SAHAMATI MEMBERSHIP POLICIES

Version History

Version	Date	Description
1.0	April 03, 2025	Published on roll out of Sahamati membership

General

These membership policies ("**Sahamati Membership Policies**") are designed to build trust amongst Members and to provide a common set of rules, values and principles that all Members agree to adhere to. Members undertake to comply with and uphold these Sahamati Membership Policies (and any bye laws framed in accordance with these Sahamati Membership Policies).

Obligations and Responsibilities of Sahamati Members

1. All Members shall, at all times:

A. comply with Applicable Laws in relation to their membership;

B. not engage in any activity or conduct in relation to their membership that is illegal or unlawful;

C. at the time of becoming a Member, undertake certification and continue to remain duly certified in accordance with the Sahamati Certification Guidelines;

D. implement all security measures mandated or recommended by ReBIT or the RBI from time to time;

E. ensure that no Data is shared with any third party other than as permitted by Applicable Law;

F. ensure that their systems and infrastructure are compliant with the Application Programming Interface (API) change management policies issued by ReBIT from time to time;

G. ensure that their systems and infrastructure remain operational with minimal disruptions;

H. ensure on a best-efforts basis that their systems are capable of enabling interoperability with every AA as per the technical protocols published by ReBIT and as permitted by Applicable Laws. The AA shall co-operate and hold discussions, on a best-efforts basis for interoperability;

I. adhere to all service levels and standards prescribed by Sahamati from time to time;

J. to provide prior notice of at least 2 (Two) Business Days to Members and Sahamati, in case of any scheduled downtime;

K. remediate any unscheduled shutdowns and other disruptions which relate to the relevant Member's operations in the AA ecosystem and notify Sahamati of such shutdown or disruption, the cause thereof and the remediation steps taken;

L. retain all Consent logs and Data flow logs for such period(s) as may be required under Applicable Law, in a readily accessible and searchable format that allows for easy retrieval;

M. co-operate with Sahamati by providing evidence of Consent logs or transaction logs as reasonably required by Sahamati to redress any grievance or dispute raised against a Member;

N. ensure that an audit is conducted by a Qualified Security Assessor ("**QSA**") approved by the regulatory body governing the business of the Member at such frequency/intervals as may be required by Applicable Laws; provided that in case the regulatory body governing the business of the Member does not specify any requirement for minimum qualification or certification or eligibility of the auditor for conducting the audit, the Member shall not be obligated to appoint a QSA;

O. to the extent permitted under Applicable Laws and as per the process prescribed by the Governing Council, allow Sahamati to seek necessary information and documents from Member(s) to review their adherence with Sahamati Membership Core Documents and the Sahamati Membership Bye-Laws. Such review(s) may be conducted through third parties approved by the Governing Council. The expenses for such review(s), as stipulated by the Governing Council, shall be borne by the relevant Member;

P. appoint grievance redressal officers whose responsibility shall be to resolve Customer Grievances and to collate all the Data transfer and Consent logs or other information as may be necessary or desirable;

Q. duly discharge payment obligations arising on account of their membership with Sahamati, (including the payment of Membership Fee or other fees as applicable and notified in the Sahamati Member Fee Policy from time to time);

R. provide their consent to AAs to share and use, in accordance with Applicable Law, entity-wise aggregated meta data (relating to technical health, adoption and use other than Personal Data) listed in the Compendium of Data Shared by AA Members for Sahamati's telemetry and other common services, as available in the records of the AA;

S. immediately inform Sahamati of any change in the status of its operating licence including but not limited to any cancellation, revocation or suspension thereof;

T. ensure implementation of strong information security processes and requirements and obtaining cyber security certifications as required under Applicable Law such as ISO, SOC 2, etc.;

U. impose measures to secure Data against hackers, viruses, unauthorised access etc.; and

V. observe best practices, codes of conduct, technical guardrails and other standards and guidelines prescribed by the committees/panels constituted by the Governing Council from time to time.

2. The Members understand, agree and acknowledge that Data is on an "as is" and "as available" basis only. Sahamati and the Members disclaim any warranty or assurance as to the completeness or accuracy of any Data transferred and any reliance that may be placed on such Data.

3. All AAs shall:

A. comply with the various duties and responsibilities of an AA as set out in the AA Master Directions;

B. create one or more AA Client Interfaces in accordance with the following:

1. The AA Client Interface should support the following features:

a. consent management including but not limited to account discovery, account linkage and activity logs;
b. profile management, including registration of Customers resulting in the issuance of Virtual User Addresses ("**VUA**"); and
c. complaint management including the ability to raise a complaint and receive updates as to the progress of the complaint till the final resolution thereof.

2. AAs shall ensure that the AA Client Interface is designed to use authentication measures as prescribed in the AA Technical Standards, from time to time, for all actions or Transactions between the Customer and the AA, including but not limited to all consent management actions and all profile management actions;

3. The AA Client Interface/s should offer the Customer the ability to check the status of a Data request and to view the entire history of their Consents and Data flows at any point in time;

C. support Consent Requests which are initiated by the Customer or by the FIU(s);

D. ensure that appropriate measures have been implemented to ensure proper Customer identification and authentication and ensure that the Consent obtained is in accordance with the AA Technical Standards;

E. ensure that no Data received from an FIP is accessed or retained by the AA for longer than is necessary for such Data to be transferred to the Customer or FIU or 1 (One) hour from time of receipt or such other configurable timeline as decided by the AA, whichever is earlier;

F. not decrypt or otherwise view, access, share or store any of the underlying contents of the Data at any point;

G. educate Customers on informed consent, significance and possible results of consenting, and the possible implications of consenting without properly evaluating the consequences or results thereof;

H. share with Sahamati, to the extent available with them, aggregated data relating to technical health, adoption and use as per the AA Master Directions in such reporting period, within the timeline and in the mode and manner prescribed by Sahamati from time to time. The list of such indicative data points shall be as provided in the Compendium of Data Shared by AA Members for Sahamati's Telemetry and Other Common Services as issued by Sahamati. The AAs shall be responsible for ensuring the accuracy of such data and taking necessary consents under the Applicable Laws;

Provided that Sahamati (i) will require only such data which does not violate any regulatory provisions or laws or other agreements that are within the framework of applicable regulations and laws, and (ii) shall not share any entity-wise business information with any third party unless prior written consent is obtained from the relevant AA for sharing such data;

I. put in place and keep current a disaster recovery or a business continuity management plan for all their operations; and

J. take appropriate action to prevent harm to any entity participating in the consented exchange of Data pursuant to the framework of the AA Master Directions, including but not limited to, disabling or suspending a Customer's AA account in order to prevent unauthorised access to the Customer's AA account.

4. AAs shall not be held responsible for any loss or damage that may arise due to a Customer's account being disabled or suspended for any reason or due to unauthorised use of such account (other than on account of failure of the AA to comply with these Sahamati Membership Policies or Applicable Laws).

5. AAs shall onboard Customers through a process that comprises the following steps:

a. The Customer provides their mobile number, email address, or any other identifier that has been declared to be suitable for digital verification in the AA Technical Standards, from time to time, to the AA.
b. The AA shall verify that the identifier provided is valid and verified.
c. Upon conclusion of such verification, the AA will issue to the Customer a virtual address that uniquely identifies the Customer in the following format:

<customer_identifier>@<AA_identifier>

Where:

(i) <customer_identifier> is a word/alphanumeric that uniquely identifies the Customer in the AA system and which may either be selected by the Customer or issued by the AA. The AA shall, at its discretion, be free to suggest a unique default identifier (such as mobile number or last name).

(ii) <AA_identifier> is the unique identifier that has been provided to the AA by Sahamati at the time of on-boarding that uniquely identifies the AA among all AAs in the ecosystem.

(iii) The entire Virtual User Address, also known as the VUA or the AA Handle, should only contain “a-z, A- Z, 0-9,.(dot), - (hyphen), @", as currently defined in the AA Technical Standards and subject to any modifications in such standards, from time to time.

d. At the time of onboarding and thereafter whenever initiated by the Customer, the AA Client Interface will facilitate discovery of the Customer’s accounts held with one or more FIPs in the following manner:

(i) The AA Client Interface will offer Customers the opportunity to provide strong identifier(s) that the Customer’s FIP will recognise. The AA will relay such identifier/s to the FIP. The FIP shall, if such identifier/s correspond with the Customer’s record within its system, provide to the AA, a set of account numbers matching the Customer identifier so provided.

(ii) The AA Client Interface shall display the account numbers so discovered from all FIPs in a masked format and in a manner that will allow the Customer to make a selection of the accounts which the Customer wishes to link.

(iii) By selecting the accounts that the Customer wishes to link on the AA Client Interface, the Customer authorises the AA to relay the Customer’s Consent to the FIP for linking such accounts to the Customer’s profile with the AA.

(iv) The FIP shall, after independently authenticating the Customer as specified in the AA Technical Standards, complete the linking request.

6. All FIUs shall:

A. ensure on a best efforts basis that their systems are capable of enabling interoperability with every AA as per the technical protocols published by ReBIT and as permitted by Applicable Laws. The FIUs shall co-operate and hold discussions on a best-efforts basis for achieving interoperability;

B. set up and continue to operate their systems so that the FIU also functions as an FIP, on the principle of reciprocity, when holding the types of Data notified by RBI as eligible for transfer through an AA pursuant to the AA Master Directions;

C. ensure that any Data received from an FIP through an AA is only used for the express purpose for which the Consent is obtained, as per the Consent Artefact;

D. not transfer, share or otherwise disclose any Data collected from an FIP to any third party whatsoever except with prior Consent of the concerned party or as permitted under Applicable Laws. Provided that, an FIU may share data in an aggregated and anonymised form with contracted third parties and with due notice to the Customer that it is sharing such data, to the extent permissible under Applicable Law;

E. permit AAs to use their name and/or logo in the AA Client Interface for the Customers' ease and convenience to understand the entity seeking Consent for Data sharing as per the AA Master Directions. Provided that any use of a Member's name and/or logo shall be subject to obtaining prior written consent from the concerned entity in respect of such usage. Provided further that such use shall be in accordance with the relevant branding guidelines of the entity whose name and/or logo is being used by a Member;

F. only retain any Data received from an FIP for as long as is necessary for the FIU to fulfil the purpose for which such Data was obtained or as required in order to comply with Applicable Laws; and

G. immediately notify the relevant AA about any Consent revocation initiated by a Customer through such FIU and desist from further fetching of any Data on the basis of the Consent so revoked by the Customer. The FIU shall purge and delete the Data once the Customer revokes the Consent except if required to retain such Data to comply with Applicable Laws.

7. All FIPs shall:

A. ensure on a best efforts basis that their systems are capable of enabling interoperability with every AA as per the technical protocols published by ReBIT and as permitted by Applicable Laws. The FIPs shall co-operate and hold discussions, on a best-efforts basis for achieving interoperability;

B. ensure that they reasonably cooperate with AAs and Sahamati to ensure compliance with the AA Master Directions;

C. refrain from providing any preferential or detrimental treatment amongst AAs in respect of response times, quality of Data provided etc.;

D. permit AAs to use their name and/or logo in the AA Client Interface for the Customers' ease and convenience, permit all AAs to discover the Accounts that the Customer has

with them, and permit the linking of these Accounts using standard protocols specified by ReBIT from time to time. Provided that any use of a Member's name and/or logo shall be subject to obtaining prior written consent from the concerned entity in respect of such usage. Provided further that such use shall be in accordance with the relevant branding guidelines of the entity whose name and/or logo is being used by a Member;

E. on receipt of a Consent Request from an AA, verify the validity of the Consent and other parameters prescribed under the AA Master Directions (including with respect to the dates and usage as specified by the Customer) before proceeding to collate and furnish any Data in response to such Consent Request;

F. once a Consent Request and Consent have been validated, collect all relevant Data under its possession and control in relation to such Data request, create a copy thereof and store it in an encrypted format, inform the AA that it is ready for collection and facilitate its collection by the AA for delivery to the FIU and/or the Customer, as the case may be;

G. ensure that its systems implement any revocation of Consent by a Customer that has been communicated to such FIP by an AA;

H. set up and continue to operate their systems so that they also function as an FIU on the principle of reciprocity;

I. have the power to reject any such request for Data received from an AA if it fails to meet the criteria for obtaining Consent of the Customer, as specified under Applicable Law;

J. ensure that the Data being transmitted through the AAs is complete in terms of the records available with the FIP;

K. take all requisite measures to ensure that there are no bugs/errors in its API gateway and to ensure smooth transmission of Data to the AAs; and

L. not disable access to any onboarded AA without providing a reasonable opportunity of being heard to such AA with respect to any alleged breach(es) of Applicable Law and/or to remediate any breach(es). If the identified deviation is remediated by the AA within such timeline as mutually agreed between such AA and the FIP, the FIP shall refrain from disabling access to such AA.

Provided that disablement of access to an AA may only be considered if there is a good faith concern in relation to any misuse of any Data or Consent requests by such AA in breach of Applicable Law.

Provided further that in an instance of any FIP disabling access to an AA, such FIP shall promptly notify Sahamati to enable Sahamati to notify all other Members of such action(s).

Provided further that upon being notified that the concerned AA has remediated any identified breach(es), the FIP shall promptly re-enable access to such AA, subject to any orders of a relevant regulatory authority or a Competent Authority, if any, in relation to the breach of Applicable Laws by the concerned AA.

8. Anti-Bribery & Anti-Corruption

Sahamati has a zero-tolerance policy with respect to any form of bribery or corruption. Members should not engage in any form of bribery or corruption, whether directly or indirectly through a third party. Without limitation to the situations described herein below, Members:

A. are prohibited from directly or indirectly offering/promising/authorising bribes, commissions, or other similar improper payments or anything of value to anyone in any form that qualifies as a bribe to any person, including government officials, private persons, FIP(s), FIU(s), AA(s), or their representatives, for the purpose of wrongfully obtaining an advantage while participating in the AA framework;

B. shall not influence or attempt to influence Sahamati's onboarding process through any kind of gift, payment, or remuneration to Sahamati employees, vendors, contractors, or their relatives or friends; and

C. are required to implement monitoring and enforcement procedures to ensure compliance with applicable anti-corruption laws.

9. Miscellaneous

A. Amendment: Sahamati reserves the right to change, modify, amend, or update the Sahamati Membership Policies from time to time as per the Process for Consultation for Proposed Amendments to Sahamati Membership Documents. The Member's continued membership with Sahamati after the proposed change, modification, update or amendments have been made effective as per the Process for Consultation for Proposed Amendments to the Sahamati Membership Documents, shall be deemed to signify their acceptance of the such changed, modified, updated or amended Sahamati Membership Policies; provided however that, any such change, modification, update or amendment shall not be applicable to the Members who have terminated their membership prior to the effective date of such change, modification, amendment or update.

B. Capitalised Terms: Capitalised terms used but not otherwise defined herein shall have the same meaning as ascribed to them in the Sahamati Membership Terms.