SECP

SECURITIES AND EXCHANGE COMMISSION OF PAKISTAN
SPECIALIZED COMPANIES DIVISION
FUND MANAGEMENT DEPARTMENT

No. SCD/PRDD/CIRCULAR/44 /2025 **August 01, 2025**

Circular No. 22 of 2025

Subject: **Pre-Qualification, Compliance and Reporting Requirements for Digital Platforms by Digital Asset Management Companies**

The Securities and Exchange Commission of Pakistan (the "Commission") in exercise of its powers conferred under Section 282B(3) of the Companies Ordinance, 1984 (XLVII of 1984) read with provisions of Regulation 67AL(a)(ii) of the Non-Banking Finance Companies and Notified Entities Regulations, 2008 (the "NBFC Regulations") hereby specifies the following pre-qualification requirements for Digital Asset Management Company (Digital AMC) for seeking NOC from respective trustees.

1. **Scope and Applicability**
These requirements are applicable to Digital AMCs as well as the AMCs which are utilizing Digital Platforms for provision of services to their investors/unitholders.

2. **Prerequisites for Obtaining NOC for Digital Platforms**

The Digital AMC shall adhere to the following requirements for provision of Digital Asset Management Services through digital platforms:

2.1. The Digital AMCs are encouraged to comply with the below listed standard guidelines as may be amended/improved/replaced from time to time:
   a. Open Web Application Security Project (OWASP) Mobile Application Security Verification Standard;
   b. OWASP Mobile Application Security Testing Guide; and
   c. OWASP Web Application Security Testing.

2.2. 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:
   a. 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.

b. 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.

c. 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.

d. 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).

e. 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.

f. 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.

g. 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.

h. 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.

i. 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 system log files are protected against unauthorized modification through appropriate technical controls. Logs must be stored in a secure manner to ensure tamper-evidence. Administrative access to logs must be monitored, and any changes or access attempts shall be recorded and auditable;
- 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.

2.3. The Digital AMC shall avail cybercrime insurance policy to indemnify losses that may arise due to cyber-attack/cybercrime on their digital platforms.

2.4. The Digital AMCs shall ensure compliance with the additional requirements relating to the Smartphone Application, as provided in Annexure – A to this Circular.

2.5. In case of a smart phone application, the Digital AMC at the time of launching of 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.

2.6. 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:

a. Disclosure of information with the specific written or recorded consent of investor/unitholder/user.
b. Release, submission or exchange of information with other financial institutions/licensed entities for transaction processing including Centralized KYC/AML/CFT screening activities.
c. Disclosure of information upon orders of a court of competent jurisdiction or any government office or agency authorized by law.
d. 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
e. Disclosure to third parties such as insurance companies, solely for the purpose of insuring the investor/unitholder/user from fraud or unauthorized charges.

3. Compliance Reporting and Grievance Redressal Mechanism/Guidelines

3.1. 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:
   - Total number of unitholders in each class (corporate and retail);
   - Total number of units held by each class of unitholders;
   - Aggregate value of assets held by each class of unitholders;
   - Any significant transactions or changes in the CIS's composition affecting each class of unitholders;
   - Any material information or disclosures relevant to the interests of corporate and retail unitholders; and
   - Gender Disaggregated Data as per Annexure – B.

d. share a monthly list of distributors appointed for distribution of CIS on Digital Platform along with following details:
   - Total Monthly CIS Sales through the distributors (digital distributor and other than digital distributor AUM); and
   - Percentage of CIS Sales through Digital Distributor and other than digital distributor on cumulative basis.

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

f. 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:

- 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., WhatAapp messaging, call or any other). Code of Conduct for Call Centers is enclosed as Annexure C.
- 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
- Lodge Online Complaint – Investor shall also be able to lodge his/ her complaint through a complaint form available at the digital platforms.

g. 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;
h. specify maximum timelines for acknowledgement and resolution of complaints; and
i. report to the Commission on a monthly basis, the following information:
   - No. of complaints outstanding from previous month;
   - Total no. of complaints during current month;
   - Nature of repetitive complaints;
   - No. of complaints resolved;
   - No. of complaints outstanding;
   - Satisfaction ratio;
   - Average time taken for disposal of a complaint; and
   - Monthly trend analysis of complaints received and disposed.

3.2. The Digital AMC shall adhere to all the standard requirements applicable to an AMC, unless expressly modified or relaxed by the above-stipulated requirements.

Zeeshan Rehman Khattak
Commissioner (SCD)

Distribution:

1. Chief Executive Officers, Asset Management Companies;
2. Mutual Funds Association of Pakistan; and
3. Trustees of Collective Investment Schemes.

Annexure - A

Requirements for Mobile Apps by the Digital Asset Management Companies

[See Clause 2.4]

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 180 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 the 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. This requirement shall not apply to user-initiated downloads or reports (e.g., transaction history) saved locally on the device by the user.
(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 restrict navigation from the App to external applications, websites or untrusted content, unless explicitly required for a business function and in accordance with the Company's approved security architecture principles.

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; and

(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; and
(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; and

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

SECP

SECURITIES AND EXCHANGE COMMISSION OF PAKISTAN
SPECIALIZED COMPANIES DIVISION
FUND MANAGEMENT DEPARTMENT

Annexure – B

(Format of Gender Disaggregated Data)

[See Clause 3.1(c)]

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

Annexure – C

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

[See Clause (3.1)(f)]

(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.