ABANS FINANCE PRIVATE LIMITED

IT POLICY

Adoption/Amended	Authority	Date
Adoption	Board of Directors	September 18, 2018
Revision	Board of Directors	January 29, 2025

INDEX

1. POLICY STATEMENT AND PURPOSE

Abans Finance Private Limited ('AFPL' or 'the Company') is a Material Subsidiary of Abans Holdings Limited. Since March 31, 2024, it has been categorized as a Middle Layer NBFC (NBFC – ML), pursuant to the scale-based regulation put forth by the Reserve Bank of India (RBI. This policy is made in accordance with IT Framework which is issued by the RBI and the same shall be subjected to the changes and amendments as per the revisions as and when carried out by the RBI.

The purpose of this policy is to establish standards for the configuration, management, and continuity of IT Operations (Network and Server) Assets owned and/or operated by AFPL. This policy aims to minimize unauthorized access, ensure business continuity, and manage changes effectively to protect AFPL's sensitive, critical, proprietary information and technology.

This policy encompasses the following sub-policies:

1. IT Framework Policy
2. Business Continuity and IT Disaster Recovery Policy
3. IT Change and Release Management Policy
4. Information and Cyber Security
5. IT and IS Audit Policy

The purpose of the information technology policy is to protect the Company's information assets from all threats, internal or external, deliberate or accidental, ensure business continuity, and prevent information security breaches. The IT Policy will be reviewed periodically.

2. SCOPE

This policy applies to all IT Operation assets owned or operated by AFPL, including those registered under any AFPL internal network domain. It covers all users, including third parties with access to AFPL's IT assets, and applies to changes in the production environment of IT applications and IT infrastructure.

INFORMATION TECHNOLOGY FRAMEWORK POLICY

1. PURCHASING NEW SYSTEMS

1.1) Requirement of New System

- Purchases of new system hardware or components for existing systems must comply with the Company's Procurement policies and current technical standards.
- Purchase requests must be based on User Requirements and consider long-term organizational business needs.
- Except for minor purchases, hardware must be acquired through a structured evaluation process, including the development of detailed Request for Proposal (RFP) or Request for Information (RFI) documents. Information Security features and requirements must be identified within the RFP or RFI.
- All requests for major new application systems or software enhancements must be presented to management with a Business Case.

1.2) Implementation

- All new hardware installations must be formally planned. Thorough testing should be conducted for system requirements and features before going live.
- The implementation of new or upgraded software must be carefully planned and managed, ensuring that increased Information Security risks are mitigated using a combination of procedural and technical control techniques.
- Decisions to upgrade software should be made after considering the associated risks and weighing them against the anticipated benefits.
- The IT team should devise ways to manage identified security or fraud risks, either by designing countermeasures, transferring the risk to a third party, or accepting the risk.
- Employees are not allowed to install or implement any additional software without permission from the IT Team.

1.3) Issuing Laptops/Portable Computers

- Management must authorize the issuance of portable computers. Usage is restricted to business purposes, and users must be aware of and accept the terms and conditions of use, especially the responsibility for the security of information held on such devices.
- Employees issued with portable computers for business travel must be made aware of information security issues related to portable computing and implement appropriate safeguards to minimize risks.

- Laptops are to be issued to and used only by authorized employees and only for the purposes for which they are issued. Information stored on the laptop must be suitably protected at all times.

1.4) Business & Office Software Packages

- The organization should generally avoid selecting business-critical software that has not been adequately proven by early adopters. The selection process for all new business software must incorporate criteria approved by management.
- All office software packages must be compatible with the organization's preferred and approved computer operating system and platform.
- To comply with legislation and ensure ongoing vendor support, the terms and conditions of all end-user license agreements must be strictly adhered to.

1.5) Patches and Hot Fixes

- Patches to resolve software bugs may only be applied where verified as necessary. They must be from a reputable source and thoroughly tested before use.
- Security patches should be updated on applicable computing systems such as desktops, laptops, and servers.

1.6) Vendor Performance Review Procedure

- The Company will follow the necessary call logging procedure to record system issues in the Vendor call logging system or Helpdesk system.
- The Vendor performance report will be reviewed internally, and any issues with vendor performance or service delivery will be highlighted.
- Periodic review meetings will be scheduled to discuss pending issues or support performance with the vendor. Confirmation from the vendor will be obtained to resolve open issues within a specified timeframe.
- Minutes of meetings will be documented and mutually recorded between the Company and the Vendor.
- Escalation of unresolved issues will follow the escalation procedure defined by the Vendor.
- If the Vendor fails to deliver service support or resolve issues despite discussions in review meetings, the Company will issue a warning to the Vendor at the highest level of escalation.
- If the Vendor still fails to resolve the issue or deliver support, a penalty will be levied as defined in the service level agreement.
- If the Vendor continues to fail in improving service despite penalties, the Company will find alternate Vendor support and issue a termination notice to the first vendor as per the terms defined in the Service Level Agreement.

2) SECURITY

The handling of very sensitive and confidential data should be governed by necessary security parameters. The appropriate measures must be used to ensure confidentiality, integrity and availability of information.

2.1) Securing Data

- Prior to sending information to third parties, not only the intended recipient be authorized to receive such information, but the security measures adopted by the third party must be seen to continue to assure the confidentiality and integrity of the information.

- All data and information must be protected against the risk of fire damage at all times. The level of such protection must always reflect the risk of fire and the value and classification of the information being safeguarded.

- Sensitive financial information is to be classified as highly confidential and security measures must be afforded (technology and procedural) which, in combination, safeguard such information from authorized access and disclosure.

- Data is to be protected against unauthorized or accidental changes and may only be deleted with the proper authority.

- Sensitive / confidential electronic data and information should be secured, whenever possible, with access control applied to the directory on the system concerned. The sole use of passwords to secure individual documents is less effective, and hence discouraged, as passwords may either be forgotten or become revealed (over time) to unauthorized people.

- Sensitive or valuable material and equipment must be stored securely and according to the classification status of the information being stored. The Documents are to be stored in a secure manner in accordance with their classification status.

- An Uninterruptible Power system is to be installed to ensure the continuity of services during power outages. Secondary & backup power generators are to be employed where necessary to ensure the continuity of services during power outages.

2.2) Managing Access Control Standards

- Access control standards for information systems must be established by management and should incorporate need-based access to prevent unauthorized access.

- Access Controls are to be set at an appropriate level which minimizes information security risks yet also allows the organization's business activities to be carried without undue hindrance.

- Access to all systems must be authorized by the concern Department head, IT head and such access, including the appropriate access rights (or privileges), must be recorded in an access control list. Such records are to be regarded as highly confidential documents and safeguarded accordingly.

- Access to operating system commands is to be restricted to those people who are authorized to perform system administration/management functions
- Access is to be logged and monitored to identify potential misuse of systems or information.
- Access to information and documents is to be carefully controlled, ensuring that only authorized personnel may have access to sensitive information.
- The physical access of server systems residing in the Company's datacenter should restricted to concerned administrator and supervisor managing the server systems only. Any temporary access should be authorized by Departmental Heads & concerned Data center manager or IT Infrastructure head.
- A quarterly review should be done of the access rights of application systems. The list of such rights should be circulated to concerned user's departmental heads.
- The department head should review and send updated user list with necessary corrections to IT application owner,
- In the absence of feedback from the department head, an escalation should be made to concerned Business Head reporting if department head fails to respond with acknowledgement.
- After obtaining the feedback from Department Head or Business Head a necessary correction of access rights should be done in the systems and the same should be informed User department head or Business head.
- All the Company's Employees should abide by the IT Policy by signing their a copy of the policy and a Non-Disclosure-Agreement to safeguard Information leaks.

2.3) Passwords Policy

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of organization network. As such, all employees (including contractors and vendors with access to systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. The scope of this policy includes all personnel who have or are responsible for a user account (or any form of access) on any system that resides within organization.

- The minimum password length should be of 8 characters.
- No blank passwords are permissible.
- The validity of Password age will be 30 days.
- The Password history to be remembered for the last 6 passwords.
- The Password lockout after 3 bad logons.
- The Lockout account to be released after 30 minutes.

- If account is not used for more than 45 days, then the same has to be brought to the notice of Department Head and based on his recommendation the same has to be deleted or kept disabled.

- Passwords must not be inserted into email messages or other forms of electronic communication.

- Employees should not share his/her password with anyone. Employees should note that activity done on an individual's password is the responsibility of the person concerned, and he/she is accountable for the same. Sharing of password for reason whatsoever cannot be treated as an excuse.

- All Systems and Application should be governed by Password Policy. Any System which deviates from Password Policy should be approved as Exemption approved by Management.

- The Administrator & equivalent password must be kept in a sealed envelope and placed in fireproof storage.

- The Administrator password is not to be used for day-to-day administration operation. An Administrator equivalent to be used for day-to-day operation

- It is strongly recommended that password should be unique and should not have any Resemblance to common personal information e.g. your name / spouse's name / telephone no. / Vehicle no. / Date of birth etc. Moreover, avoid writing down your password specifically at most obvious & visible Places like calendar on your desk, diary, scratch pad etc. Do not email / sums / print your passwords.

2.4) Network Security

- Security must be considered as a key component of all network design activities.

- Appropriate filters must guarantee that only authorized traffic will flow between network domains.

- Network monitoring software tools must be used to trigger alarms, alerting the company when suspicious activity occurs.

- All the network designs and configurations must be documented.

- All connections from external networks to internal company networks will be protected by gateways systems and only authorized services should be allowed. Rest all traffic should be denied.

- Only equipment which has been approved and authorized by IT will be permitted to be connected to the network.

2.5) Antivirus Protection

- All Windows computers (clients and servers) except Trading Environment Servers and Clients connected to the Computer Network resources shall have antivirus software (preferably the most

current version) correctly installed, configured, activated, and updated with the latest version of virus definitions before or immediately upon connecting to the network.

- Employees must not disable or otherwise change anti-virus software on a workstation, laptop or any other system without specific authorization.

- The Central gateways must have virus scanning software installed.

- If deemed necessary to prevent viral propagation to other networked devices or detrimental effects to the network, computers infected with viruses or other forms of malicious code (herein collectively referred to as "virus" or "viruses") shall be disconnected from the network until the infection has been removed.

- If a Windows computer does not have antivirus software installed, it should be installed before establishing any connection to the network. Upon establishing the initial network connection, the virus definitions shall be updated to the most current version immediately and before loading or installing any other software or data.

- Virus definitions should be updated in a scheduled manner to all windows computers.

- All files on all hard drives should be scanned weekly.

- When an enterprise-wide virus attack is in progress, a notification to the campus computing community via the best available method and all files on all hard drives should be scanned immediately using the newest virus definitions available.

- Other operating systems or computing platforms shall have comparable protection, if available. In the event that no antivirus protection is available for a particular operating system or platform, anyone using or accessing these unprotected systems shall apply all prudent security practices to prevent infection, including the application of all security patches as soon as they become available. When antivirus software becomes available for an operating system or platform previously lacking antivirus software, it should be installed on all applicable devices connected to the network.

2.6) Remote Access

- Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. The Remote access grant must strictly control.

- Off-site computer usage, whether at home or at other locations, may only be used with the authorization of Head of Department and Head of IT.

- Usage should be restricted to business purposes, and users must be aware of and accept the terms and conditions of use, which must include the adoption of adequate and appropriate information security measures.

- The remote access to third party support personnel will be confined on the Data Network to only the system that they are supporting.

- The remote access must be logged, and adequate amount of information must be captured to assist with investigations and to detect misuse of the remote access service.

2.7) Desktop Policy

- All local sharing should be password protected with authorized access.
- A User should not store explicit material and games in the local drive of the PC.
- An audit is to be made at a regular interval to check if any explicit material is stored in the local drive.
- The user should not be allowed to change any local configuration of the PC such as Computer Names, Workgroup name or Networking configuration of the PC.
- The user should not be allowed to load any unauthorized or illegal program into local desktop. All the software on the local PC should have a proper authorized license.
- The use of removable media disks, e.g. disks and CD-ROMS should not permit except where specifically authorized. Employees are not allowed to use external sources of information without the permission of IT, like floppies, disks (CDs, DVDs, and DLT etc).
- The temporary files on users PC and laptops are to be deleted regularly to prevent misuse by possible unauthorized users.
- The local administrative access to users PC will be restricted Helpdesk Administrations.
- The Desktop needs to be safeguarded appropriately with Screen saver especially when left unattended.
- Employees should protect the provided IT tools like desktops /laptops / assets etc. from being misused and damaged.

2.8) Network Shares Access

- All the File and Print Shares on the network should be maintained by the administrator and access should be given with necessary approval by function head and IT head.
- All Network Share will have restricted access to users based on requirement. The level of Access to be defined based on requirement. All Sharing of information must have proper password protection.
- Access to the resources on the network (Server, Desktops & other systems) and must be strictly controlled to prevent unauthorized access. Access to all computing and information systems and peripherals shall be restricted unless explicitly authorized.

2.9) Users Login

- The creation of user id should be done after having a user request form being duly approved by the Department head and IT Infrastructure Manager.

- The creation of new user should follow all password policy parameters.
- The user should get option to change the same at first logon.
- The deletion of user id should be done for a user resigning from the company.
- Guest accounts to be kept locked.
- If contract employees require a user IDs. Then it should be remarked indicating a contract user ID. All the contract / Temporary/ guest / consultant IDs will be valid as per required time frame only. These IDs should expire automatically. If such ids are required again then renewal requisition has to be raised.
- The concern IT Head would be responsible for maintaining the security of guest ids.
- All user IDs creation should be based on approvals from functional head and IT head.
- The Guest ids as per required business process under following consideration:
    - Guest IDs for Consultant doing project development/testing etc.
    - Guest IDs for Data entry operators.
    - Guest IDs for Web Cafe PC for surfing the internet.
    - Guest IDs for Customers email correspondence.

2.10) Audit

- Auditing should be enabled for Unsuccessful full logons, User and group management, Rights management and policy changes.
- The error logs must be properly reviewed and managed.
- An auditing should be done for administrative access or for the change in the application system.
- An Audit trail of activities on the network must be maintained to ensure that an adequate amount of information can be captured to assist with investigations to detect misuse of network.
- Audit trail log should be examined on a regular basis to determine if unauthorized or suspicious activity has taken place.

2.11) Hardware movement

- Any movement of hardware between the organization's locations is to be strictly controlled by Manager-IT Infrastructure. Only authorized personnel are permitted to take equipment belonging to the organization off the premises; they are responsible for its security at all times.
- All the hardware movement should have proper approval from IT and Security staff.

2.12) Corporate Website

- The Corporate website is an important information resource of the organization. Its safety from unauthorized intrusion should govern all security concerns. The authorized person should have access to change the information on the web site. The same should be documented.

2.13) Hardening

- The hardening of the server system should be done as stated in Server Hardening Policy.
- The hardening of the network system should be done as stated in Network Hardening Policy.

3) SYSTEM OPERATION & ADMINISTRATION

3.1) System Operations and Administration

- The organization's systems are to be managed by a suitably qualified systems administrator who is responsible for overseeing the day-to-day running and security of the systems.
- For authorized personnel, the appropriate data and information must be made available as and when required; for all other people, access to such data and information is prohibited with appropriate technical control required to supplement the enforcement of this policy.
- Third party access to corporate information is only permitted where the information is asked for and the risk of possible unauthorized access is considered to be negligible.
- The organization's systems must be operated and administered using documented procedures in a manner which is both efficient but also effective in protecting the organization's information security.
- System documentation is a requirement for all organization's information systems. Such documentation must be kept up to date and be available.
- System logs and operational audit logs must be properly reviewed and managed by qualified staff and discrepancies reported to the owner of the Information system.
- System Operations schedules/checklist is to be formally adhered to.
- Changes to routine systems operations are to be fully tested and approved before being implemented.

3.2) System Maintenance

- The system changes and Maintenance policy & procedures should be defined and documented.
- All the Maintenance procedure should be planned and executed regularly.
- The Maintenance plan should be approved by Head of Department and user department head.
- The Maintenance report should be prepared and documented.

3.3) Data Management

- Sensitive or confidential data / information, may only be transferred across networks, or copied to other media, when the confidentially and integrity of the data can be reasonably assured.
- Day-to-day data storage must ensure that current data is readily available to authorized users and that archives are both created and accessible in case of need.
- The integrity and stability of the organization's databases must be maintained at all times.
- Emergency data amendments may only be used in extreme circumstances and only in accordance with emergency amendment procedures.
- The classification of spreadsheets must be appropriate to the sensitivity and confidentiality of data contained therein. All financial / data models used for decision making are to be fully documented and controlled by the information owner.
- The database must be fully tested for both business logic and processing prior to operational usage. Where such databases are to contain information of a persona nature, procedures and access con controls must ensure compliance with the necessary legislation.
- Version control procedures should always be applied to documentation belonging to the organization or its customers.
- The naming of the organization’s data files must be meaningful and capable of being recognized by its intended users.
- Customer Information may only be updated by authorized personnel. Customer data is to be safeguarded using a combination of technical access controls and robust procedures, with all changes supported by journals and internal audit controls.
- Customer contact information is to be classified as confidential and secured accordingly.
- All users requires them to create or amend data files, must save their work on the system regularly in accordance with best practice, to prevent corruption or loss through system or power malfunction.

3.4) Backup, Recovery and Archiving

- Information system owners must ensure that there are adequate backup and system recovery procedures and in place.
- Information and data stored on laptops or portable computers must be backed up regularly. It is the responsibility of the user to ensure that this takes place on a regular basis.
- The storage media used for the archiving of information should be appropriate to its expected longevity. The format in which the data is stored must be carefully considered, especially where proprietary formats are involved.

- Management must ensure that safeguards are in place to protect the integrity of data files during the recovery and restoration of data files; especially where such files may replace more recent files.
- The Backup guidelines defined in the Backup should be followed by all systems.
- A System backup specification should be documented for all respective application.
- The backup media should have proper labeling defined.
- The backup media should be store in a offsite location in a fire proof safe.
- The access of backup should be restricted to concern authorized people only.
- The Backup log should be maintained.
- The archiving backup of information must take place with due considerations for legal, regulatory and business issues with liaison between technical and business staff. The information retained for a minimum period that meets legal and business requirements.
- At a regular interval a restoration test should be carried out for all backed up data on media by restoring a sample data.

3.5) Monitoring

- The Business Critical system should have proper Monitoring system to assure uptime of system.
- A Monitoring procedure should be developed.
- Any new product or business system will be monitored for fraud and security breaches on an ongoing basis as appropriate.

4) SOFTWARE CONTROL

4.1) Software Control

- When a new product or business system is being developed, or subsequently enhanced, a through review of fraud and security risks should be conducted.
- Program listing must be controlled and kept fully up to date at all times.
- Vendor developed software must meet the user requirement specification and offer appropriate product support.
- Developing Interfacing software systems is a highly technical task and should be undertaken in a planned and controlled manner by properly qualified personal.

- All application software must be provided with the appropriate level of technical support to ensure that the organization's business is not compromised by ensuring that any software problems are handled efficiently with their resolution in an acceptable time.

4.2) Testing and Training

- The use of live data for testing new system or system changes may only be permitted where adequate controls for security of the data are in place.

- New systems must be tested for capacity, peak loading and stress testing. They must demonstrate a level of performance and resilience which meets or exceeds the technical and business needs and requirements of the organization.

- Normal system testing procedures will incorporate a period of parallel running prior to the new or amended system being acceptable for use in the live environment. The result of parallel running should not reveal problems or difficulties which were not previously passed during user acceptance testing.

- Where practicable the new product or business system will be tested to ensure all risks are identified and countermeasures are in place prior a launch date.

- A Test strategy should be built up and testing will be done in staging system for the application having test environment. If the test result fails, then a further mitigation plan should be formed to eliminate these test failures.

- The success results of the test strategy should lead to build a plan to implement the new version of change configuration or executable.

- Training is to be provided to uses and technical staff in the functionality and operations of all new systems.

4.3) Documentation

- Documentation is a must for :

- All Servers (Hardware + Software)
- All Routers (Hardware + Configuration)
- Entire Network Layout.
- Server Closet Wiring.
- All Telecom Links.
- Switches (Hardware + Configuration)
- Begin of the Day Processes for all Application Servers.
- End of the Day Activities for all application Servers.

The above documentation is to be updated as and when a change occurs in the IT Environment. All new and enhanced systems must be fully supported at all times by comprehensive and up to date documentation.

New systems or upgraded systems should not be introduced to the live environment unless supporting documentation is available.

5) Risk Assessment Purpose

Risk assessment is conducted to identify the risks and assess the possible damage that would be caused in order to justify the security controls.

A risk is the probability of a threat agent, exploiting vulnerability in the current environment and creating damage to the information assets of an organization. Risk assessment exercise is the key activity which would help identify the applicable controls for an organization.

5.1 Objectives

- Enhance business performance by informing and improving decision making and planning
- Promote a more innovative, less risk averse culture which encourages the taking of calculated risks in pursuit of opportunities to benefit the organization
- Provide a sound basis for integrated risk management and internal control as components of good corporate governance
- Increase the likelihood of achieving the organization's aims, objectives, and priorities
- Prioritize the allocation of resources
- Give an early warning of potential problems
- Provide everyone with the skills to be confident risk takers

5.2 Audience

All employees have a responsibility for maintaining good internal control and managing risk in order to achieve personal, team and corporate objectives. Collectively, all employees need to have the appropriate knowledge, skills, information and authority to establish, operate and monitor the system of internal control. This requires an understanding of the organization, its objectives, the risks it faces and the people we deal with. Everyone should be aware of the risks they are empowered to take, which should be avoided and which reported upwards.

5.3 Scope

The risk assessment exercise involves valuating the information assets, identifying the threats to the asset, identifying the vulnerabilities in the information assets and system and finally prioritizing risks based on its impact, and probability of occurrence.

1. Identify Risk Assessment Participants
2. Information Asset Analysis
3. Threat Assessment

4. Identify Vulnerabilities

5. Risk Tolerance

5.4 Identify Risk Assessment Participants

For each application or process, develop a matrix to list down the risk assessment participants. This list of participants also includes members from Interdependent processes as well as external customers or business partners of the Company's as the need may be.

2) Information Asset Analysis

Asset Analysis primarily consists of three sub-processes. They include:

a. Asset Identification

Assets to be identified include information assets, software assets, physical assets, service assets and paper assets. These assets would be grouped under their corresponding processes, for effectively conducting the risk assessment.

b. **Asset Classification**

Every Asset must be classified according to the perceived importance of the asset within the organization and/or the value of the asset to the competition.

c. Asset Valuation

Asset Valuation is primarily obtained to determine the safeguards/controls to be used for the protection of the asset. Some of the parameters that have to be taken into consideration while determining the value include:

- Cost of procuring the asset
- Cost of maintenance of the asset
- Value of the information held by asset to business
- Value of the asset to the competition
- Business Impact Analysis for the asset and so on

d. Business Impact Analysis

In this analysis, the business value of the asset is of prime consideration. The business value of the asset is the tangible loss incurred by the organization when the asset is unavailable. It is imperative, that a company will incur intangible losses also, which will be covered under the qualitative risk assessment.

3) Threat Assessment

The core activity in this phase is to identify threats to assets. In order to identify the threats a pre - threat analysis interview needs be conducted with asset owners to understand the following:

- Access Controls

- Details of the Change Control procedures
- General day-to-day administration activities
- Backup and Recovery Procedures
- System Documentation and Process Manual Security
- Disciplinary activities
- Incident Response Procedures
- Email and Internet Usage mechanisms
- Use of encryption and so on.

Depending on the nature of the asset, the datasheet lists the threats that could harm and, thus adversely affect critical operations and assets of the Company's . Threats agents include intruders, criminals, terrorists, and natural disasters. Additionally, the threats inside and outside the control of the organization are determined in this phase.

4) Identify Vulnerabilities

Threats materialize because of the vulnerabilities in the process/the system. Additionally, the supporting IT infrastructure of the Company's will be assessed for possible vulnerabilities, using sophisticated tools and techniques. These tools would be deployed from various segments of the network on the target environment to launch network based and operating system-based exploits to uncover all the security holes in the target environment.

5) Risk Tolerance

The organization's tolerance towards Acceptable Risks can be defined in reference to the following components:

- All personnel should be willing and able to take calculated risks to achieve their own and the organization's objectives and to benefit the organization. The associated risks of proposed actions and decisions should be properly identified, evaluated and managed to ensure that exposures are acceptable
- Within the organization, particular care is needed in taking any action which could:
- Impact on the reputation of the organization
- Impact performance
- Undermine the independent and objective review of activities
- Result in censure/fine by regulatory bodies
- Result in financial loss

- Any threat or opportunity which has a sizeable potential impact on any of the above should be examined, its exposures defined, and it should be discussed with the appropriate line manager. Where there is significant potential impact and high likelihood of occurrence it should be referred to the management

- Organizational policies and guidance manuals define where there are mandatory processes and procedures, e.g., the Equal Opportunities Policy, etc. Full compliance with these standards is required and confirmation of compliance will be sought in the annual Certificates of Assurance process. Non-compliance with prescribed procedures constitutes an unacceptable risk

- Some risks are acceptable provided the prescribed organizational process is followed, e.g. expenditure proposals, staff recruitment, and designated responsibilities/authorities are adhered to

Risk Assessment Policy

All risk management activities will be aligned to corporate aims, objectives and organizational priorities, and aims to protect and enhance the reputation and standing of the organization. Risk analysis will form part of organizational strategic planning, business planning and investment/project appraisal procedures. Risk management will be founded on a risk-based approach to internal control which is embedded in day-to-day operations of the organization.

Guidelines

- Our risk management approach will inform and direct our work to gain an assurance on the reliability of organizational systems and will form the key means by which the Board gains its direct assurance

- Managers and staff at all levels will have a responsibility to identify, evaluate and manage or report risks, and will be equipped to do so

- Risk Management in the organization should be proactive and reasoned. Corporate and operational risks should be identified, objectively assessed, and, where this is the appropriate response, actively managed

- The aim is to anticipate, and where possible, avoid risks rather than dealing with their consequences. However, for some Key areas where the likelihood of a risk occurring is relatively small, but the impact on the organization is high, we may cover that risk by developing Contingency Plans, example our Business Continuity Plans. This will allow us to contain the negative effects of unlikely events which might occur

- In determining an appropriate response, the cost of control/risk management, and the impact of risks occurring will be balanced with the benefits of reducing risk. This means that we will not necessarily set up and monitor controls to counter risks where the cost and effort are disproportionate to the impact or expected benefits

• We also recognize that some risks can be managed by transferring them to a third party, for example by contracting out, Public Private Partnership arrangements, or possibly, but unlikely for our organization, by insurance

6) Problem Management Objective

The Company's IT Problem management policy helps to assist in the timely resolution of problems that end users may be experiencing with networked IT systems and Applications. They also assist IT personnel in the discovery of trends where additional training for user or IT personnel may be required, and global issues where IT may be able to proactively resolve those issues in a timely manner. Lastly, problem resolution policy and procedures facilitate communication and escalation in a critical situation.

Scope

Problem resolution policies are applied to the The Company IT environment where Applications are actually used to conduct The Company Business Operations.

Definitions

The Problem Resolution and Process Roles & definitions are as under

• End Users - Any User of any application working in the Trading/BackOffice environment.

• Helpdesk - An IT Helpdesk where user can report his/her problem

Level 1 - A First level technical support.

Level 2 - A Second Level technical support.

Level 3 - A Extended Level technical support or expertise or vendor

• Severity l - Critical. A department or the company as a whole cannot perform business as usual, or the non-resolution of the problem would lead to a department or the company not being able to perform business as usual. These problems will be addressed immediately and worked until resolved. Communication with the end user(s) occurs every hour during the resolution process and is immediate upon resolution of the problem to let the end user(s) know that the problem has been resolved and any actions that need to occur by the end user(s) to resume operation.

• Severity 2 - Major. The user is unable to perform some function, and a work around is difficult. Department business can go on as usual. Response is within 24 hours and the schedule for the fix is negotiated with the user. Communication to the end user(s) is within 24 hours to let the user know that the support person is working on the problem, as needed during the resolution process, and immediately after the problem is resolved to let the user know that the problem has been resolved any whether or not the end user needs to take any action to resume operation.

• Severity3 - Minor. There is a workaround available or the problem is aesthetic in nature. There is no guaranteed service level for Severity 3 problems. The support person should communicate to the end user as needed and within 24 hours after the problem has been resolved to let the enduser knows the problem has been resolved and whether or not the end user needs to take any action to resume operation in the fixed environment.

Problem Management Policy

- When a problem is experienced, the end user should first contact the IT Team.
- The IT Team personnel should log and document the problem in the Problem tracking/sheet or Module. The IT Team should assign the call to Level 1 support who then work with the user to determine if the problem and can be resolved immediately without further escalation and if so, resolve the problem.
- If the Level 1 cannot resolve the problem, they should determine the severity of the problem and escalate to level 2 support people is to which the problem should be routed.
- The problem should then be routed to the appropriate level 2 support person. Immediately after getting level 2 contacts in person and handing off the problem, the IT Team personnel should send out a notification of a Severity 1 Problem via email to, the VP, Dir IT and Dir Ops including the Function Manager.
- The Level 2 support person should work with the end user to resolve the problem according to the defined severity level. The level 2 support person may determine in this process that the defined the severity of the problem is not the actual severity and with end user agreement, change the severity and respond appropriately.
- If the Level 2 support person cannot resolve the problem, they should contact the Level 3 support personnel according to procedures for resolving application problems. It is the responsibility of the Level 2 support person to work with the Vendor and communicate to the end user appropriately according to the severity of the problem. Once a problem of any severity has been resolved, the support person should update the documentation in the IT tracking sheet /Module. The end user should test the resolution and communicate back to the support person that the problem has been resolved or further action is needed. Only upon end user confirmation that the problem has been resolved can an issue be closed in IT Problem Tracking Sheet/Module

7) Change Management Objective

The purpose of the Change Management Policy is to manage changes in a rational and predictable manner so that staff and clients can plan accordingly. Changes require serious forethought, careful monitoring and follow up evaluation to reduce negative impact to the user community and to increase the value of Information Resources.

Audience

The Change Management Policy applies to all individuals that install, operate or maintain Information Resources.

Definitions

Following are the definition for Change Management Policy

Information Resources (IR): any and all computer system which affects the business operations such as server systems, storage systems, database, routers, firewall, switches, modems, IPS, links, application software operating system and configuration of any such hardware or software.

Owner: The manager or agent responsible for the function which is supported by the resource, the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide the security. The owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared by managers of different departments.

Custodian: Guardian or caretaker; the holder of data, the agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information. For mainframe applications Information Services is the custodian; for micro and mini applications the owner or user may retain custodial responsibilities. The custodian is normally a provider of services.

Change Management: The process of controlling modifications to hardware, software, firmware, and documentation to ensure that Information Resources are protected against improper modification before, during, and after system implementation.

Change:

• Any implementation of new functionality

• Any interruption of service

• Any repair of existing functionality

• Any removal of existing functionality

Scheduled Change: Formal notification received, reviewed, and approved by the review process in advance of the change being made.

Unscheduled Change: Failure to present notification to the formal process in advance of the change being made. Unscheduled changes will only be acceptable in the event of a system failure or the discovery of security vulnerability.

Emergency Change: When an unauthorized immediate response to imminent critical system failure is needed to prevent widespread service disruption.

Change Management Policy

- Every change to a the Company's Information Resources resource such as: operating systems, computing hardware, networks, and applications is subject to the Change Management Policy and must follow the Change Management Procedures.
- All changes affecting computing environmental facilities (e.g., air-conditioning, electricity, and alarms) need to be reported to or coordinated with the leader of the change management process.
- The Custodian will receive a change request from data owner, Or the custodian find necessity to apply a patch or changes resulting security threats.
- The Custodian will analyze and reviews the request of change.
- A Formal Change Request will be floated by Custodian of Data for approval with relevant information like, Risk Assessment, Fallback Plan. Outage details to the Data Custodian.
- The Change Request approval will be assessed and approved by the Data Owner.
- The Change Request then will be approved by Head of Custodian (IT).
- A Formal communication will be floated informing all concern party about schedule of change.
- The Custodian will implement the change.
- A Formal communication will be floated informing Custodian about the result of change.
- The Periodic review will be carried out to for the fulfilled change request and their impact.
- Customer notification must be completed for each scheduled or unscheduled change following the steps contained in the Change Management Procedures.
- A Change Review must be completed for each change, whether scheduled or unscheduled, and whether successful or not.
- A Change Management Log must be maintained for all changes. The log must contain, but is not limited.

INTERNET POLICY

Objective: To provide guidelines for acceptable usage of the Internet system and to reduce the potential risks involved in accessing the Internet.

Audience: This policy applies to all users of the Company's Internet browsing system, including all permanent and temporary staff, contractors, and business partners.

Policy Statements:

1. Internet Browsing:
    - All connections to the Internet shall pass through appropriate access control mechanisms like firewalls and proxy servers.
    - Public mailing sites shall be blocked to maintain data security, except for the management.
    - The Company's systems must not be accessible from the Internet unless hosted in a Demilitarized Zone (DMZ).
    - Internet browsing access shall be provided on a need-to-have basis with written approval from the Operational/Functional Director and respective Departmental Head.
    - All employees will have default access to the Internet.
    - Access to the Internet shall be granted only for HTTP and HTTPS services. Any other requests like FTP access will require special permission from the business head.
    - Incoming traffic into the internal network via file downloads, file exchanges, or file transfers (FTP protocol) of any software, executable files like .exe, .vbs, .scr, etc., shall be prohibited by default.
    - No public instant messaging solutions like MSN, Yahoo Messenger, etc., will be allowed due to inherent security weaknesses.
    - Access to objectionable sites like hacking, pornography, gambling, etc., should be blocked by an appropriate content filtering solution.
    - Any documents downloaded from the Internet shall be scanned for viruses and malicious content.
    - Internet access from servers/systems with critical data shall not be allowed.
    - By default, all sites for all Internet users will be shut down. Users must furnish a list of sites they need access to, which will be opened after thorough examination for safe content and being virus-free.

- All access to the Internet must be logged, and adequate information must be captured to assist with investigations and detect misuse. Monitoring Internet browsing by other employees shall be prohibited unless specifically delegated.
- The Company is entitled to examine and/or monitor any Internet usage, including email or instant communication messages, downloaded content, and usage mechanisms.
- The Company is not responsible for any personal financial transactions or consequent loss of personal information or incidental financial or other losses.

2. Usage of Company Internet Browsing System:

- Users shall use the system responsibly and prudently, avoiding objectionable, frivolous, libelous, offensive messages, prejudice, harassment, or illegal activities that may damage the company's business or image.
- All existing company policies apply to users' conduct on the Internet, especially those dealing with intellectual property protection, privacy, misuse of company resources, information and data security, and confidentiality.
- Internet facilities must not be used to download or distribute pirated software or data, pornography, or other salacious or frivolous material, view or download audio, video, or music material, games, obtain or purchase executables like *.exe, make legal commitments by email on behalf of the company, or play games against opponents over the Internet.
- Users must not attempt to bypass security controls governing access to the Internet.
- Users must not utilize the Internet to disclose any company/subscriber information without authorization.
- Users will make all efforts to ensure that bandwidth resources are not negatively affected.
- Users must only access the Internet using approved software.
- Internet facilities must not be used to propagate any virus, worm, Trojan horse, or trap door program code.
- Internet facilities must not be used to disable or overload any computer system or network or circumvent any system intended to protect the privacy or security of another user.
- Internet facilities must not be used to upload software licensed to the company or data owned or licensed by the company without explicit authorization.

- Connection to the Internet through dial-up modems from systems (while connected to the LAN network) is strictly prohibited as it bypasses the perimeter firewall network.
- Internet access systems should be restricted to authorized systems only and must not be misused by extending the system to unauthorized systems or users.
- Users must bear in mind that email communication, however confidential, may have to be disclosed in court proceedings or investigations.

Violations to Policy: Violations of this policy may subject personnel to disciplinary action, up to and including discharge from employment, including discontinuation of Internet/email access.

Exception Procedure: Exceptions to the above policies shall be approved through a documented exception format and approved by the Functional/Operational Director, Area IT Head, and Head IT Security after considering the impact of the exception sought, the risk involved, and the compensating controls implemented to mitigate the risk.

EMAIL POLICY

Objective: To encourage the authentic and effective use of the Company's email facility as a valuable corporate resource and an effective business communication facilitator.

Audience: This policy applies to all users of the Company's email system, including all permanent and temporary staff, contractors, and business partners.

2. POLICY STATEMENTS:

Acceptable Uses of Company Email Access:

- The company provides email access for business usage. Every staff member has the responsibility to maintain and enhance the company's public image and use company email in a responsible and productive manner that reflects well on the company.
- The distribution of company information via email must be performed on a need-to-know basis.
- The company recognizes that there may be occasional personal use, but this shall not be excessive or unreasonable.

3. UNACCEPTABLE USES OF COMPANY EMAIL ACCESS:

- Company email access must not be used for transmitting, retrieving, or storing communications of a discriminatory or harassing nature, obscene materials, or involving gambling or lascivious materials.
- All data transmitted shall be the property of the Company.
- No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, or sexual preference shall be transmitted.
- Solicitation of non-company business or any use of the company email or Internet for personal gain is prohibited.
- Email system users must not attempt to forge email messages or disguise their identity when sending email.
- Email system users must not use automatic forwarding to forward internal email to external mail systems (e.g., Hotmail).
- The use of public email systems (e.g., Hotmail) for the Company's business is prohibited. The company understands that some vendors may have public email systems and may need to communicate with them using the company's email system.
- Chain mails, which urge users to propagate message contents to multiple users, are strictly prohibited.
- The email system should not be used for any illegal purpose, against company policy, or contrary to the company's best interests.

- Email system users must not transmit copyrighted materials belonging to entities other than this company. All employees obtaining access to other companies' or individuals' materials must respect all copyrights and may not copy, retrieve, modify, or forward copyrighted materials without permission.

4. SECURITY:

- Each email system user is responsible for the content of all text, audio, or images they place or send over the company's email and therefore responsibility for any misuse of email shall remain with the user.
- All emails on the company email system are property of the Company and can be read, intercepted, and, if necessary, deleted by management. All messages sent by employees via email are records of the company. At any time and without prior notice, management reserves the right to examine email, personal file directories, and other information stored on the company's computers and servers.
- Email system users must not assume electronic communications are totally private and should transmit highly confidential data in other ways. Email messages regarding sensitive matters should warn that such communications are not intended to be secured or confidential.
- Monitoring of individual users' email shall be explicitly authorized by management (IT Director or Head IT Security). Unless specifically delegated, the task of monitoring email messages by other employees shall be prohibited.
- Users shall report any offensive emails, either from the company email system or external email systems.
- Users shall take suitable preventive actions to prevent transmitting and downloading files with viruses and refrain from opening dubious attachments.
- Creation, modification, and revocation of email accounts shall be authorized and controlled. Creation of group IDs shall be allowed only for special business requirements.
- The size of email attachments should be restricted as per company predefined limits.
- An appropriate disclaimer should be added to all outgoing emails.
- The email servers shall be protected by a gateway-level antivirus product and anti-spam solution and should scan each incoming and outgoing mail for any malicious codes, viruses, worms, Trojans, etc.

Violations to Policy: Violations of this policy may subject personnel to disciplinary action, up to and including discharge from employment, including discontinuation of Internet/email access.

Exception Procedure: Exceptions to the above policies shall be approved through a documented exception format and approved by the Functional/Operational Director, Area IT Head, and Head IT Security after considering the impact of the exception sought, the risk involved, and the compensating controls implemented to mitigate the risk.

BUSINESS CONTINUITY AND IT DISASTER RECOVERY POLICY

Revision & Version History:

Version	Effective Date	Author	Approved By	Remarks
1.0	1st June 2019	Manager - IT	Head - IT	Initial Release
2.0	1st June 2020	Manager - IT	Head - IT	Review
2.0	2nd June 2021	Manager - IT	Head - IT	Review
2.0	3rd June 2022	Manager - IT	Head - IT	Review
2.0	1st June 2023	Manager - IT	Head - IT	Review
2.1	26th April 2024	Manager - IT	Head - IT	Review

1. PURPOSE

The purpose of this policy is to establish necessary controls for maintaining Business Continuity and IT DR Plan for all Information (electronic, paper form etc.) and supporting IT assets, Technology and People within AFPL's Infrastructure.

2. SCOPE

This policy applies to all IT & IS assets, applications and its supporting IT facilities like Data center that is either outsourced, owned or managed by AFPL. The policy applies to all users, including those users affiliated with third parties / outsourced parties who own and have access to AFPL IT & IS assets.

3. POLICY

The Business Continuity and IT Disaster Recovery Policy shall ensure that critical services needed for meeting business requirements, safe guarding employees live and organisation property are maintained with minimal interruption in event of disaster and failures.

Major business continuity risks that threaten the continuation of the delivery of products and services shall be identified, and an effective preventative, detective and responsive recovery strategies shall be developed, implemented, tested and maintained.

The BCP and IT DR policy shall help AFPL's employees including Business Continuity Management Team (BCMT) and Emergency Response Team (ERT) in responding to any type major or minor business continuity risks.

4. BUSINESS CONTINUITY

- AFPL's respective department heads and supporting teams are responsible for assessing the potential impact that loss of data would have on their business processes and shall derive acceptable RPO / RTO values.
- Each department shall have a completed and updated business continuity and IT DR plan.
- The plans shall include provisions for business continuity of critical business process and recovery in the event of disaster and failures.
- Plan shall contain considerations of backups of critical information supporting these business operations based on Business Impact and Risk Assessment in line with respective department's RPO / RTO values.
- Based on the business need and nature of changes undergone, a paper-based walk through or an actual test of all business continuity plan / disaster recovery plans shall be conducted as appropriate.
- The CISO / Head IT / CTO or its designee shall perform a business impact analysis (BIA) as and when appropriate.

5. RECOVERY STRATEGY/ CONTINGENCY PLAN

- Every critical production business application supported by IT & IS asset and its facility shall have a recovery strategy / contingency plan.
- Procedures for restoring service shall be formally documented.
- All designated stakeholders / users should receive necessary training.
- To the extent practical and feasible, business contingency and IT DR Contingency plans shall be tested at regular intervals and records be maintained.
- The roles and responsibilities for business contingency and IT DR Contingency plans must be reviewed and updated as and when appropriate.

6. REFERENCE DOCUMENTS

- RBI Master Direction - Information Technology Framework for the NBFC Sector dated June 08, 2017 (RBI/DNBS/2016-17/53)
- Section 6 of RBI Master Direction - Information Technology Framework for the NBFC Sector.

IT CHANGE AND RELEASE MANAGEMENT POLICY

Revision & Version History:

Version	Effective Date	Author	Approved By	Remarks
1.0	1st June 2019	Manager - IT	Head - IT	Initial Release
2.0	1st June 2020	Manager - IT	Head - IT	Review
2.0	2nd June 2021	Manager - IT	Head - IT	Review
2.0	3rd June 2022	Manager - IT	Head - IT	Review
2.0	1st June 2023	Manager - IT	Head - IT	Review
2.1	26th April 2024	Manager - IT	Head - IT	Review

1. Purpose:

To ensure that all changes to the production environment of IT applications and IT infrastructure are recorded, tracked, assessed, classified, prioritized, approved, tested, implemented and reviewed in a controlled manner to minimize disruption.

2. Scope:

This policy is applicable for changes in the production environment of IT applications and IT infrastructure owned and managed by AFPL including new application procurements / Application as a Service. This policy does not apply to changes and releases at an operational level e.g. repair to printers or other routine service components.

3. Policy:

- All changes to AFPL IT Infra and applications shall undergo formal change management process.
- All changes to the IT&IS assets and supporting processing facilities shall be authorized by the relevant approving authority, based upon the requirement, inter-dependency, compliance and potential impact analysis on AFPL's business operations.
- The implementation scheduling information of approved changes shall be maintained and communicated to relevant stakeholders. A mechanism shall exist to maintain documentation related to changes and releases.
- Based on the analysis by relevant approving authority and CAB (Change Advisory Board), the CR then may be approved / rejected.

- Change classification viz. Normal / Emergency / Major / Minor shall exist to define changes and control the authorization and implementation of emergency changes and releases.
- Major changes to information processing systems and utilities may be tested in an isolated, controlled, similar setup prior to implementation (if similar hardware / platform is available) and the result be recorded to produce as an evidence to relevant approving authority to seek the approval.
- Change impact analysis and roll back plan shall be prepared for all changes as appropriate.
- Unauthorized change, if any, shall be reported to the Head-IT for appropriate actions.
- All change requests shall be prioritized in terms of benefits, urgency, effort required and potential impact on operations.
- A controlled acceptance test environment to deploy and test all releases prior to distribution shall be established.
- All changes and releases shall be observed for success or failure post implementation. The changes shall be reversed, if unsuccessful, in a controlled manner.
- The release and distribution of release shall be designed and implemented to ensure integrity of hardware and software during installation, handling, packaging and delivery.
- The change and release management processes shall be integrated with other processes to establish traceability, detect unauthorized changes and identify change related incidents.
- In case of the absence of a similar (hardware / software) test bed, downtime may be requested from relevant approving authority preferably over the weekend to implement the change.
- Audit log shall be maintained for all Change Requests by the **CISO / Head IT / CTO.**
- All the modifications and changes pertaining to the IT & IS assets shall be verified by approving authority and CAB. In case change found inappropriate, fall back mechanism needs to be revert and lesson learned report needs to be prepared.

4. Reference Documents

- RBI Master Direction - Information Technology Framework for the NBFC Sector dated June 08, 2017 (RBI/DNBS/2016-17/53)
- Section 4.2 of RBI Master Direction - Information Technology Framework for the NBFC Sector.

INFORMATION AND CYBER SECURITY POLICY

Revision & Version History:

Version	Effective Date	Author	Approved By	Remarks
1.0	1st June 2019	Manager - IT	Head - IT	Initial Release
2.0	1st June 2020	Manager - IT	Head - IT	Review
2.0	2nd June 2021	Manager - IT	Head - IT	Review
2.0	3rd June 2022	Manager - IT	Head - IT	Review
2.0	1st June 2023	Manager - IT	Head - IT	Review
2.1	26th April 2024	Manager - IT	Head - IT	Review
2.2				

1. PURPOSE

The purpose of this policy is to establish a framework for protecting the information assets of THE COMPANY'S Finance Private Limited (AFPL) to achieve organizational goals. This policy aims to control access to sensitive information, ensuring its use only by legitimate users, and to protect against unauthorized access, modification, and destruction.

2. SCOPE

This policy applies to all information assets, IT & IS assets, applications, and supporting IT facilities like data centers that are either outsourced, owned, or managed by AFPL. It covers all employees and third parties with access to AFPL's information from within or outside AFPL's premises.

3. INFORMATION SECURITY

3.1 Basic Tenets

- **Confidentiality**: Ensuring access to sensitive data to authorized users only.
- **Integrity**: Ensuring accuracy and reliability of information by preventing unauthorized modification.
- **Availability**: Ensuring uninterrupted access to data when needed.
- **Authenticity**: Ensuring that data, transactions, communications, or documents are genuine.

3.2 IS Framework

- **Identification and Classification of Information Assets**: Maintain a detailed inventory of information assets with clear identification.
- **Segregation of Functions**: Separate duties of the Security Officer/Group from the Information Technology division. Ensure adequate resources for the information security function.
- **Role-based Access Control**: Access to information should be based on well-defined user roles. Avoid dependence on a few individuals for critical tasks.
- **Personnel Security**: Conduct rigorous background checks for personnel with privileged access.
- **Physical Security**: Secure physical components to protect the confidentiality, integrity, and availability of information.
- **Maker-Checker Principle**: Ensure that each transaction requires at least two individuals for completion to reduce risk and ensure reliability.
- **Incident Management**: Define incidents and develop processes for preventing, detecting, analyzing, and responding to information security incidents.
- **Audit Trails**: Ensure audit trails exist for IT assets to meet business, regulatory, and legal requirements.
- **Public Key Infrastructure (PKI)**: Increase the usage of PKI to ensure data confidentiality, access control, data integrity, authentication, and non-repudiation.

4. CYBER SECURITY

4.1 Cyber-Security Policy

- Develop a board-approved cyber-security policy outlining strategies to combat cyber threats based on business complexity and acceptable risk levels.
- Review organizational arrangements to ensure security concerns receive adequate attention and are escalated appropriately.

4.2 Vulnerability Management

- Develop a strategy for managing and eliminating vulnerabilities, clearly communicated in the Cyber Security policy.

4.3 Cyber Security Preparedness Indicators

- Develop indicators to assess the level of risk/preparedness and use them for comprehensive testing through independent compliance checks and audits.

4.4 Cyber Crisis Management Plan (CCMP)

- Develop a CCMP addressing detection, response, recovery, and containment of cyber incidents. Take measures to prevent, detect, respond to, recover from, and contain cyber-attacks.

4.5 Reporting Cyber-Security Incidents

- Report all types of unusual security incidents to the DNBS Central Office, Mumbai, as specified in the CSIR Form of Annex I.

4.6 Cyber-Security Awareness

- Promote cyber-security awareness among staff, top management, and board members. Ensure stakeholders understand and support cyber resilience objectives.

4.7 Digital Signatures

- Use Digital Signature Certificates to authenticate identity electronically and ensure the privacy of online transactions.

4.8 IT Risk Assessment

- Conduct a comprehensive risk assessment of IT systems annually. Analyse threats and vulnerabilities to determine appropriate controls for risk mitigation.

4.9 Mobile Financial Services

- Develop mechanisms to safeguard information assets used by mobile applications, ensuring confidentiality, integrity, authenticity, and end-to-end encryption.

4.10 Social Media Risks

- Implement controls to mitigate risks associated with social media, such as account takeovers and malware distribution.

4.11 Training

- Implement ongoing training and information security awareness programs. Track the effectiveness of training through assessments and maintain updated training status.

5. GOVERNANCE STRUCTURE

5.1 Security Roles & Responsibilities

a) Steering Committee

- Ensure Information Security objectives and plans are established.
- Communicate the importance of meeting information security objectives and conforming to the information security policy.
- Provide sufficient resources to develop, implement, operate, and maintain adequate security measures.
- Approve new or revised information security policies and major initiatives.

- Appoint AFPL's Head IT / CTO / CISO.
- Ensure periodic Information Security audits.
- Report the security posture to the board as appropriate.
- Meet quarterly to discuss and review the security program.

b) Chief Information Security Officer (CISO) / Head IT / CTO

- Coordinate the implementation of the Information Security program.
- Develop Information Security policies, procedures, standards, and guidelines.
- Assist the Steering Committee with planning and budgeting for Information Security functions.
- Communicate Information Security requirements to relevant stakeholders.
- Conduct and oversee AFPL's risk assessment.
- Review and monitor remedial work related to Information Security incidents.
- Ensure employees receive extensive training on Information Security.
- Stay updated with relevant security requirements through forums, special interest groups, and consulting experts.

c) Head of Departments

- Be responsible for the security of assets/business processes under their purview.
- Ensure appropriate security controls are applied and resources are allocated to maintain required security levels.
- Work closely with the CISO / Head IT / CTO in implementing AFPL's Information Security policies.
- Appoint/nominate an Information Security Officer (ISO).
- Serve as the Designated Approving Authority for the department's assets.
- Assist with planning, budgeting, and implementing Information Security for the department.

d) Information Security Officers (ISOs)

- Assist in implementing AFPL's security program within their respective departments.
- Recommend how best to implement the Information Security program and policy.
- Coordinate the implementation of the security program within their department.
- Assist system owners in developing security plans, risk assessments, and contingency plans.
- Serve as the contact point for all security-related issues/incidents for the department.

- Participate in the development of Information Security policies and procedures.

e) Users

- Be responsible and accountable for adhering to Information Technology and Information Security policies.
- Report incidents of non-compliance or breaches to the CISO / Head IT / CTO or respective Line Managers.
- Comply with user expectations as detailed in the "Acceptable Usage Policy".

6. ENFORCEMENT

This policy supersedes any previous policies in the organization. It will be implemented in conjunction with other departmental policies/practices. In case of conflict, this policy will take precedence to ensure Information Security. The CISO / Head IT / CTO is responsible for enforcement and regular upkeep of the policies under the guidance of the Board and Steering Committee.

7. POLICY EXCEPTIONS

Any exceptions or policy waivers must be recommended and justified with compensatory controls by the related department and Head IT for IT-related exceptions. Approval from ITSC and/or ISSC and/or MD shall be sought as appropriate.

8. POLICY VIOLATIONS

Any policy violation impacting AFPL's security posture will be dealt with according to Human Resource Policies and the law of the land.

9. REFERENCE DOCUMENTS

- RBI Master Direction - Information Technology Framework for the NBFC Sector dated June 08, 2017 (RBI/DNBS/2016-17/53)
- Section 3 of RBI Master Direction - Information Technology Framework for the NBFC Sector

IT & IS AUDIT POLICY

Revision & Version History:

Version	Effective Date	Author	Approved By	Remarks
1.0	1st June 2019	Manager - IT	Head - IT	Initial Release
2.0	1st June 2020	Manager - IT	Head - IT	Review
2.0	2nd June 2021	Manager - IT	Head - IT	Review
2.0	3rd June 2022	Manager - IT	Head - IT	Review
2.0	1st June 2023	Manager - IT	Head - IT	Review
2.1	26th April 2024	Manager - IT	Head - IT	Review

1. PURPOSE

The purpose of this policy is to establish and maintain an effective process of IT & IS audits within AFPL. The IT & IS audit process is designed and implemented to provide an insight into the effectiveness of security controls that are in place to ensure confidentiality, integrity and availability of the organization's information is preserved. The IT & IS Audit policy shall cover effectiveness and oversight of IT & IS assets, evaluating adequacy of processes and internal security controls. It shall recommend corrective action to address deficiencies and check for remediation and compensatory controls implemented.

2. SCOPE

This policy applies to all process that is designed and implemented that impacts IT&IS infrastructure to meet AFPL's business requirements.

3. POLICY STATEMENTS

- **CISO / Head IT / CTO** is responsible for ensuring the implementation of appropriate framework of IT & IS review. He is also responsible for the overall coordination related to IT & IS Audit with Internal Audit Department and external agencies wherever appropriate.
- Department Heads and Line Managers are responsible for providing necessary co-operation while IT & IS Audit are conducted and ensure timely closures of audit findings and implementation of corrective actions.

- The IT & IS Audit team shall use the guidance issued by Professional and regulatory bodies like RBI, ISACA, ISO while implementing the framework for conducting IT & IS Audit.
- AFPL shall impart Internal Quality Auditor training to selected employees' part of IT & IS Audit team.
- Select and appoint external IT&IS auditors based on their audit qualification, accreditation, experience and certifications.
- The IT & IS Audit team (in coordination with Internal Audit team) shall prepare annual audit calendar throughout IT&IS infrastructure within AFPL.
- AFPL management shall be responsible for deciding the appropriate action to be taken in response to reported observations and recommendations during IT&IS Audit.
- The IT&IS Audit framework shall clearly mention responsibilities for compliance/sustenance of compliance, reporting lines, timelines for submission of compliance and authority for accepting compliance.
- Auditors shall not audit their own functions.

4. REFERENCE DOCUMENTS

- RBI Master Direction - Information Technology Framework for the NBFC Sector dated June 08, 2017 (RBI/DNBS/2016-17/53)
- Section 5 of RBI Master Direction - Information Technology Framework for the NBFC Sector

IT SECURITY POLICY

Revision & Version History:

Version	Effective Date	Author	Approved By	Remarks
1.0	1st June 2019	Manager - IT	Head - IT	Initial Release
2.0	1st June 2020	Manager - IT	Head - IT	Review
2.0	2nd June 2021	Manager - IT	Head - IT	Review
2.0	3rd June 2022	Manager - IT	Head - IT	Review
2.0	1st June 2023	Manager - IT	Head - IT	Review
2.1	26th April 2024	Manager - IT	Head - IT	Review

1. PURPOSE

The purpose of this policy is to establish standards for the base configuration of IT Operations (Network and Server) Assets owned and/or operated by AFPL. Effective implementation of this policy shall minimize unauthorized access to AFPL's sensitive, critical, proprietary information and technology. The purpose of this policy is to establish standards for the base configuration of IT Operations (Network and Server) Assets that is owned and/or operated by AFPL.

2. SCOPE

This policy applies to IT Operation (Network and Server) assets owned and/or operated by AFPL and to IT Operations assets registered under any AFPL internal network domain. The policy applies to all users, including those users affiliated with third parties/outsourced parties who owns and have access to AFPL's IT assets. The policy also applies to all computer, network, owned by and/or administered by AFPL.

3. POLICY STATEMENTS

The IT Policy shall define, document and implement appropriate security architecture and procedures, taking into consideration legal/regulatory requirements, data flows, monitoring requirements, and required protection measures. Access to AFPL's IT Operations (Network and Server) assets and its resources shall be strictly controlled, managed, and reviewed to ensure only authorized users gain access based on the privileges granted. The IT Operations Assets

shall be adequately controlled, monitored and protected from both internal and external threat source.

IT Operation assets shall be registered, and the following information is required to positively identify the point of contact:

- Contact(s) and location, and a backup contact
- Hardware and Operating System/Version
- Main functions and applications, if applicable
- Vendors details and SLA location (if services are outsourced)
- Information inventory list shall be kept up to date.
- Configuration changes for IT production assets shall follow the appropriate change management procedures

4. GENERAL CONFIGURATION GUIDELINES AND SERVICES

- The configuration of IT Operations (Network and Server) Assets shall be in accordance with approved security guidelines.
- Ports, Protocols, Daemons, Services and applications that are not used shall be disabled where practical.
- Access to services shall be logged and/or protected through proper access-control methods
- The most recent security patches shall be installed on the asset as soon as practical or in accordance with Information security policy, the only exception being when installed applications would interfere with business requirements.
- Always use standard security principles of least privilege access to perform a function.
- Do not use root or other administrator level user id's when a non-privileged account can be used.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access shall be performed over secure channels, (e.g., encrypted network connections using SSH or IPsec, WPA SSL).
- Users shall have their identity verified with AFPL's issued user-id and a confidential password prior to being permitted to access its services through IT assets.
- Users shall be allowed to browse Internet and given network connectivity to any other internal networks provided there is a strong business need and after approval from Head of Department/Security.

- Security risk assessment of all such connectivity shall be done prior to providing the connectivity.
- Networks/Systems that can be reached by third party networks shall have appropriate (e.g. multi-factor) access control systems approved by Head of Department/Security.
- Internal networks that store sensitive information shall have strong authentication, authorization and accounting/logging system.

5. AUDIT AND MONITORING

- Audits shall be performed on a regular basis by authorized departments within AFPL.
- Audits shall be managed by the ISMS, in accordance with the Audit Policy based on regulatory and compliance requirement.
- Audit trails from IT Operations (Network and Server) Assets shall be protected from tampering and saved in a centralized logging server. All security-related events on critical or sensitive systems shall be logged and audit trails saved based on regulatory and compliance requirement.
- All login and logout events on IT Operations (Network and Server) Assets like domain, servers, applications, databases, network and security devices shall be logged.
- All logs shall have minimum log of following things:
    - User ID
    - Date and time of logon and logoff
    - Logon method, location, terminal identity (if possible), network address.
    - Records of successful and unsuccessful system access attempts.
- All such log files shall be reviewed on weekly basis/regularly by the security operations or concerned team.
- If any suspected activities found in such logs then ISO/Incident response team shall investigate such activities.
- The internal clock of all servers, desktops, networking devices, firewall, and other computing devices shall be synchronized with the Domain Controller Server.

6. PHYSICAL AND LOGICAL SEPARATION

- IT Operations (Network and Server) Assets shall be physically located in an access-controlled environment.

- IT Operations (Network and Server) Assets are specifically prohibited from operating from uncontrolled cubicle areas
- Separations of logical network domains shall be used to restrict network access. Examples: VLANs etc. Access across the VLANs shall be restricted and only required services shall be permitted.
- The network diagram with all VLANs and all corresponding restrictions shall be prepared and maintained
- Wireless access points shall be adequately protected within AFPL's network. Accepted wireless encryption standards shall be used for configuration.
- All the Internet traffic shall flow only via firewall or proxy. All interfaces to Internet shall be protected by firewall. The default firewall shall be configured to the Default Deny stance – "deny all traffic unless explicitly allowed"

7. REMOTE ACCESS MANAGEMENT

- In-bound connections to AFPL's systems shall be protected with an approved multi-factor access control system. Prior approval by relevant Authority shall be obtained before opening any applications outside of AFPL's (e.g. making any application available from the Internet).
- Access to AFPL's internal network shall be done only through VPN software using multi-factor access control approved by Head of Security.
- Up-to-date virus checking programs shall be continuously enabled on all web servers, LAN servers, mail servers, firewalls, and networked PCs.
- Systems accepting remote connections from public networks or the Internet shall include a session time-out mechanism.
- Login banners "Unauthorized access prohibited" shall be used on all AFPL's IT Operations (Network and Server) Assets that are directly accessible through external networks.
- All AFPL's IT Operations (Network and Server) assets which interface to external networks shall be enabled to maintain system logs that indicate the time and date, identity and activity performed by each user who gains access to these systems.
- Access filters are applied to user VPN connections to restrict access to specific services and servers

8. REFERENCE DOCUMENTS

- RBI Master Direction - Information Technology Framework for the NBFC Sector dated June 08, 2017 (RBI/DNBS/2016-17/53)

- Section 2 of RBI Master Direction - Information Technology Framework for the NBFC Sector.