GOVERNMENT OF PAKISTAN

SECURITIES AND EXCHANGE COMMISSION OF PAKISTAN

-.-.-.-

Islamabad 22nd January, 2025

NOTIFICATION

S.R.O.76(I)/2025.- In exercise of the powers conferred by sub-section (2) of section 282B of the Companies Ordinance, 1984 (XLVII of 1984), the Securities and Exchange Commission of Pakistan hereby makes the following amendments in the Non-Banking Finance Companies and Notified Entities Regulations, 2008, and the same is hereby published for information of all persons likely to be affected and notice is hereby given that comments, if any, received by the Commission within fourteen days from the date of placement of the draft amendments on the website of the Commission will be taken in to consideration, namely:-

AMENDMENTS

In the aforesaid Regulations, -

(1) In regulation 2, in sub-regulation (1),-

(a) after clause (v), the following new clause shall be added, namely:-

"(va) "Cooling off Period" means period of one business day commencing from the date of issuance of investment report to the unitholder as per Circular No. 10 of 2022;";

(b) after clause (xiaaac), the following new clauses shall be added, namely:-

(xiaaaa) "Digital Asset Management Company (Digital AMC)" means a Fund Management NBFC licensed by the Commission to offer Digital Asset Management Services;"

(xiaaaab) "Digital Asset Management Services (DAMS)" means provision of the asset management services (AMS) to the customers/unitholders through Digital Platform with limited or no human interaction with the customer/unitholders;"

(c) after clause (xiaaab), the following new clause shall be added, namely:-

"(xiaaaba) "Digital Platform" means tool/application/software/solution which uses digital/IT as the primary interface between the Digital AMC, Investor/Unitholder and other parties involved in the process of offering DAMS and includes mobile phone application, web-based portal, internet-based channels, digital distribution/aggregation platforms and other enabling or supplementing support services;"

(2) After "Part V" the following new Part shall be added, namely: -

"Part VA

Requirements to undertake Digital Asset Management Services (DAMS) by the Digital Asset Management Company (Digital AMC)

67AB. The provisions of this part shall apply to Digital AMCs for provision of DAMS and digital services offered by the Asset Management Companies using or intending to utilize Digital Platforms for provision of their services to the customers/investors. The requirements shall be applicable to all Digital Platforms being administered, managed and/or owned by the Digital AMCs.

67AC. DAMS Licensing and Other Eligibility Requirements.- (1) A Fund Management NBFC, subsequent to grant of permission in terms of Rule 4 of the Rules, shall in addition to compliance of all requirements/conditions for grant of license as provided in Rule 5 of the NBFC Rules, shall clearly mention the intention to obtain a license for undertaking DAMS in Form-II of the NBFC Rules.

(2) The SECP in terms of sub-rule 6 and 7 of Rule 5 of the NBFC Rules may, if so satisfied, grant AMS license conditional to the restriction that such Asset Management Company (AMC) shall be eligible to provide DAMS only through digital platforms.

(3) A Fund Management NBFC at the time of application for grant of license to undertake DAMS and during its life, as the case may be, shall comply with the following additional requirements:

(a) A Fund Management NBFC desirous to engage in the business of DAMS, shall along with its application for grant of license, submit a viable business plan and comprehensive financial projections supported by underlying assumptions for a minimum of five years from the commencement of business; where such business plan shall encompass, but not restricted to, the following aspects:

(i). Detailed Digital Business Strategy demonstrating technological resources to offer DAMS;

(ii). IT Organogram outlining the Organizational Structure for IT Operations;

(iii). Evidence showcasing the capacity and expertise of human resources for executing Digital and IT Business Strategies for effectively providing DAMS to prospective investors;

(iv). Comprehensive Business Continuity Planning and Disaster Recovery Strategy Plan (BCP/DRP);

(v). Comprehensive Marketing Strategy with a special focus on retail outreach; and

(vi). Cyber Information Technology Security Strategy and details of Infrastructure Plans outlining data Security Measures.

(b) Such Fund Management NBFC in addition to the requirements under Schedule – I of the NBFC Rules and fit and proper criteria as laid down under Schedule – IX of these Regulations shall comply with following additional requirements for its board of director (BOD) and Key Executives:

(i) The BOD shall include at least one or 1/3 members, whichever is higher, with knowledge and high-level expertise along with a working/business experience of at least three years in emerging technologies and digital space. These technologies may include software development, cloud computing, open APIs, cybersecurity, advanced data analytics, artificial intelligence, and other similar domains. Prior experience of working in a fintech environment or digital infrastructure domain of a local or a foreign Financial Institution servicing retail clientele would be considered as a strong advantage.

(ii) In addition to the requirements regarding the statutory committees of the BOD, it shall establish a BOD level "Information Technology (IT) and Digital Risk Management Committee (the "Committee")" which shall hold its meetings at least quarterly. Such Committee shall also have representation of senior management from the following areas:

- Specialized Information Technology Department or a representative from the service-providing agency's IT Department;
- Risk Management Department;
- Compliance Department; and
- An Independent Director from the BOD.

The Committee shall be chaired by the Independent Director of the BOD. The committee shall be focused on designing policies and approving strategies for Digital and IT based services related issues including Digital Risk Management and Cyber Security with the objective to identify and mitigate IT-related risks, formulation of BCP/DRP policies and mechanisms, ensuring compliance with prevalent regulations, and overseeing cybersecurity measures. Furthermore, the

Committee shall play a critical role in strategic Digital/IT decision-making, vendor efficiency and risk management, and incident response planning. A focus on emerging technology trends shall also be essential aspects of its responsibilities.

(iii) Such Fund Management NBFC shall either establish its own IT Department/Function and the Cyber Security Function or it may utilize agency/outsourced services for the same. Such departments/functions or in case of outsourcing, the service providing agency, shall have a team led by the Chief Technology Officer (CTO) who holds strong qualification and relevant experience in the related fields. The Digital AMCs owing to fast changing needs of data and client identification security, are strongly encouraged to engage services of a Chief Information Security Officer (CISO) in addition to the CTO. The CISO if so hired, shall have a separate reporting line from the CTO. The CTO and CISO shall have the following minimum qualifications and experience requirements: -

Criterion	**Details**
Education	Bachelor's or Master's degree in computer science, information technology, information security, cyber security, software engineering, or a related field.
Professional Experience	5 years of experience in IT management, information security/cyber security management or Software Development or Networking or Cloud Computing or Data Analytics and/or Emerging IT trends, etc., preferably in the digital financial/fintech services industry.

67AD. Permitted Categories of CIS/Fund and Investor Mix.- (1) A Digital AMC will be eligible to offer DAMS for all categories of Open-End Collective Investment Schemes (CIS), provided it shall only offer DAMS for equity-based CIS if it appoints a Chief Investment Officer possessing the following competencies and capabilities:

(a) Qualification and Experience:

(i) Master’s degree in Finance, Economics, Business Administration, or a related field; or

(ii) Professional Qualification preferably a Chartered Financial Analyst (CFA) or similar certification (e.g. CAIA, FRM); and

(iii) A minimum of 5 years of fund management experience in equity with an AMC.

(2) At least 70% of the AUM of each open-end CIS, shall belong to retail investors at all times during the life of the CIS. However, a newly established perpetual CIS shall ensure compliance with the minimum level of retail investment in the following manner at close of each period after close of IPO:

Period from the date of IPO	**% of AUM**
12 Months	25%
24 Months and beyond	50%
36 Months and beyond	70%

Provided that, in case of fixed maturity CIS/Plan, compliance in terms of minimum of 70% of retail investments shall be ensured by close of Initial Public Offer or Subscription Period, whichever is later:

Provided further that, if the DAMC achieves a minimum retail investor mix of 50% within the first 12 months from the Initial Offering Period (IOP) or upon achieving a retail investment mix of 70% within 24 months from the IOP date, the DAMC may impose an additional charge of 0.25%, over and above the limit set forth in Regulation 67AG in conjunction with Regulation 60(5) of the Regulations for the respective CIS category:

Provided further that in case, the Digital AMC fails to ensure compliance with above mentioned thresholds, it shall immediately intimate the grounds to the Commission upon which it believes that the CIS shall be able to ensure requisite compliance within a reasonable timeframe not exceeding 90 days. Where the Commission is not satisfied with the reasons provided by the Digital AMCs, it may direct the Digital AMC or the trustee to revoke the CIS.

(3) A Digital AMC shall not qualify for registration as a Pension Fund Manager unless it has a minimum of three years of experience managing all categories of CIS. Upon achieving the requisite three years of experience across all CIS categories as specified, the Digital AMC may apply to the Commission for registration as a Pension Fund Manager. The Commission, after a detailed evaluation of the AMC's compliance with the below parameters, may grant approval for such registration:

(a) Strong track record of the DAMS provided by it;
(b) Status of compliance with minimum investor mix requirements for each CIS under the its management as stated under regulation 67AD(2) of the Regulations above;
(c) Stability rating of any of the CIS for which it acted or acting as a fund manager (where applicable) shall at least be AA-(f) by a Credit Rating Agency registered with the Commission;
(d) Performance (dividends/bonus, etc., to the unit holders) of the CIS under its management;

(e) HR and Operations strength and necessary skills to offer investment management in pension fund scheme business;

(f) Compliance track record of Digital AMC and CIS under its management with the applicable regulatory framework; and

(g) Client servicing efficiency, Complaint redressal mechanism and trend of monthly investors' complaint data.

(4) Any existing AMC licensed to undertake AMS business and desirous to provide DAMS only shall comply with the MER conditions in the following manner:

(a) The AMC may continue to meet MER as prescribed for AMS in the Schedule I (currently being Rs. 200/- million) to remain eligible for offering services to all segments of investors, including retail and corporate investors, without any minimum limit on retail segment ratio; and

(b) In the event that such an AMC chooses to convert to a Digital AMC by reducing its equity to meet MER as prescribed for a Digital AMC in the Schedule I, it shall adhere to the requirement of minimum investor mix as prescribed herein for Digital AMCs at the time of conversion and going forward. For clarity, such Digital AMC shall have at least 70% of its AUM of each CIS under its management belonging to retail investors.

67AE. Admissible Sales Load for CIS/Funds or other Charges.- Digital AMC shall be eligible to charge sales load or such other charges/onboarding charges as may be admissible for AMCs. However, the Digital AMC, may with a clear disclosure to the customer in terms of amount and %age, adopt any other feasible mechanism/mode for charging sales load; including deferment of the front-end load until the announcement of the first dividend by the subject CIS (without affecting the principal investment), or at the time of redemption request by the unitholder, whichever occurs earlier.

67AF. Minimum Maintainable Fund Size of CIS by Digital AMC.- (1) The minimum fund size (net assets) of a CIS shall be twenty-five million rupees at all times during the life of the scheme:

Provided that a newly established CIS other than fixed maturity scheme, shall ensure compliance with the minimum fund size requirement in two phases following its IOP period, i.e. attain a minimum of twelve million rupees within six months of the first day/date of the IOP period and ensure compliance with the overall minimum fund size within one year of the close of IOP period.

(2) The Digital AMCs are strongly encouraged to invest or arrange the investment of a seed capital of five million rupees for every new CIS for a minimum period of one year from the close of the IOP period, or until it satisfies the minimum fund size requirements as prescribed above shall be duly met, whichever is later.

(3) Subsequent to the closing of the IOP period; at any time, if the size of a CIS falls below the minimum fund size as specified above, the Digital AMC shall ensure compliance with the minimum fund size within three months of its breach.

(4) If the fund size remains below the minimum fund size limit for consecutive ninety days, the Digital AMC shall immediately intimate the grounds to the Commission upon which it believes that the CIS is still commercially viable and its objective can still be achieved along with following documents: -

(a) the unit holder's resolution passed by 3/4th in value of total outstanding units supporting Digital AMCs views:

Provided that the Digital AMC may use digital mechanism for voting by the unitholders which shall be duly certified by the trustee; and

(b) a time bound action plan to increase the fund size to the minimum requisite fund size for consideration of the Commission.

(5) Where the Commission is not satisfied with the reasons presented by the Digital AMC in terms of above sub-regulation (4), it may direct the Digital AMC or the trustee to revoke the CIS.

67AG. Total Expense Ratio (TER) and Risk Disclosures.- (1) The Digital AMC shall maintain TER of 0.50% less than the respective TER limits as capped in terms of regulation 60(5) of the Regulations.

(2) In matters of disclosure of expenses (TER, Management Fee and Trustee Fee) and sales load, the Digital AMC shall diligently adhere to the provisions outlined in Regulation 60(6) of the Regulations or such other instructions as prescribed by the Commission from time to time.

(3) A Digital AMC is eligible for the reimbursement of formation cost, subject to an audit of costs as applicable in terms of Schedule XIX of the Regulations. The formation cost will be systematically spread out and amortized over a period spanning not less than five years, or within the maturity date of the CIS, as applicable.

(4) The Commission may modify or amend such TER limits or may prescribe such other limits from time to time to preserve the best interests of the investors.

67AH. Cooling-Off Period for New/Subsequent Investment.- (1) A Digital AMC shall clearly communicate the availability of Cooling Off period to the individual unit holders on every transaction.

(2) The cooling-off right shall be exercised by the unit holder through the Digital Platform of the Digital AMCs within the specified cooling-off period.

(3) In case of exercise of cooling-off right within the cooling-off period by the unitholder, the Digital AMCs is obligated to refund any sales load paid by the unit holder. However, Contingent Load (the load charged upon redemption and which forms part of the CIS property) shall be borne by the

unit holder. However, the Digital AMCs are highly encouraged to avoid charging such Contingent Load without prejudice to the interests of other unitholders.

(4) The refund for each unit held by a unit holder exercising the cooling-off right shall be based on the Net Asset Value (NAV) per unit applicable on the date the right is exercised by the unitholder. However, in such cases, Digital AMCs may recover the actual costs incurred for client identity verification, such as NADRA Verisys charges or other third-party verification costs, provided these costs are clearly attributable to the individual investor and pertain to their first-time onboarding. This cost recovery or deduction shall not apply to subsequent investments by the same investor.

67AI. Net Asset Value Dissemination and Disclosures.- (1) The Digital AMCs shall announce daily NAV of all CIS (except for fund of funds scheme) under management latest by 18:30 hours on their own Digital Platforms as well as on MUFAP's website. The NAV of Fund of Funds scheme(s) shall be announced by 10:30 hours of the next business day.

(2) The Digital AMCs shall ensure that the NAV disclosed and reflected on all digital forums (such as application, website, portal etc.) shall be uniform at all times. In case of any loss to the unitholder due to any discrepancy in disclosure of NAV on digital platforms, the Digital AMCs shall compensate the respective unitholders within 7 working days of becoming aware of such discrepancy.

(3) The Digital AMCs are strongly encouraged to deploy latest investment performance disclosure tools/graphics to make it easy for the investors to understand both quantitative and qualitative movements of their investments, especially in comparison to the performance benchmarks and/or risk adjusted returns.

67AJ. Requirements in case of Appointment of Distributor.- (1) The Digital AMCs shall sale the units of a CIS digitally through distributors that undertake distribution functions through digital means. The Digital AMCs shall enter into a written agreement with the distributors clearly stating the terms and conditions for avoidance of fraud and mis-selling of CIS units.

(2) The Digital AMCs may engage distributors beyond those classified as digital distributors. However, these distributors must ensure that onboarding and/or investment/redemption and all transactions by unitholders or prospective unitholders are conducted in a paperless manner through a fully integrated Digital Platform based ecosystem.

(3) The Digital AMCs is obligated to inform the Commission within thirty days of signing a distribution agreement with a distributor, along with an undertaking that the distributor has undergone pre-screening by the Digital AMC for compliance with relevant regulatory requirements, including but not limited to licensing, cybersecurity, risk disclosure, Anti-Money

Laundering & CFT Compliances, and data protection (as per the prevailing regulatory framework). Additionally, the Digital AMCs must include the names and details of their appointed distributors in their audited annual financial statements.

(4) The Digital AMCs shall be responsible for the acts and omissions of all persons to whom it may delegate any of its functions including the distribution function, as if they were its own acts and omissions.

67AK. Guidelines for Unitholders relating to Investment and Redemption Process.- (1) The Digital AMCs shall develop and make available to the users/unitholders, the comprehensive guidelines outlining the unitholders' journey for investments and redemptions through their Digital Platforms. The Digital AMCs are encouraged to use the latest educational and mass awareness techniques to ensure that investors make well-informed decisions.

(2) The Digital Platforms shall include and prominently display a dedicated 'Help or Contact Us' button easily accessible to users/unitholders, which shall offer essential information about a designated contact person responsible for the prompt resolution of any issues, complaints, or queries raised by the investors.

67AL. Prerequisites for Qualifying to be listed in SECP's Approved Digital Platform List.- (1) The requirements as prescribed under this regulation are applicable to Digital AMCs as well as the AMCs which are utilizing Digital Platforms for provision of services to their investors/unitholders. No licensed Digital AMC shall launch or make available to the public its Digital Platform without seeking NOC from the respective trustee and without listing it on the SECP's website. Following requirements shall be applicable as pre-qualification for listing of Digital Platforms on SECP's website:-

(a) Prior to the launch of the DAMS Digital Platform, the Digital AMCs shall seek No Objection Certificate (NOC) from the appointed Trustees for its Digital Platform in the following manner:-

(i). The Company Secretary or the CEO of the Digital AMC shall be required to submit a compliance certificate to the Commission as well as the Trustee(s), duly signed, affirming that the Digital AMC has adhered to requirements of these regulations including the additional requirements for the Composition of BOD, BOD Committees and Key Executive(s).

(ii). The respective trustees (if more than one for different CIS), after conducting due diligence and ensuring the effective compliance of the Digital Platforms in all aspects, including evaluation of both software and hardware infrastructures through

User Acceptance Testing (UAT), shall issue the requisite NOC.

(iii). The Digital Platform shall become live within six months of the grant of NOC by the Trustees under intimation to the Commission.

(b) The Digital AMCs are encouraged to comply with the below listed standard guidelines as may be amended/improved/replaced from time to time:

(i). Open Web Application Security Project (OWASP) Mobile Application Security Verification Standard;

(ii). OWASP Mobile Application Security Testing Guide; and

(iii). OWASP Web Application Security Testing.

(c) The Digital AMC shall ensure that at the time of accessing/registration of the users/investor; which shall be subsequent to the legitimate download or gaining access of any Digital Platform, all important requirements related to the respective Digital Platform, associated investment risk factors and terms governing the access to user data/information, shall be provided to such user/investor in a summary form along with a warning/disclosure or a prompt (pop up).

(d) The Digital Platform shall be subject to IT/Info Security Audit, once every three years by an Independent Audit Service Provider having qualified Certified Information Systems Auditor (CISA)/Certified ISO27001:2013 Lead Auditor Certification to check compliance with regulatory requirements. The Digital AMC shall submit the report to the Trustee, its external auditor and the Commission within three months of the end of the respective financial year.

(e) The Digital AMCs providing DAMS or AMCs providing services through Digital Platforms shall ensure that adequate cybersecurity measures and controls are in place to ensure confidentiality, integrity and availability of the data and information. The controls shall include but not limited to:

(i). Secure Access Management infrastructure ensuring:

- Implementation of approved policies and procedures for secure access management are available;
- Policy of disabling user accounts of such employees who have left the organization in an immediate manner is effective;
- Separation of user accounts across technology environments e.g. separate accounts to be used in development, test and production environments;
- All IT administrative activities are performed using Privilege (Admin) Access Management Solution;

- Minimum number of such Privilege (Admin) access user accounts with formal approval requirements and complete log of activity/access;
- Clearly defined and efficiently implemented Inventory of Privileged Accounts and review frequency;
- Access rights review document/policy for application is in place;
- Creation, modification of rights, revocation of rights are performed after approvals from line manager with a clear policy framework in place;
- Strong password policy is implemented which covers password complexity, minimum length, history and minimum age;
- Access control requirements for information and information systems based on business needs and classification of information are defined considering the principle of least privilege access;
- Shared accounts are discouraged unless approved by the CTO/CISO for a documented business reason;
- Services accounts are configured to:
    - disable interactive logon; and
    - be monitored for inappropriate use.
- Configure maximum number of failed attempts of authentication for user and service accounts, after which access to the accounts shall be blocked;
- User access requests for third-party service suppliers shall be approved & validated subject to the condition that access is restricted to services supplied under contracts or agreements;
- User accounts for third-party service suppliers shall be disabled upon expiry or cessation of contract or agreement; and
- Implementation of multi-factor authentication shall be ensured for registration/signup of users.

(ii). Perimeter and Network Security is effective to:

- Maintain high level network diagram of mobile application environment indicating the location of network devices, app and database servers and other attached components;
- Ensure implementation of adequate security measures to protect against unauthorized access or attacks;
- Validate that inbound security policies are enabled for in scope application environment;

- Secure authentication mechanism is in placed to ensure that only Trusted Users are allowed to access the applications;
- Logging and monitoring process on firewall are in place;
- Validate the details of Encryption mechanism, Transport Layer Security (TLS) version, Digital certificate on application portal;
- Prevent malware, such as viruses, spam, phishing attacks, denial-of-service attacks and other unauthorized access attempts, using specialized network security software and other appropriate prevention and detection resources, such as firewalls, intrusion detection systems and intrusion prevention systems;
- Regularly review all software associated with network perimeter breach prevention systems and applications and the rules for analyzing suspicious code are updated regularly to remain current with existing and unplanned threats; and
- A formal process is established and documented for identifying possible breaches in the network perimeter, capturing and containing the malicious code if possible, assessing the breach, determining the nature and impact of the breach, notifying management of the breach, minimizing the impact of the breach and documenting the steps taken when dealing with the incident. This process will apply to all network perimeters, whether internal, hybrid and/or public clouds.

(iii). Endpoint, Server and cloud security:

- Versions and patches of all endpoints are updated till stable versions and secured;
- Ensure that software installation and upgradation rights on servers/instance is only limited to the Authorized Person;
- Software installation on endpoints are restricted and approved on a need-to-use basis;
- End point must be secured using well known end point security solution including Endpoint Detection and Response (EDR) & advanced threat detection capabilities; and
- Implementation of Continuous Threat monitoring external service including digital risk to identify any security weakness at the internet exposed infrastructure for timely remediation.

(iv). Application level Security ensuring:

- All the components required for the application such as webserver and other components are updated and running on latest stable versions;
- Web Application Firewall (WAF) are effectively implemented on customer facing interfaces;
- Details are maintained on the latest Vulnerability Assessment and Penetration Testing (VAPT) conducted at least on annual basis of digital platforms, in-scope system, IT Infrastructure and database;
- APIs are not using outdated Secure Sockets Layers (SSL)/Transport Layer Security (TLS) protocols;
- Secure Software Development Life Cycle (SSDLC) process during each phase must be implemented which will include Static Application Security Testing (SAST) & Dynamic Application Security Testing (DAST) activities before promoting any release to production environment; and
- API security requirements must be considered including Weak authentication/authorization controls, misconfiguration, business logic abuse (credential stuffing, account takeover), Server-side request forgery (SSRF).

(v). Data Security:

- Data security policy and procedure are in place;
- Classification of data against pre-defined categories in light of the approved policy;
- Relevant documentation is maintained and reviewed at a defined frequency to ensure adherence and effective implementation;
- Appropriate access controls are established for accessing the data, including requiring authentication for access, which is not public;
- Encrypt data at rest (including backups) and in transit use strong and non-obsolete cryptographic algorithms;
- Appropriate measures are undertaken to avoid accidental deletion or overwrite of data/information;
- Ensure that the separate channels are being used for storage and transmission of critical data; and
- Appropriate controls must be implemented for the prevention of data leakage incidents.

(vi). Incident surveillance and monitoring;

- Ensure that incident management Policies and Procedures are in place for Incident Management and Reporting covering responsibilities for planning, detecting and responding to cyber security incidents, resources assigned to cyber security incident planning, detection and response activities including guidelines for triaging and responding to cyber security events and cyber security incidents;
- Ensure that the anomalies are detected and resolved in a timely manner;
- Ensure that incident management procedure is implemented and appropriate reporting matrix for such incidents is maintained;
- Incident response functions shall be implemented in application system, responses to any incident should be documented for record;
- Ensure that cyber security incident response plan is exercised during regular intervals to ensure it remains fit for purpose; and
- Ensure that the potential risks and vulnerabilities are identified in a timely manner, which could impact business continuity.

(vii). Vulnerability Management:

- Ensure that security patches or updates are being identified & applied in a timely manner to applications, operating systems, drivers and firmware. It is essential that all assets are regularly identified within the environment using an automated method of asset discovery via an asset discovery tool or a vulnerability scanner. Moreover, ensure reviewal and updating of the risk assessment.

(viii). Patch Management:

- Log of patches deployed are documented;
- Formal process of approval is in place for patch testing, User Acceptance Testing (UAT) and migration to production;
- Approved patch management policies and procedures should be in place;
- Procedure for approval of tested patches should be defined. UATs of the patches should be in segregated environment; and
- Validate that patches are applied on test system first before provisioning to live.

(ix). Logging and backups:

- Validate that policies and procedures are approved and implemented for Backup and recovery of in-scope application

- Validate that appropriate logging with sufficient details is enabled at application, platform, database and operating system levels;
- Validate that log file should be tempered proof, even system administrator not have access to modify own logs and logs must be secured at directory levels;
- Frequency of backups should be defined in the system for both production and development and the same shall be documented in relevant policy;
- Backups must be encrypted;
- Adopt the 3-2-1 rule for data storage i.e. have 3 copies of information (1 original and 2 backups), saved on 2 different media types, with 1 copy kept off site;
- Back-ups maintained must be kept immutable form. It would be more appropriate to consider air-gapped backup solution ensuring the availability of clean copy of back-up in case of a ransomware attack;
- Data restoration process should be in place in application system and documented; and
- Backup logs should be generated and verification of the backup restoration log should be in practice.

(f) The Digital AMCs shall:

(i). develop a policy governing Digital Platform's business objectives, standards, compliance, guidelines, controls, responsibilities and liabilities. As a principle, the policy shall achieve a balance between the security of Digital Platform, convenience and performance. The policy shall at least be revisited annually by the relevant Committee of the BOD and/or when a significant change is made in the business environment;

(ii). ensure compliance of all applicable laws in force in Pakistan related to cyber security, personal data protection, cloud usage and data privacy;

(iii). be responsible for any digital fraud as a result of security lapse, operational issues, architecture or any other malfunction of the digital platforms;

(iv). be responsible for loss of any unitholder due to delay on their part in taking timely remedial and control measures such as delay in announcement of NAV, blocking digital platforms in case of any cyberattack, delay in disposing dispute requests in a timely manner, etc. In this regard, the Digital AMCs shall compensate for such losses to the unitholders;

(v). avail cybercrime insurance policy to indemnify losses that may arise due to cyber-attack/cybercrime on their digital platforms; and

(vi). ensure compliance with the additional requirements relating to the Smartphone Application, as provided in Schedule XXIV to these Regulations.

(g) The Digital AMCs are encouraged to offer transactional insurance to its unitholders for Debit Card Services or similar offerings, at reasonable and competitive rates. Activation of the insurance shall require clear disclosure and the explicit consent or request of the unitholder.

(h) Data related to Personal Identifiable Information (PII) shall not be stored on any cloud infrastructure outside the jurisdiction of Pakistan.

Explanation: PII means any information relating to an identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier.

However, the global cloud infrastructure resources and computing services may be utilized, including but not limited to networks, servers, applications, and services such as on-demand self-service, broad network access, and resource pooling.

Furthermore, when utilizing software application services through global cloud infrastructure, Digital AMCs shall ensure the encryption or anonymization of customers' PII, preventing their identities from being readily inferred.

For purposes of clarification, the Digital AMCs shall store sensitive PII within Pakistan with one cloud provider, while it may employ another local or foreign cloud provider for specific software application services. These services may include, but are not limited to, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Function as a Service (FaaS), Backup as a Service (BaaS), Disaster Recovery as a Service (DRaaS), or Security as a Service (SECaaS).

Data collected by Digital AMCs through Digital Platforms is subject to privacy of the investor/unitholder/user and shall be used only for activities related to registration and operations of an account by an individual with the respective Digital AMCs. A Digital AMC shall keep the data of the investor/unitholder/user strictly confidential, except in the following circumstances:

(i). Disclosure of information with the specific written or recorded consent of investor/unitholder/user.

(ii). Release, submission or exchange of information with other financial institutions/licensed entities for transaction processing including Centralized KYC/AML/CFT screening activities.

(iii). Disclosure of information upon orders of a court of competent jurisdiction or any government office or agency authorized by law.

(iv). Disclosure to third party service providers solely for the purpose of assisting or rendering services to the Digital AMC in the administration and provision of its DAMS business; and

(v). Disclosure to third parties such as insurance companies, solely for the purpose of insuring the investor/unitholder/user from fraud or unauthorized charges.

(i) The BCP/DRP shall be approved by the Committee on Information Technology and Digital Risk Management and endorsed by the BOD:

Provided that, the Specialized Information Technology Department, or the service provider in the case of outsourcing, shall maintain a comprehensive log of frequent Disaster Recovery Testing (DRT), which shall be conducted at least quarterly. A summary report of DRT shall be shared with respective Trustees and the Commission on semi-annual basis.

(2) DAMS may simultaneously be provided through an App and the Digital AMC's website or any other form of Digital Platform.

(3) A Digital AMC shall conspicuously disclose its full corporate name and licensing status (including license no.) on its Digital Platforms, documentation, published materials and advertisements.

(4) The Commission subsequent to grant of NOC and confirmation from the respective Trustee(s) shall maintain and publish the list of the Digital Platforms on the official website of the Commission.

(5) In case of a smart phone application, the Digital AMC at the time of launching of such app shall provide license status along with NOC granted by the Trustees for respective App to Google Play Store and/or App Store. Proof for the same shall subsequently be provided to the Commission and maintained by the Digital AMC as record. The app on Google Play Store/App Store (Apple Inc.) shall only be hosted with the URL which is provided on SECP Approved Digital Platform List.

(6) The Digital AMC, subsequent to the listing of its Digital Platform on the Commission's website, shall conduct third-party vulnerability assessments, penetration testing, and performance evaluations of the Digital Platforms on an annual basis from the date of listing, with due intimation to the respective Trustees and the Commission.

(7) In case of any violations or breaches occur after the launch of a Digital Platform, the Trustees reserves the right to revoke the previously granted NOC and to report the same to the Commission. The Commission upon such intimation by the Trustee, may initiate regulatory

proceedings against the respective Digital AMC and remove the name of the non-compliant digital platform from the list.

67AM. Compliance Reporting and Grievance Redressal Mechanism/Guidelines.- (1) The Digital AMC shall:

(a) ensure compliance with the requirements as laid down under Circular No. 01 of 2010 dated January 15, 2010 related to Specialized Companies Return System (SCRS) or any other subsequent requirement as may be specified from time to time by the Commission;

(b) conduct a self-assessment every six months to evaluate its compliance with the prevailing regulatory framework, including the specific requirements of this Circular, and must duly inform its BOD of the results;

(c) prepare and submit a monthly report to the Commission, containing unitholders' data for each CIS under its management. The unitholders shall be categorized into two distinct classes, namely "corporate" and "retail. The report shall include, but not be limited to, the following information for each class of unitholders:

(i). Total number of unitholders in each class (corporate and retail);

(ii). Total number of units held by each class of unitholders;

(iii). Aggregate value of assets held by each class of unitholders;

(iv). Any significant transactions or changes in the CIS's composition affecting each class of unitholders;

(v). Any material information or disclosures relevant to the interests of corporate and retail unitholders; and

(vi). Gender Disaggregated Data as per Schedule XXIV-A.

(d) share a monthly list of distributors appointed for distribution of CIS on Digital Platform along with following details:

(i). Total Monthly CIS Sales through the distributors (digital distributor and other than digital distributor AUM); and

(ii). Percentage of CIS Sales through Digital Distributor and other than digital distributor on cumulative basis.

(2) The Digital AMCs shall:

(a) establish and implement written policies and procedures to ensure that complaints from investors are handled in a timely and appropriate manner.

(b) develop an efficient complaint management process for effective handling of related complaints. It shall prominently display on its website the Complaint redressal mechanism. A system shall be developed whereby the investors can lodge their complaints through the following multiple channels:

(i). Call Centre – Investor shall be able to call at a toll-free number of the digital portal/platform/website during the business hours; Such access may also be offered through other cost-effective mediums of audio/visual communication (i.e., whatsapp messaging, call or any other). Code of Conduct for Call Centers is enclosed as Schedule XXIV-B.

(ii). Details of Dedicated Point of Contact – Provide name, designation, email address and phone number of personnel designated to deal with DAMS related enquiries and complaints/issues; and

(iii). Lodge Online Complaint – Investor shall also be able to lodge his/ her complaint through a complaint form available at the digital platforms.

(c) Every Complainant shall be given a unique Complaint Number for future tracking and all necessary information of the complainant including nature of complaint shall be logged to facilitate its investigation and resolution;

(d) specify maximum timelines for acknowledgement and resolution of complaints; and

(e) report to the Commission on a monthly basis, the following information:

(i). No. of complaints outstanding from previous month;

(ii). Total no. of complaints during current month;

(iii). Nature of repetitive complaints;

(iv). No. of complaints resolved;

(v). No. of complaints outstanding;

(vi). Satisfaction ratio;

(vii). Average time taken for disposal of a complaint; and

(viii). Monthly trend analysis of complaints received and disposed.

67AN. Conversion of an Existing AMC into a Digital AMC and Vice Versa.- An existing AMC that holds a valid license from the Commission to undertake AMS may be converted into a Digital AMC, subject to prior approval of the Commission. To proceed with this conversion, such an AMC shall apply for a revised license specifically for DAMS. This application should include:-

(a) Application on Form – II of the NBFC Rules along with an undertaking to surrender the existing AMS license upon grant of DAMS license;

(b) Copy of existing valid AMS License;

(c) Approval of the BOD for conversion into a Digital AMC;

(d) Approval of shareholders for conversion into a Digital AMC (if applicable);

(e) NOC for conversion from respective trustees of all CIS under management;

(f) Business Plan as per requirements of the Circular including details/profile of requisite human resource evidencing the capacity and expertise for providing DAMS;

(g) Profiles of proposed existing BOD for DAMS;

(h) Profile of CTO heading specialized Information Technology Department;

(i) An undertaking, confirming its compliance with the chosen MER condition at the time of application for DAMS and additional requirements regarding Composition of the BOD, Committees of the BOD and Key Executives under clause 3.2;

(j) Undertaking of compliance with the necessary requirements outlined in this circular, as well as other relevant requirements under prevalent regulatory framework;

(k) The subject applicant shall prior to issuance of DAMS license shall surrender its existing AMS license to the Commission in original; and

(l) Following its conversion, such converted Digital AMC shall seek the Commission's approval to continue managing pension funds (if any), as per the criteria specified under regulation 67AD(3) of the Regulations:

Provided that, if the converted Digital AMC is not granted authorization to manage pension funds, it must adhere to the following requirements with respect to the pension funds it currently manages: -

(i). Make immediate arrangements in terms of Rule 6 of the Voluntary Pension System Rules, 2005 for transfer of the management rights of pension funds under its management and subsequently cancellation of its registration as Pension Fund Manager;

(ii). For the CIS under its management, it shall ensure compliance with the following minimum level of retail investment in each year of the post conversion period:

Post Conversion Period	**% of AUM**
12 months	35%
24 months	70%

Provided that, for every new CIS, at least 70% of its AUM shall belong to retail investors to be achieved in a period as specified in regulation 67AD(2) of the Regulations:

Provided further that, in case such a converted Digital AMC fails to ensure compliance with above mentioned thresholds, it shall immediately intimate the grounds to the Commission upon which it believes that the CIS shall be able to ensure requisite compliance within an extended timeframe not exceeding 90 days or such other time period as may be ascertained by the Commission on case to case basis. Where the Commission is not satisfied with the reasons provided by such converted Digital AMCs, it may direct the subject converted Digital AMC or the trustee to revoke the CIS.

(m) A Digital AMC may convert into a conventional AMC upon compliance with the relevant provisions under prevalent NBFC Regulatory Framework including requisite MER compliance.

67AO. Applicable Requirements for AMCs offering AMS through Digital Platforms to their Investors.- AMCs which are using Digital Platforms prior to the date of these requirements or which intend to utilize Digital Platforms for provision of AMS services to their investors:

(a) shall ensure compliance with additional applicable requirements in terms of regulation 67AC of the Regulations regarding composition of the BOD and constitution of the Committee of the BOD within three year or forthcoming election of the board whichever is earlier and for the Key Executive within a time of one year from the date of grant of NOC by the Trustees. In this regard, the concerned AMC shall also submit a duly signed compliance certificate by Company Secretary to the Commission;

(b) may apply sales load as allowed under regulation 67AE of the Regulations;

(c) shall ensure compliance with regulation “67H”, “67AI”, “67AJ” and “67AK” of the Regulations in their entirety;

(d) shall comply with the provisions set forth in regulation “67AL” of the Regulations including but not limited to seeking NOC from the respective Trustees in compliance of sub-regulation “67AL(1)” and listing of their Digital Platforms on Commission’s website in terms of sub-regulation “67AL(4)” of the Regulations within twelve months (year since the date of issuance) of the issuance of these requirements; and

(e) shall ensure compliance with Regulation “67AM(1)(b), (c) and (d)”, as well as sub-regulation “2” in its entirety.

Note: The Digital AMC shall adhere to all the applicable requirements as applicable for a conventional AMC under the NBFC Regulations, Circulars and Directives, unless expressly modified or relaxed by the above-stipulated requirements.

(3) In the Schedules after the Schedule XXIII, the following three new Schedules, "Schedule XXIV", "Schedule XXIV-A" and "Schedule XXIV-B" shall be added namely:

"Schedule XXIV

Requirements for Mobile Apps by the Digital Asset Management Companies

[See Regulation 67AL(1)(f)(vi)]

Note: The term **"Company"** is used as replacement for **"Digital Asset Management Company"**.

App Requirements – covers the entire mobile app ecosystem involved in capturing, storing, processing and transmitting financial/non-financial information. The Companies are responsible to ensure that their mobile apps and associated infrastructure is aligned with these requirements. The Company may develop mobile apps in-house, through outsourcing or by a combined approach. To manage mobile app development projects, Company shall:

(i) Put in place necessary app documentation including manuals on development, testing, trainings, production, operational administration, user guides and Service Level Agreements (SLAs);

(ii) Carry out vulnerability assessment, penetration testing and performance assessment of mobile apps to ensure effective and smooth operation before deploying the same in production environment;

(iii) Carry out system and user Acceptance Testing in an environment separate from the production environment; and

(iv) Put in place an escrow arrangement in case where third-party vendors develop mobile apps but the source codes are not released to the Company.

A. Architecture of App

(i). The Company shall be responsible for development of a standard architecture based on set of security principles, rules, techniques, processes, and patterns to design a secure App;

(ii). The entire development of App shall revolve around the architecture principles, which can be updated based on the learnings during the course of development of application layers (or equivalent) and operational usage and consumer feedback;

(iii). The Company shall ensure that the App architecture is robust and scalable, commensurate with the application volumes and user growth. For this purpose, a robust capacity management plan shall be put in place to meet evolving demand.

B. Device Registration/Binding

(i). The Company shall implement a flexible device registration/binding functionality using multiple properties unique to the device (such as IP address, location, remote server, time of the day, device type, location, PIN code, Wi-Fi information, screen size, browser, etc.) so that only registered devices are allowed to access backend servers.

(ii). The device registration/binding shall preferably be implemented using a combination of hardware, software and service information. In case, multiple devices are registered by a user:

a) the user must be notified of every new device registration on the registered mobile number, email or phone call; and

b) The Company shall maintain record of all registered devices, providing the user a facility to disable a registered device.

C. Authorization and Authentication of the User

(i). The Company shall ensure that explicit customer/user/unitholder/investor consent in a convenient manner is obtained before allowing registration of App;

(ii). A login authentication shall be in place.

(iii). The Company shall ensure that the access to personal data is protected by strong customer/user/unitholder/investor authentication mechanism including:

a) Implementation of multi-factor authentication (MFA) for registration of App user-account;

b) Strong and configurable PIN/password/pattern or a biometric credential such as face recognition or fingerprint recognition;

c) Time-based one-time passwords (TOTP) for authentication;

d) OTP auto-fetching functionality. The validity of OTP shall not exceed more than 120 seconds.;

e) Configure maximum number of failed attempts of authentication after which access to the app is blocked;

f) Define maximum duration for termination of inactive mobile service sessions. Maximum duration for termination of inactive mobile service sessions shall not exceed thirty minutes;

g) Ensuring that user authentication shall be processed only at the app owner's server-end; and

h) Ensure that authentication attempts are logged and monitored to detect login anomalies and possible breaches.

D. Protection of Sensitive Personal Data

(i). The Company shall ensure that sensitive information is not stored in a shared store segment with other App on mobile devices. It is recommended to utilize only the device internal storage, which is virtually sandboxed per app or preferably in a container app without meddling with other applications or security settings of the mobile devices;

(ii). The Company shall ensure that confidential data is deleted from caches and memory after it is used and/or uninstalled. Further, The Company shall ensure that App erase/expire all application-specific sensitive data stored in all temporary and permanent memories of the device during logoff or on unexpected termination of app instance.

(iii). Customer credentials and transactional data shall be encrypted while in-transit and at rest using strong, internationally accepted and published standards for key length, algorithms, cipher suites, digital certificates and applicable protocols that are not deprecated/ demonstrated to be insecure/ vulnerable;

(iv). Encryption keys shall only be stored with appropriate robust security controls and shall remain in a non-exportable form in a highly secure and standard key store. It may be bound to the secure hardware (e.g. Trusted Execution Environment, Secure Element for Android or its equivalent on any other platform). Further, Key Use Authorization shall be implemented, which should not be changed after generation of keys.

E. Network and Interfacing Security

(i). The Company shall ensure to enforce secure communication during the session establishment, exchange of data among App and backend services (including microservices);

(ii). Transport layer encryption shall be implemented for all communications between the App and app servers.

(iii). The Company shall setup their own Trust Manager to avoid accepting every unknown certificate. App shall use valid certificates issued by a trusted certificate authority;

(iv). App shall have inbuilt controls to mitigate bypassing of certificate pinning;

(v). App shall cease operations until certification errors are properly addressed;

(vi). The Company shall ensure that App must be able to identify new network connections and appropriate controls shall be implemented under such circumstances;

F. Session Management

(i). The Company shall ensure that App has automatic user-logoff functionality after a configurable idle time-period not exceeding thirty minutes;

(ii). The Company shall ensure that App has an easy to use and clearly visible logoff method;

(iii). The Company shall ensure that App erase/expire all application specific sensitive data stored in all temporary and permanent memories of the device during logoff or on termination of app instance;

(iv). The Company shall ensure that a procedure is in place to detect multiple simultaneous login attempts and immediately communicate it to the concerned user through alternate channels such as callback, SMS, email etc.

G. Tampering Detection

(i). The Company shall implement necessary checks on the server-side to verify App integrity and to detect any manipulation.

(ii). The Company shall ensure that installation of App is not allowed on rooted/jail broken devices;

(iii). The Company shall ensure that App is not allowed to run inside a debugger/emulator. For this purpose, App shall have debugger/emulator detections in place. Further, The Company shall not allow any third party to debug the application during runtime.

H. App Permissions

(i). The Company shall ensure to restrict data shared with other applications on the device through fine-grained permissions;

(ii). The Company shall ensure to minimize the number of permissions requested by the app and ensure that the permissions correlate to functionality required for the app to work. App shall defer or relinquish permissions when the same are no longer needed;

(iii). Unless for a specific business requirement in accordance with the security architecture principles, The Company shall not allow users to navigate to other App, sites or view objects that are not trusted and outside of app environment.

I. Secure Coding

(i). The Company shall ensure that their App developers adhere to industry accepted secure coding practices and standards;

(ii). The Company shall ensure that security libraries offered by mobile operating systems are correctly designed and implemented and that the cipher suites they support are sufficiently strong. Accordingly, The Company shall only use necessary and secure services, protocols, components, and dependent software and hardware, including those provided by third parties.

(iii). The Company shall document all required protocols, services, components, and dependent software and hardware that are necessary for any functionality of the application.

(iv). The Company shall have knowledge of all off-the-shelf libraries/modules/components utilized in the development of App;

(v). The Company shall ensure that code signing is used for the App to confirm the software author and guarantee that the code has not been altered or corrupted since it was signed;

(vi). The Company shall ensure that private key used for code signing is generated, securely stored and appropriately backed-up;

(vii). The Company shall ensure that minification and source code obfuscation techniques are used in the App;

(viii). The Company shall ensure to review application code prior to release to customers after any significant change, to identify any potential coding vulnerabilities;

(ix). The Company shall verify that App is not vulnerable to common coding vulnerabilities by performing manual or automated penetration testing that specifically attempts to exploit injection flaws, buffer overflow, insecure cryptographic storage, insecure communications and improper error handling etc.

J. Input and Output Handling

(i). The Company shall ensure that any input coming from the client that is to be stored in databases is properly validated to avoid SQL injection attacks;

(ii). The Company shall ensure that input and output data is properly sanitized and validated at the server and at the client-end;

(iii). Auto-complete feature shall be disabled for sensitive information such as login IDs and passwords;

(iv). Clipboard/copy-paste function shall be disabled for sensitive data. The Company may also use in-app keypad/ keyboard to capture the input from users.

K. Error and Exception Handling

(i). App shall have a proper error-handling mechanism and all errors shall be logged in the server.

(ii). Sensitive information and/or hints shall not be disclosed in error/warning messages and notifications;

L. Monitoring, Logs and Data Leakage

(i). The Company shall ensure that the app usage behavior is maintained and monitored through automated mechanism and deploy tools to identify any anomaly in the usage and behavior. The mechanism shall integrate with complete process of customer support for verification to clear the anomaly for consumer protection;

(ii). The Company shall ensure that App logs do not contain any sensitive data and where essentially required should be masked such that it no longer remains directly constructible in its complete form by collating components;

(iii). The logs shall be stored separately from the application/database servers and protected with appropriate access controls;

(iv). The Company shall implement appropriate security safeguards to protect the logs from unauthorized modification or destruction;

(v). The Company shall ensure that all the ecosystem logs are available for audits;

(vi). The Company shall implement appropriate control to protect transactional data/information against any loss or damage;

(vii). Server access controls and audit logs shall be maintained at the server level as per data retention policy.

M. App Vulnerability Assessment, Patching and Updating

(i). The Company shall ensure that the App has passed through extensive and recursive vulnerability assessment, scan and intrusion tests to identify weaknesses in app through both internal and independent assessors;

(ii). The Company shall ensure that the vulnerabilities identified during assessment scans, usage of the app or through independent identifier sources are fixed and updated to respective platform stores;

(iii). The Company shall ensure notifying users about update and enforce it within a grace period depending upon the criticality of fixes. The information about fixes shall be published in app release notes.

N. Application Programming Interface (APIs)

In order to establish adequate safeguards to manage the development and provision of APIs for secure delivery of third party provided services through App, The Company shall implement following measures:

(i). Establish security standards for designing and developing secure APIs including measures to protect the API keys or access tokens, which are used to authorize access to APIs to exchange confidential data. The Company shall define and enforce a reasonable timeframe for access token expiry to reduce the risk of unauthorized access;

(ii). A well-defined vetting process shall be put in place for assessing the appropriateness of third parties in connecting to the App via APIs, as well as governing third-party API access. The vetting criteria shall consider third party's nature of business, security policy, industry reputation and track record amongst others;

(iii). Perform risk assessment before allowing third parties to connect to their systems via APIs, and ensure the security implementation for each API is commensurate with the sensitivity and business criticality of the data being exchanged;

(iv). Strong authentication and access control mechanism to authorize and control access to designated API services in order to safeguard customer information;

(v). Strong encryption standards and key management controls to secure transmission of sensitive data through APIs;

(vi). The Company shall have the ability to log the access sessions by the third party(ies), such as the identity of the third party making the API connections, and the data being accessed by them. The Company shall ensure to perform a robust security screening and testing of the API between the Company and third party before going live;

(vii). Deploy real-time monitoring and alerting capabilities to ensure visibility of the usage and performance of APIs and detect suspicious activities. In the event of a breach, measures shall be in place to promptly revoke API keys or access tokens;

(viii). Take steps to handle high volumes of API call requests by legitimate applications, and implement measures to mitigate denial-of-service attacks while ensuring that

these measures are commensurate with the criticality and availability requirements of the app.

O. Customer Awareness

(i). The app shall have a visible section/tab/module containing necessary legal, regulatory and compliance related information with required disclaimers and acknowledgment of facts (such as relating to the extent of collection, storage, and disposal of data), rights, responsibilities and liabilities of both the users and the Company;

(ii). The Company shall ensure to educate and inform users clearly about how to access, download, securely use and cease to use the App within the App interface as well as through official application release channels in order to mitigate the risk of running malware-infected App;

(iii). The Company shall ensure that a robust remedial process of customer support and complaint resolution is defined and implemented to address any security incidence albeit targeted, sectoral or global related to App user(s) or their back-end infrastructure;

(iv). The Company shall ensure that App are hosted only at the relevant app platform and shall not be hosted for downloading at app owner's website or the vendor website or any other third-party website;

(v). The Company shall undertake active awareness campaigns to educate customer and internal staff about malicious messages, phishing attacks, and spoofing;

(vi). All of the above information should be in a structured, clear and understandable form at least both in English and Urdu languages.

Schedule XXIV-A

(Format of Gender Disaggregated Data)

[See Regulation 67AM(1)(c)(vi)]

Name of AMC/Digital AMC:

License Type:

Name of App:

Reporting Month

During the Month

No. of users registered/onboarded		No. of Investment Transactions Executed		Total Amount Invested		Total Amount Redeemed		Net Amount of Investment	
Male	Female	Male	Female	Male	Female	Male	Female	Male	Female

Total as of till date:

No. of users registered/onboarded		No. of Investment Transactions Executed		Total Amount Invested		Total Amount Redeemed		Net Amount of Investment	
Male	Female	Male	Female	Male	Female	Male	Female	Male	Female

Description	As end of Month,
Assets under Management	
Active UIN	
Avg Amount of Investment per UIN	

No. of downloads	Registered Users	No. of Verified UIN	% of user retention

Schedule XXIV-B

Code of Conduct for Call Centers by the Digital Asset Management Company (Company)

[See Regulation 67AM(2)(b)(i)]

(i). The Company shall have a comprehensive policy and Standard Operating Procedures (SOP) on call center management duly approved by their Board of Directors;

(ii). Display, at conspicuous position on Company's websites/digital Apps/digital channel, the approved Policy and SOPs, as required under Clause (i) of this Code.

(iii). Ensure that call center numbers are displayed prominently on Company's websites/digital Apps/digital channel. Moreover, the companies are encouraged to deploy toll-free numbers for their call centers;

(iv). Customers/user/unitholder/investors must be given the choice to select their preferred language between Urdu or English;

(v). Agents must not refuse to lodge complaint of the customer/user/unitholder/investor;

(vi). Complaints received through the call center are properly recorded in the Complaint Management System (CMS), preferably through appropriate automation;

(vii). The Company must ensure the confidentiality of customer's data shared with the call center agents through appropriate oversight and security clauses in employment contract;

(viii). The company must ensure to implement direct dialing call center solutions, wherein the customer/user/unitholder/investors are contacted without exposure of their number or confidential data to the contacting staff;

(ix). Ensure periodic trainings of their call center staff on product features, approved SOPs and regulatory frameworks to avoid mis-selling and breach of regulatory requirements;

(x). The Company shall mandate periodic reporting on performance of call centers including Complaint Management turnaround time (TAT);

(xi). The Company shall ensure that supervision function like quality assurance checks of call center should not be outsourced;

(xii). Conduct consumer testing/ consumer recalls at least on an annual basis to assess customer awareness regarding call centers and take actions for improvement where required;

(xiii). Call center agent/staff must treat all customers with respect, courtesy, and professionalism at all times;

(xiv). Offensive/threatening language, discriminatory remarks, or disrespectful behavior towards customers is strictly prohibited;

(xv). Agents maintain a level of professionalism throughout the entire conversation. All conversations should be in line with corporate values and goals;

(xvi). An objective professional tone should be used with customer to hear/register their complaint and a tentative TAT shall be shared with them for complaint resolution;

(xvii). Agents must avoid mis-selling, maligning other competitive market products and exaggerating facts to their benefit;

(xviii). Agents must ensure that customer/user/unitholder/investor are explicitly informed about their calls being recorded at the call center; and

(xix). Upon resolution of complaint within committed TAT customer should be intimated as such, in case the complaint remains unresolved, a call/email should be made to customer, depending upon the mode through which complaint was initially lodged, to update on the progress made and a revised TAT shall be shared with customer."

No. SCD/NBFC/NBFCR/2025-

(Bilal Rasul)
Secretary to the Commission