STANDARD OPERATING PROCEDURE (SOP)

Handling of Same Mobile Number and/or Email Address Captured in Multiple Demat Accounts

1. **Purpose**

   This Standard Operating Procedure (SOP) has been framed to establish a uniform process for identifying, verifying, approving, and maintaining records where the same mobile number and/or email address is captured in multiple demat accounts maintained with the Depository Participant (DP).

2. **Regulatory Reference**

   This SOP is framed in accordance with the following NSDL Circulars:

   - NSDL/POLICY/2024/0115 dated 21 August 2024
   - NSDL/POLICY/2015/0040 dated 13 April 2015
   - NSDL/POLICY/2015/0068 dated 06 August 2015
   - NSDL/POLICY/2015/0074 dated 21 August 2015

3. **Scope**

   This SOP shall be applicable to all demat accounts maintained by the DP where:

   - The same mobile number is registered in more than one account;
   - The same email address is registered in more than one account; or
   - Both mobile number and email address are common across multiple accounts.

4. **Policy**
   - Every demat account should normally have a unique mobile number and email address.
   - Common mobile number/email address shall be permitted only in cases of:
     - Self (multiple accounts of the same client)
     - Spouse
     - Dependent Children
     - Dependent Parents

- Such exceptions shall be allowed only after proper verification, written declaration, and approval by the Compliance Department.
- Where common contact details are found for unrelated clients, separate mobile numbers/email addresses shall be obtained immediately and records updated.

5. Standard Operating Procedure

- Step 1 – Identification
  - Generate Duplicate Mobile Number and Duplicate Email ID reports from the NSDL i-Assist Portal or Local DPM.
  - Review all duplicate cases.

- Step 2 – Verification
  - Verify all accounts sharing the same contact details.
  - Confirm the relationship between the account holders.
  - Verify KYC documents and supporting records.

- Step 3 – Documentation Obtain:
  - Written request/declaration from the client.
  - Relationship proof (where applicable).
  - Supporting KYC documents.

- Step 4 – Approval
  - Submit the case to the Branch Manager/Compliance Officer.
  - Update records only after obtaining approval.

- Step 5 – Non-Compliant Cases
  - If clients are unrelated or no declaration is available:
  - Contact the concerned clients.
  - Obtain separate mobile number/email address.
  - Update the DP records immediately.
  - Escalate unresolved cases to the Compliance Officer.

- Step 6 – Record Maintenance

- Maintain all declarations, approvals, KYC documents, verification records, and correspondence for audit and regulatory inspection.
- Verification Format

Sr. No.	Particulars	Details
1	DP ID / Client ID	
2	Client Name	
3	Mobile Number	
4	Email Address	
5	Duplicate Found In	Same Mobile / Same Email / Both
6	Number of Accounts Sharing Details	
7	Other Client IDs Using Same Contact	
8	Relationship Between Clients	Self / Spouse / Dependent Child / Dependent Parent
9	Family Declaration Available	Yes / No
10	Written Request from Client Obtained	Yes / No
11	KYC Verified	Yes / No
12	Reason for Common Mobile/Email	
13	Verification Done By	Name & Employee ID
14	Verification Date	
15	Branch Manager/Compliance Approval	Name & Signature
16	Remarks	

- **Compliance Checklist**

Check	Status (✓/✗)
Duplicate report reviewed	
Relationship verified	
Written declaration obtained	
KYC verified	
Compliance approval obtained	
Records updated (if required)	

Check	Status (✓/✗)
Documents archived	

All records including reports, declarations, approvals, KYC documents, correspondence, and verification sheets shall be preserved as per SEBI/NSDL record retention requirements and shall be made available during inspections and audits.

- **Effective Date**

This SOP shall come into effect immediately upon approval by the Competent Authority and shall remain in force until revised or superseded.