INFORMATION TECHNOLOGY POLICY

Table of content

1. Preamble to the Information Technology Policy

1.1 Document Distribution

This document is owned by Chief Technology Officer (CTO) and will be distributed to all the staff through email communication and/or upload on web portal. It shall also be distributed to the third parties associated with 360 ONE Group by the respective departments, wherever needed.

1.2 Primary recipients

All Employees of 360 ONE Group, 360 ONE WAM LIMITED (holding company, holding a Merchant Banking licence), 360 ONE Wealth Distribution Services Limited (covering Stock and Commodities Broking, Depository Participant business and Distribution), 360 ONE Prime Limited (NBFC), 360 ONE Asset Management Limited (covering Mutual Funds, Portfolio Management Services and Alternative Investment Funds), 360 ONE Wealth Portfolio Managers Limited (covering PMS and AIF), and 360 ONE Investment Advisory and Trust Services Limited (covering Trustee Services and Advisory), collectively referred to as "360 ONE" Entity.

1.3 Document Confidentiality

This document is confidential – Internal Use only and hence would be made available through internal portal.

1.4 Objective of IT Policy

The objective of 360 ONE IT policy is to set the guiding principles for establishing IT infrastructure and IT operations that would enable the users identify opportunities, improve performance and understand business environment, and at the same time to achieve Confidentiality, Integrity and Availability of the information and information systems used by those IT Operations.

This document provides the framework to manage IT infrastructure by means of structured service delivery, service management and IT governance processes. It states the responsibilities of management, executives, employees and suppliers to ensure that the IT supports business objectives.

1.5 Authority

The policy document is issued under the authority of Board of Directors - Information Technology Strategy Committee (ITSC).

1.6 Review and approval

This policy shall be updated once annually or in the case of major change in IT environment or a regulatory requirement. This policy shall be reviewed by CTO and approved by the Board.

1.7 Procedures and Guidelines

A separate document for "Procedures and Guidelines" is created. It documents the detailed guidelines for implementation of the policies and standards.

The key objectives of developing Procedures and Guidelines are:

1. To ensure that IT Policy is interpreted correctly and uniformly across the 360 ONE.
2. To provide guidelines for implementation of the policies
3. To create awareness about policies and assist in policy compliance

1.8 Scope

These policies & standards are applicable to all locations of 360 ONE Entities within India including all IT and IS assets, all IT and IS processes, all business processes supported by IS and all employees in India. s

1.9 Management of IT Policy

The Information Technology Steering Group (ITSG) shall have the overall responsibility of implementation & maintenance of this policy, and it shall review this Policy on yearly basis or if any significant changes occur. ITSG shall also review the compliance & implementation status, effectiveness of controls & their implementation, Incidents, suggestions & feedback from various stakeholders.

1.10 Board Approval of IT Policy

In case of any changes the IT policy shall be reviewed and approved by IT Strategy Committee and shall be tabled for board approval.

2. Organization of Information Technology

2.1 IT Framework

IT Governance is an integral part of corporate governance. It involves leadership support, organizational structure and processes to ensure that the organisation's IT sustains and extends business strategies and objectives.

2.2 Roles & Responsibilities

IT Strategy Committee:

IT Strategy committee should periodically review IT organizational structure to check if it commensurate with the size, scale and nature of business activities carried out. The IT Strategy Committee should meet at an appropriate frequency but not more than six months should elapse between two meetings. The Committee shall work in partnership with other Board committees and Senior Management (internal working groups such as Information Security Steering Group, Information Security Working Group) to provide input to them.

It will also carry out review and amend the IT strategies in line with the corporate strategies, Board Policy reviews, cyber security arrangements and any other matter related to IT Governance. Its deliberations may be placed before the Board.

Composition:

Independent Director
Chief Information Officer (CIO)
Chief Risk Officer (CRO)
Chief Operations Officer (COO)

Responsibilities:

1. Approving IT strategy and policy documents
2. Ensuring that the management has put an effective strategic planning process in place.
3. Ratifying that the business strategy is indeed aligned with IT strategy.
4. Ascertaining that management has implemented processes and practices that ensure that the IT delivers value to the business
5. Ensuring IT investments represent a balance of risks and benefits and that budgets are acceptable
6. Monitoring the method that management uses to determine the IT resources needed to achieve strategic goals and provide high-level direction for sourcing and use of IT resources.
7. Ensuring proper balance of IT investments for sustaining growth and becoming aware about exposure towards IT risks and controls.

Information and Technology Steering Committee:

An IT Steering Committee needs to be created with representatives from the IT, HR, legal and business sectors. Its role is to assist the Executive Management in implementing IT strategy that has been approved by the Board. It includes prioritization of IT enabled investment, reviewing the status of projects (including, resource conflict), monitoring service levels and improvements, IT service delivery and projects

Composition:

Chief Executive Officer
Chief Operations Officer
Chief Strategy Officer,
Chief Information Officer,
Chief Risk Officer,
Head of Credit Risk,
Chief Finance Officer,
Compliance Officer and
Head Program Management IT

Responsibilities

1. Design and implementation of IT projects within approved budgets.
2. Approve the appropriate system providers/solutions for implementation. Take decision on Buy v/s Build approach
3. Provide oversight and monitoring of the progress of various projects, including deliverables to be realized at each phase of the project
4. Milestone tracking according to the project timetable
5. Ensure adherence to Change Management Policy.
6. Consult and advice on the application of architecture guidelines
7. Ensure compliance to regulatory and statutory requirements
8. Provide direction to IT architecture design and ensure that the IT architecture reflects the need for legislative and regulatory compliance, the ethical use of information and business continuity
9. CTO shall periodically evaluate the IT training requirements and ensure that sufficient, competent and capable human resources are available.

3. IT Planning

3.1 IT Strategy

1. The IT Strategy committee, based on key inputs from the business leadership and the board of directors of the organization design an IT strategy that is aligned with the enterprise/business strategy.
2. While defining the IT strategy, due consideration should be given to attributes such as cost-effective, appropriate, realistic, achievable, enterprise and technological obsolescence.
3. The strategy shall be designed and maintained in a manner that it will serve as a guidance for building an IT roadmap around IT-enabled investment commitments, IT programs/Projects to be undertaken, business IT services to be instituted and IT assets to be acquired.
4. The IT strategy, shall be communicated and be accessible to all appropriate business and IT stakeholders and throughout the enterprise.

3.2 IT Budget & Cost Management

IT budget and cost management policy shall help IT achieve business goals in a cost-efficient manner.

1. The IT and finance function shall Establish and maintain a method for accounting for all IT-related costs, investments and depreciation as an integral part of the organizations cost and financial management process.
2. The Board and senior management shall provide adequate support for financial allocations to the budgets to ensure that IT strategy objectives can be met effectively.

3. The IT function shall prepare a budget reflecting the investment priorities supporting the IT strategy and Operational requirements based on the portfolio of IT-enabled programs and IT services.

3.3 IT Portfolio Management

360 ONE shall ensure that all stakeholders can view an accurate, consistent picture of the IT services, their details and status

3.3.1 Request for addition of a new service in the portfolio

For addition of new service, prior business approval should be obtained. In case of major service addition, workshop with key stakeholders should be conducted.

3.3.2 Request for modification of existing service

Approval should be taken for modification of existing service and should be communicated to stakeholders.

3.3.3 Retiring a service from existing catalogue/decommissioning of a platform.

The request for retiring an existing service should be approved and the service should be retired from the existing service catalogue and catalogue should be updated and communicated to all stakeholders.

3.4 Manage Enterprise Architecture

Manage enterprise architecture shall act as reference point in managing the IT enterprise effectively.

3.4.1 Developing and documenting Enterprise Architecture

1. The IT function should ensure that a common architecture consisting of information/data, application and technology architecture layers for effectively and efficiently realizing enterprise IT strategies is documented in the form of enterprise architecture diagram.
2. The enterprise architecture documentation shall be maintained only with personnel authorized by CIO or Head of Application Support and shall be stored in a common repository with access to Technology team.
3. The enterprise architecture document should be reviewed yearly basis or whenever needed.

3.4.2 Redesign/updates to the enterprise architecture

1. All changes to enterprise architecture shall be approved and implementation over seen by the IT steering committee.

2. All proposed upgrades/changes/revisions to the enterprise architecture shall be done on completion of the project/implementation.

3.5 IT Risk Management

1. 360 ONE shall ensure that a standard IT Risk Management process which ensures compliance with functional, security, performance and applicable regulatory requirements shall be followed for all IT assets/processes/services. The goal of IT risk management policy is to protect the organization and its ability to perform their mission, not just IT assets.

3.5.1 Risk Identification, Assessment, Mitigation and Reporting

1. A risk assessment methodology should be identified that is suitable to the 360 ONE and the identified information security, legal, statutory and regulatory requirements.
2. Information Security risk should be identified, assessed, mitigated and reported based on the risk management framework defined in the Risk Management procedure.
3. Business Continuity risk should be identified, assessed, mitigated and reported based on the Risk management framework defined in the Risk management policy/procedure.
4. IT risk assessment including IS risk should be brought to the notice of the Chief Risk Officer (CRO), CIO, CTO and the Board of directors.
5. IT risk assessment should be conducted at least on yearly basis.
6. Board and top management to take into consideration risks associated with planned IT operations and risk tolerance of the company.

4. IT Solution Delivery

DESIGN & BUILD

4.1 System Acquisition, Development & Maintenance Policy

A standard approach which ensures compliance with functional, security, performance and applicable regulatory requirements shall be followed for software development/procurement.

4.1.1 Procurement Strategy

1. Organization should treat all bidders with fairness and ensure that they are given the same level of information when preparing quotations or tenders.
2. Quotations and tenders should be evaluated not only on competitiveness in pricing but also factors such as the quality of the products/services and track records of the bidders.

4.1.2 Procurement Proposal

1. A proposal containing the details of the proposed procurement request should be defined and approved.

1.1.3 Supplier Database

1. A database should be maintained by procurement team in order to store performance records and results of the IT supplier evaluation. Database should be referred whenever a new IT procurement process is being initiated or considered.
2. Centralized database for all existing Technology, IT Hardware & Software inventory should be maintained and reviewed annually.

1.1.4 Technology Refresh

1. The existing applications, IT systems and technology should be assessed at least yearly for a need of technology refresh. The assessment of new technology should follow the complete procurement process.

4.2 Contract Management

1. IT services shall have well defined contract agreements that specify scope of services and establish accountability of suppliers.

4.2.1 Contract Requirements

1. Supplier Contract Agreements together with other supporting service agreements and corresponding procedures should be defined with suppliers providing services related to management of 360 ONE's information assets.

4.3 Supplier Management

360 ONE shall establish and manage the supplier relationships so as to ensure quality of service provided by suppliers.

4.3.1 Maintenance of Supplier and Contact Database

1. Supplier and contact database for all the IT supplier relationships should be maintained with **IT- Partner Relationship Department.**

4.3.2 Supplier and Contract categorization and Risk Assessment

1. Risk assessment of suppliers should be performed to ensure availability and continuity of services procured by the respective Verticals.

4.3.3 Contract Review, Renewal and Termination

1. The supplier contracts should be reviewed at least on annual basis by the respective department and status to be confirmed to IT- Partner Relationship Department.
2. In case of termination of contract, supplier should be informed and exit transition plan should be defined. Transition plan should include Knowledge transfer and handholding activities for 360 ONE or new supplier.

4.4 IT Outsourcing

1. The objective of this section is to identify risks associated with external parties and establish appropriate controls to ensure security in line with the 360 ONE Outsourcing Policy.

4.4.1 Framework and Governance over decision to outsource

1. The IT function and the senior management shall ensure that sound and responsive risk management practices for effective oversight, due diligence and management are in place for outsourcing of IT activities as per the policy framework.
2. The IT outsourcing propositions shall be put to the IT steering committee for approval (only if core NBFC IT activity is being outsourced).
3. Risk assessment and mitigating controls to be defined as per the Policy.
4. The current material/significant IT outsourcing arrangements shall be reviewed on an annual basis by the IT steering committee to assess and ensure that the risks posed by such a function

are low and adequately mitigated. The board shall be informed of any material risk arising of an outsourcing arrangement in a timely manner.

4.4.2 **Evaluating Vendors Outsourcing arrangements**

1. All requirements for outsourcing of IT activities shall be clearly be defined in the RFI/RFP's floated to vendors.
2. Ensure the below clauses/conditions are contractually enforced by the outsource vendors on their sub-contractors.
3. Maintaining, confidentiality, integrity, availability of internal data, customer and compliance data (to the extent relevant to the context of outsourcing).
4. Sign off NDA's by the vendors and their employees (where relevant to context).
5. Secure deletion of 360 ONE data and its customer data at the time of contract termination
6. Right for 360 ONE or the regulator governing 360 ONE (e.g. RBI. SEBI) to audit the service provider or their sub-contractor to ensure compliance to contract and prevailing regulations/legislations.
7. All security controls outlined in suppliers' security clause and ISMS audit policy which is a part of the Cyber security and IS policy shall be adhered in relation to all material IT outsourcing arrangements.

TRANSITION

4.5 Change Management Policy

All changes to Information assets must be recorded, classified, assessed for risk, impact and business benefit, approved and implemented in a controlled manner.

4.5.1 Change Request & Approval

1. 360 ONE to prioritize and responding to change proposals from business
2. Perform cost benefit analysis of the changes proposed
3. Assess the risks associated with the changes proposed
4. Change Approval Board (CAB) should be established for all application groups to take decisions on changes to be implemented.
5. For every change, a change request should be documented and shared with appropriate authorities for review.
6. All change requests should be approved before implementation.
7. All changes should be compliant with statutory and legal/regulatory requirements as applicable to 360 ONE.

4.5.2 Implementation of Change

1. Change should be implemented based on the implementation plan approved as part of change request.
2. Post Implementation, business verification review should be performed to confirm if the change is working as desired

4.5.3 Documentation of Change

1. All Documents related to change request should be retained for audit purpose.

4.6 Data Migration

360 ONE shall ensure migration of data between systems in controlled manner to ensure data integrity

4.6.1 Data Migration

1. Data migration requirement should be identified, analysed and impact of data migration should be communicated to respective stakeholders.
2. An identification and feasibility study should be conducted, reviewed and approved before initiating the data migration activity.
3. Procurement of migration software or outsourcing of migration activities shall be performed as per IT policy of 360 ONE.
4. Post migration audit/reconciliation should be performed to ensure integrity of data.
5. Two copies of back-up of the data, both pre-migration and post-migration along with reconciliation details should be maintained.

Project Management

360 ONE shall ensure that all IT projects are approved, managed and tracked in controlled environment to minimize errors and risks associated.

Steps/Activities to be followed in each project will be:

1. Project Initiation
2. Project Planning
3. Resource Planning
4. Project Monitoring
5. Project Closure

5. IT Operations

5.1 Service Request Management

360 ONE shall have a service request fulfilment process to provide quick and effective access to standard services which can be used to improve productivity and the quality of business services and products.

5.1.1 Logging Service Request

1. Service request should be raised by user department either by writing an email/ or using a portal (service desk) for the same.

5.1.2 Approval for Service Request

1. Cost of fulfilling the request should be established. Estimate of the cost should be produced and submitted to the user department / authorized dept. for management/ financial approval.

5.1.3 Request Fulfilment

1. Request fulfilment activity should depend upon the nature of the Service Request. Simple requests should be completed by service desk, while others should have to be forwarded to

specialist group/ technical team for fulfilment.

2. Service desk should monitor and track progress and keep users informed about the request fulfilment.

5.2 IT Incident Management

1. A formal IT incident management process shall be established to discover, report, respond and contain IT incidents effectively

5.2.1 Incident Management Procedures

1. 360 ONE's IS Policy - Incident Management policy and procedure should be referred along with this policy.
2. Procedures for IT Incident Management should include the recording, prioritization, business impact analysis and classification of incidents, responsibility of the personnel, escalation matrix, and process for resolution and formal closure of all IT incidents.

5.2.2 Detection and Recording

1. All events which are not part of the standard operation of a service and which causes or may cause disruption to or reduction in the quality of service and productivity should be recorded as incidents.
2. All IT incidents occurring at different 360 ONE branches/ offices should be recorded.

5.2.3 Incident Classification and Initial Support

1. All incidents should be classified and prioritized.
2. IT Incidents should be classified into different severity level based on the business impact and urgency of the incident.
3. Service Desk should own the incident ticket at all times and should be able to provide a status to the user during the entire incident management lifecycle.

5.2.4 Investigation and Diagnosis

1. Escalation matrix should be defined for incident diagnosis and resolution.

5.2.5 Resolution and Recovery

1. As a process, the service desk team should refer the known error database for documented workaround or solution prior to initiating diagnosis.
2. Change management process should be followed to implement a solution in a production environment.

5.2.6 Closure

1. On resolution, the service desk team and user should independently validate if the original state of services has been restored.
2. IT incident should be updated with closed status as soon as its resolution has been confirmed by the user.

5.3 Asset Management

360 ONE's IT assets shall be controlled and managed throughout the asset lifecycle

5.3.1 Asset Lifecycle

1. IT Asset acquisition request should be approved by respective department head and CTO.
2. All assets should be identified, classified and protected during their whole lifecycle as per the IS Policy - Asset Management.
3. All 360 ONE's Hardware IT Assets should be insured for damage, theft or loss.
4. The IT Assets should have a unique identification code and it should be maintained in the centralized database.
5. In case the retired IT assets needs to be destroyed, the process for disposal of media should be followed.
6. Asset Inventory should be updated upon retirement and disposal of assets.

5.3.2 Asset Records

1. An inventory of all assets shall be maintained and updated. The inventory should at least include the details of unique asset identification number, the asset owner, contact details, asset allocation period.
2. An inventory of all software licenses shall be maintained and updated in the database.

5.3.3 Asset Review

1. The inventory of assets should be reviewed at least annually.
2. The inventory of software licenses should be reviewed at least annually.

5.4 Application Management

1. 360 ONE shall manage the entire life-cycle of application including maintenance to provide resilience, availability of application in efficient and cost-effective manner.

5.4.1 Application Maintenance

1. Application Portfolio should be created with the record of the applications and content. Portfolio should be linked to supporting infrastructure and devices.
2. All resources required for managing and supporting the applications should be trained at least annually.

5.4.2 Continuity of Operations

1. Applications should be monitored for capacity, performance and availability.
2. Application should have a comprehensive EOD process plan to conduct activities in off business hours.

5.4.3 Application Assessment

1. Risk Matrix / Criticality Rating for the applications based on their risk criticality should be defined and reviewed at least annually.
2. Risk Assessment should be conducted for all applications on periodic basis.

3. Vulnerability Assessment and Penetration Testing should be conducted for all applications on periodic basis at a frequency and the test report with the action taken and mitigation plan to be submitted to CIO.

5.4.4 Training

1. Applications should be managed by personnel with appropriate technical skill sets and training.

5.5 Infrastructure Management

1. 360 ONE shall ensure efficient management of the IT infrastructure and build the technical capabilities to manage IT Infrastructure.

5.5.1 IT Infrastructure Management

1. Roles and responsibilities should be defined for managing and monitoring the IT infrastructure.
2. All IT infrastructure related incidents/ problems should be logged in the service desk.
3. Identified risks should be mitigated and communicated to stakeholders.
4. Network architecture diagrams as applicable to be maintained for any
5. application's infrastructure.

5.5.2 Continuity of Operations

1. Continuity should be ensured by executing the daily and periodic processes.
2. IT Infrastructure should be continuously monitored for threats and operational issues.

5.5.3 Training

1. Technical skills development activity should be conducted for the users/ teams, responsible for operating, maintaining and supporting the IT infrastructure at least half annually.

5.6 Access Management

Please refer to "Authorization & User Management" in Information Security & Cyber Security Policy.

5.7 Back up & IT DR Policy

1. 360 ONE shall manage the entire life-cycle of application including maintenance to provide resilience, availability of application in efficient and cost-effective manner.

5.7.1 Backup Strategy

2. Information backup and recovery procedures should be established and implemented as per legal, regulatory and contractual requirements.
3. Information backup frequency and retention period of backup should be defined based on identified requirements of backup.
4. Business-critical data should be duplicated and stored at different site. In case of backup media, the same should be kept in fireproof safe
5. Backup logs should be stored with appropriate access rights assigned to them. The backup operator should carry out a log analysis for all failed backup and restorations and take necessary actions including raising an incident.
6. Restoration testing should be conducted for the backed-up data on regular basis to check the integrity and adequacy of the backup.

5.7.2 Disaster Recovery Strategy

1. 360 ONE should ensure that disaster recovery capability is in place and tested sufficiently to ensure that ability of the company to provide service to its customers and secure its revenues can continue in the event of a disaster.
2. Time to recover access to the application, and the allowable data loss that can be tolerated after a disaster should be documented for all the critical applications.
3. Recovery testing should be performed at least once a year for all business-critical applications

5.8 PATCH MANAGEMENT

5.8.1 Objective

The purpose of this policy is to define patch management of the organisation's information systems, networks, data, databases, and other information assets.

5.8.2 Scope

All information technology systems, software, databases, applications, network and other information resources that are being used by the organization to conduct its business.

5.8.3 Policy

1. All the IT systems including servers, network & security devices, operating systems, applications, any information processing devices and applications shall be properly configured to install the recommended software updates to maintain operational efficiency.
2. Patches shall be identified and categorized according to their priority.
3. Security patches shall be given priority and deployed as soon as the testing is complete.
4. Servers managed by the organization shall apply regular patches as per the schedule.
5. Patches for business critical systems shall be carried out manually in a controlled manner.
6. All patches shall be tested prior to full implementation by deploying in a test environment that is similar to the production environment, wherever applicable.
7. A remediation plan that allows for return to the previous stable state prior to the patch deployment shall be devised in case a roll back is required.

6. IT Support for Business MIS

6.1 MIS Requirements & Support

360 ONE shall ensure compliance to all process identified in IT policy.

6.1.1 IT Support for Business MIS formulation and Compliance

The business user group shall be responsible for design of MIS requirements for monitoring business scenarios and requirements such as:

1. Performance MIS - A dashboard for the Top Management summarizing financial position vis-à-vis targets. It may include information on trend on returns on assets

across categories, major growth business segments, movement of net-worth etc.

2. Functional requirement for automation of Fraud alerting & design of Transaction Anomaly MIS System - The business teams may evaluate conceptualizing from time to time the functional requirement for aspects like:
3. Account Classification - System enabled identification, alerting and classification of Special Mention Accounts and NPA as well as generation of MIS reports in this regard.
4. Lending Transaction MIS -The MIS should facilitate pricing of products, especially large ticket loans and any alerts on deviation on lending terms.
5. Regulatory reporting & MIS - The MIS should capture regulatory requirements and their compliance.
6. Financial Reports including operating and non-operating revenues and expenses, cost benefit analysis of segments/verticals, cost of funds, etc. (also regulatory compliance at transaction level)
7. Treasury Transaction Reports- MIS Reports relating to treasury operations (including anomaly alerts like trade limit breaches, high volume transactions).
8. Fraud analytics and alerting - Suspicious transaction analysis, embezzlement, theft or suspected money-laundering, misappropriation of assets, manipulation of financial records etc. The regulatory requirement of reporting fraud to RBI should be system driven.
9. Integration of systems to regulatory reporting portals. E.g. COSMOS.
10. IT team along with the business teams shall provide an adequate infrastructure and support in updating business applications for generating MIS and automated control features wherever possible.