Which account and which administrator/operator was involved.

20. CYBER SECURITY

'Cyber security' Means - Preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved

21.IT Governance

a. IT Governance Framework

(a) The key focus areas of IT Governance shall include strategic alignment, risk management, resource management, performance management and Business Continuity/ Disaster Recovery Management.

(b) REs shall put in place a robust IT Governance Framework based on the aforementioned focus areas that *inter alia*:

(i) specifies the governance structure and processes necessary to meet the RE's business/ strategic objectives;

(ii) specifies the roles (including authority) and responsibilities of the Board of Directors (Board) / Board level Committee and Senior Management; and

(iii) includes adequate oversight mechanisms to ensure accountability and mitigation of IT and cyber/ information security risks.

(c) Enterprise-wide risk management policy or operational risk management policy shall also incorporate periodic assessment of IT-related risks (both inherent and potential risk).

b. Role of the Board of Directors

(a) The strategies and policies related to IT, Information Assets, Business Continuity, Information Security, Cyber Security (including Incident Response and Recovery Management/ Cyber Crisis Management) shall be approved by the Board of Directors.

(b) Such strategies and policies shall be reviewed at least annually by the Board.

C.IT Strategy Committee of the Board

(a) REs shall establish a Board-level IT Strategy Committee (ITSC)[1].

(b) While constituting the ITSC, REs shall ensure:

(i) Minimum of three directors as members;

(ii) The Chairperson of the ITSC shall be an independent director and have substantial IT expertise[2] in managing/ guiding information technology initiatives; and

(iii) Members are technically competent[3].

(c) The ITSC shall meet at least on a quarterly basis.

(d) The ITSC shall:

(i) Ensure that the RE has put an effective IT strategic planning process in place;

(ii) Guide in preparation of IT Strategy and ensure that the IT Strategy aligns with the overall strategy of the RE towards accomplishment of its business objectives;

(iii) Satisfy itself that the IT Governance and Information Security Governance structure fosters accountability, is effective and efficient, has adequate skilled resources, well defined objectives and unambiguous responsibilities for each level in the organisation;

(iv) Ensure that the RE has put in place processes for assessing and managing IT and cybersecurity risks;

[1] Foreign banks operating in India through branch mode need not constitute any Committees (Board or Executive level) referred in this Master Direction at the branch level. They may leverage upon controlling office/ head office/ regional/ zonal Committees for compliance with this Master Direction as long as governance obligations / responsibilities outlined for the prescribed committees are met.

[2] "Substantial IT expertise" means the person has a minimum of seven years of experience in managing information systems and/or leading/ guiding technology/ cybersecurity initiatives/ projects. Such a member should also understand the business processes at a broader level and the impact of IT on such processes.

[3] Technically competent herein will mean the ability to understand and evaluate information systems and associated IT/ cyber risks.

(v) Ensure that the budgetary allocations for the IT function (including for IT security), cyber security are commensurate with the RE's IT maturity, digital depth, threat environment and industry standards and are utilised in a manner intended for meeting the stated objectives; and

(vi) Review, at least on annual basis, the adequacy and effectiveness of the Business Continuity Planning and Disaster Recovery Management[4] of the RE.

d.. Senior Management and IT Steering Committee

(a) The Senior Management of the RE shall, *inter alia,* ensure:

(i) Execution of the IT Strategy approved by the Board;

(ii) IT/ IS and their support infrastructure are functioning effectively and efficiently;

(iii) Necessary IT risk management processes are in place and create a culture of IT risk awareness and cyber hygiene practices in the RE;

(iv) Cyber security posture of the RE is robust; and

(v) Overall, IT contributes to productivity, effectiveness and efficiency in business operations.

(b) REs shall establish an IT Steering Committee with representation at Senior Management level from IT and business functions.

(c) The responsibilities of IT Steering Committee, *inter alia,* shall be to:

(i) Assist the ITSC in strategic IT planning, oversight of IT performance, and aligning IT activities with business needs;

[4] The reference to Business Continuity/ Disaster Recovery Management in this Master Direction is limited to operational resilience focussing on People, Processes and Systems associated with the IT, IS, information/ cyber security controls and operations.

(ii) Oversee the processes put in place for business continuity and disaster recovery;

(iii) Ensure implementation of a robust IT architecture meeting statutory and regulatory compliance; and

(iv) Update ITSC and CEO periodically on the activities of IT Steering Committee.

(d) The IT Steering Committee shall meet at least on a quarterly basis.

e. Head of IT Function

(a) REs shall appoint a sufficiently senior level, technically competent and experienced official in IT related aspects as Head of IT Function[5].

(b) The Head of IT Function shall, *inter alia*, be responsible for the following:

(i) Ensuring that the execution of IT projects/ initiatives is aligned with the RE's IT Policy and IT Strategy;

(ii) Ensuring that there is an effective organisational structure to support IT functions in the RE; and

(iii) Putting in place an effective disaster recovery setup and business continuity strategy/ plan.

(c) As a first line of defence, the Head of IT Function shall ensure effective assessment, evaluation and management of IT controls and IT risk, including the implementation of robust internal controls, to (i) secure the RE's information assets (ii) comply with extant internal policies, regulatory and legal requirements on IT related aspects

f. Controls on Teleworking

In the teleworking environment, REs, *inter alia*, shall:

[5] By whatever name called viz. Chief Technology Officer or Chief Information Officer, etc.

(a) Ensure that the systems used and the remote access from alternate work location to the environment hosting RE's information assets are secure;

(b) Implement multi-factor authentication for enterprise access (logical) to critical systems;

(c) Put in place a mechanism to identify all remote-access devices attached/ connected to the RE's systems; and

(d) Ensure that data/ information shared/ presented in teleworking is secured appropriately.

22. IT and Information Security Risk Management

g.Periodic review of IT related risks

The risk management policy of the RE shall include IT related risks, including the Cyber Security related risks, and the Risk Management Committee of the Board (RMCB) in consultation with the ITSC shall periodically review and update the same at least on a yearly basis.

22. IT and Information Security Risk Management Framework

REs shall establish a robust IT and Information Security Risk Management Framework[6] covering, *inter alia,* the following aspects:

(a) Implementation of comprehensive Information Security management function, internal controls and processes (including applicable insurance covers) to mitigate/ manage identified risks. The implemented controls and processes must be reviewed periodically on their efficacy in a risk environment characterised by change;

[6] REs may have flexibility to define Information / Cyber security risk management framework distinct from IT risk management framework.

(b) Definition of roles and responsibilities of stakeholders (including third-party personnel) involved in IT risk management. Areas of possible role conflicts and accountability gaps must be specifically identified and eliminated or managed;

(c) Identification of critical information systems of the organisation and fortification of the security environment of such systems; and

(d) Definition and implementation of necessary systems, procedures and controls to ensure secure storage/ transmission/ processing of data/ information.

23. Information Security Policy and Cyber Security Policy

(a) The Information Security Policy shall take into consideration, *inter alia*, aspects such as the objectives, scope, ownership and responsibility for the Policy; information security organisational structure; exceptions; compliance review and penal measures for non-compliance of Policies. REs shall also put in place a Cyber Security Policy and Cyber Crisis Management Plan (CCMP).

(b) An Information Security Committee (ISC), under the oversight of the ITSC, shall be formed for managing cyber/ information security. The constitution of the ISC, with Chief Information Security Officer (CISO) and other representatives from business and IT functions, etc., shall be decided by the ITSC. The head of the ISC shall be from risk management vertical. Major responsibilities of the ISC, *inter alia*, shall include:

(i) Development of information/ cyber security policies, implementation of policies, standards and procedures to ensure that all identified risks are managed within the RE's risk appetite;

(ii) Approving and monitoring information security projects and security awareness initiatives;

(iii) Reviewing cyber incidents, information systems audit observations, monitoring and mitigation activities; and

(iv) Updating ITSC and CEO periodically on the activities of ISC.

(c) A senior level executive (preferably in the rank of a General Manager or an equivalent position) shall be designated as the Chief Information Security Officer (CISO). The CISO shall not have any direct reporting relationship with the Head of IT Function and shall not be given any business targets. REs shall ensure the following:

(i) The CISO has the requisite technical background and expertise;

(ii) She/He is appointed for a reasonable minimum term;

(iii) The CISO's Office is adequately staffed with people having necessary technical expertise, commensurate with the business volume, extent of technology adoption and complexity; and

(iv) The budget for the information/ cyber security is determined keeping in view the current/ emerging threat landscape.

(d) REs shall ensure that the roles and responsibilities of the CISO are clearly defined and documented covering, at a minimum, the following points:

(i) The CISO shall be responsible for driving cyber security strategy and ensuring compliance to the extant regulatory/ statutory instructions on information/ cyber security.

(ii) The CISO shall be responsible for enforcing the policies that a RE uses to protect its information assets apart from coordinating information/ cyber security related issues within the RE as well as with relevant external agencies.

(iii) The CISO shall be a permanent invitee to the ITSC and IT Steering Committee.

(iv) The CISO's Office shall manage and monitor Security Operations Centre (SOC) and drive cyber security related projects.

(v) The CISO's office shall ensure effective functioning of the security solutions deployed.

(vi) The CISO shall directly report to the Managing Director or equivalent executive overseeing the risk management function; and

(vii) CISO shall place a review of cyber security risks/ arrangements/ preparedness of the RE before the Board/ RMCB/ ITSC atleast on a quarterly basis.

MANAPPURAM
ASSET FINANCE LIMITED