SOP – Dissemination and Sharing of Updated Client Information (Clause 15(f)), SEBI KRA Regulations, 2011

TABL OF CONTENTS

Executive Summary

Dissemination of Updated Client Information – Clause 15(f), SEBI KRA Regulations, 2011

As per Clause 15(f) of SEBI KRA Regulations, 2011, the KRA ensures that any update to client KYC information is disseminated to all intermediaries availing KRA services for that client in a timely, secure, and standardized manner.

All client updates are received only from authenticated SEBI-registered intermediaries through secured portals, APIs, or bulk upload mechanisms. Each update undergoes system validations, document completeness checks, PAN/OVD verification, and risk-based controls. A mandatory maker–checker framework is followed before any change is committed to the KRA master database.

Once approved, the updated information is stored in the centralized KRA repository with full versioning and audit trail. The system automatically identifies all intermediaries mapped to or having previously accessed the client record. Dissemination is performed on a T+0 / near real-time basis through secured APIs, portal access, and bulk/delta download facilities. Intermediaries receive update indicators/alerts prompting them to refresh their local records.

Strict access controls, IP whitelisting, role-based permissions, and encrypted communication channels are enforced to safeguard data confidentiality. Complete logs are maintained capturing old and new values, submitting intermediary, maker–checker details, timestamps, and recipient intermediaries.

Exception monitoring, system alerts, and re-push mechanisms ensure reliability of dissemination. Periodic internal audits and sample testing are conducted to confirm effectiveness. This framework ensures continuous compliance with Clause 15(f) and related SEBI KYC/KRA guidelines.

SOP – Dissemination of Updated Client Information to Intermediaries
(In accordance with Clause 15(f) of SEBI KRA Regulations, 2011)

1. Objective

To ensure that any update in client KYC information captured by the KRA is promptly, securely, and uniformly disseminated to all SEBI-registered intermediaries who have accessed or rely upon that client's KYC record, in compliance with Clause 15(f) of SEBI KRA Regulations, 2011.

2. Scope

This SOP applies to all client KYC updates including, but not limited to:

- Personal details (name, address, contact information)
- Identity and address proofs
- PAN / Officially Valid Documents (OVDs)
- Bank details
- FATCA/CRS information
- IPV / Aadhaar XML / DigiLocker updates
- Status changes (Active / Inactive / On Hold, etc.)

The SOP covers updates originating from intermediaries as well as internally triggered corrections validated by KRA.

3. Source of Client Updates

Client information updates are received by KRA through:

1. SEBI-registered intermediaries via KRA system/API/portal.
2. Bulk upload mechanisms provided to intermediaries.
3. Client-initiated modifications routed through registered intermediaries.
4. KRA internal rectifications based on regulatory directives or validation outcomes.

All updates must originate only from authenticated intermediaries.

4. Validation and Approval Process

4.1 Initial System Validation

Upon receipt of update request:

- Mandatory field checks are performed.
- Format validations (PAN, DOB, email, mobile, etc.).
- Document completeness verification.
- De-duplication checks against existing KYC records.

Records failing validation are rejected and returned to the originating intermediary with error codes.

4.2 Independent Verification

- Uploaded documents are verified against OVD standards.
- PAN is validated through authorized system integration.
- IPV / Aadhaar XML / DigiLocker authenticity is checked wherever applicable.
- Risk-based checks are applied for sensitive fields (identity/address/bank).

4.3 Maker–Checker Authorization

- Every approved update follows a maker–checker mechanism.
- Maker performs initial processing.
- Checker independently reviews and authorizes before the update is committed to the master KYC database.

Only after checker approval does the update become effective.

5. Update Posting in KRA Master Database

Once approved:

- The updated information is written to the centralized KRA master repository.
- Versioning of KYC records is maintained.
- Previous values are archived for audit trail.
- Date/time stamp, intermediary code, and user ID are captured.

6. Identification of Relevant Intermediaries

System automatically identifies:

- All intermediaries who have previously accessed/downloaded the client's KYC.
- All intermediaries currently mapped to the client.

This mapping is maintained through unique KYC identifiers (PAN / CKYC / KRA ID).

7. Dissemination Mechanism (Clause 15(f))

Dissemination is carried out through the following automated modes:

7.1 API / System Push

- Updated KYC data is made available in real time through secured APIs.
- Intermediaries integrated via API receive update flags/status on subsequent pulls.

7.2 Portal Access

- Updated records are immediately visible on the KRA portal for all mapped intermediaries.
- Change indicators highlight modified fields.

7.3 Bulk Download Facility

- Intermediaries may download updated KYC data through bulk files provided by KRA.
- Delta files (only changed records) are generated where applicable.

7.4 Update Notifications

- System-generated alerts/flags are enabled for intermediaries indicating that client KYC has been updated.
- Intermediaries are required to refresh their local records based on these alerts.

Dissemination is completed on T+0 / near real-time basis post approval.

8. Security and Access Controls

- Dissemination occurs only over encrypted channels (HTTPS/SFTP/API).
- Access restricted to whitelisted IPs and authenticated credentials.
- Intermediaries can view/download only those clients mapped to them.
- Role-based access is enforced.

9. Audit Trail and Logging

KRA maintains complete logs including:

- Nature of change
- Old and new values
- Intermediary submitting update
- Maker and checker IDs
- Date and time of dissemination
- List of recipient intermediaries

Logs are retained as per regulatory record retention policy and are available for inspection.

10. Exception Handling

- Failed dissemination events (if any) are captured by system alerts.
- Technology team investigates and re-pushes updates.
- Incident records are maintained.
- Root cause analysis is performed for repeated failures.

11. Periodic Review and Compliance Monitoring

- Internal audits verify dissemination effectiveness.
- Sample testing is performed to confirm receipt by intermediaries.
- SOP and system controls are reviewed periodically or upon regulatory change.

12. Regulatory Compliance

This SOP ensures compliance with:

- SEBI KRA Regulations, 2011 (Clause 15(f))
- SEBI Circulars on KYC/KRA operations
- Information Security and Data Privacy requirements.