23 Finverse Web Application Standard Operating Procedure (SOP)

Document Title: Web Application Standard Operating Procedure (SOP)
Document Owner: Operations & Compliance Department
Version: 1.0
Effective Date: [Insert Date]
Review Frequency: Annual or as required
Classification: Internal Confidential

---

1. Purpose

This Standard Operating Procedure (SOP) defines the end-to-end operational workflow for the **23 Finverse Web Application**, ensuring consistent, secure, compliant, and efficient onboarding, verification, approval, activation, servicing, renewal, suspension, and termination of customers and partners.

The SOP applies to all internal departments including Operations, Compliance, Finance, Customer Support, Technology, Sales, Risk, and Administration.

---

2. Scope

This SOP covers:

- Customer onboarding
- Partner onboarding
- Registration
- OTP verification
- PAN verification
- GST verification
- Bank verification
- Agreement execution
- eSign
- Payment processing
- KYC verification
- Backend approvals
- Account activation
- Suspension

- Renewal
- Termination
- Refund processing
- Complaint handling
- Audit logging
- Version control
- Administrative access management

---

3. Roles & Responsibilities

Customer

- Complete registration
- Submit required documents
- Complete payment
- Execute agreements
- Complete KYC
- Maintain accurate information

Partner (CP/DP)

- Complete onboarding
- Verify customer information
- Follow compliance requirements
- Support customer onboarding
- Maintain ethical conduct

Operations Team

- Verify applications
- Process approvals
- Coordinate onboarding
- Resolve operational issues

Compliance Team

- KYC verification
- AML review
- Risk assessment
- Regulatory compliance
- Fraud investigation

Finance Team

- Verify payments
- Process refunds
- Manage subscriptions
- Commission settlement

Technology Team

- Platform availability
- Security monitoring
- Audit logs
- User access management

Administrator

- User administration
- Backend approvals
- Role management
- System configuration

---

4. Customer Journey

Step 1 – Registration

Customer accesses the 23 Finverse Platform.

The customer shall provide:

- Full Name
- Mobile Number
- Email Address
- Password
- Referral Code (if applicable)

System validates mandatory fields.

Step 2 – OTP Verification

System sends OTP to:

- Registered Mobile Number

- Email Address (where applicable)

Customer enters OTP.

System validates:

- OTP correctness
- Validity period
- Maximum retry limit

Upon successful verification, registration proceeds.

Step 3 – Profile Completion

Customer completes profile including:

- Address
- Date of Birth
- Occupation
- PAN
- GST (if applicable)
- Bank Details

Incomplete applications remain in Draft status.

Step 4 – PAN Verification

System validates:

- PAN format
- Duplicate PAN
- Existing account mapping
- Verification status

Failed verification triggers manual review where required.

Step 5 – GST Verification (Business Users)

Applicable only where GST registration is required.

System validates:

- GSTIN format
- Business details
- Registration status

GST information is stored securely.

Step 6 – Bank Account Verification

Customer submits:

- Account Holder Name
- Account Number
- IFSC Code

Verification may include:

- Penny-drop verification
- Banking API validation
- Manual verification

Only verified bank accounts become eligible for payouts or refunds.

Step 7 – Agreement Acceptance

Customer reviews:

- Terms of Use
- Privacy Policy
- Subscription Policy
- Payout Policy (where applicable)

Acceptance is recorded with:

- Timestamp
- IP Address
- Device Information
- User ID

Step 8 – Electronic Signature (eSign)

Where applicable:

Customer completes:

- Aadhaar eSign
- Digital Signature
- OTP eSign

Executed agreements are securely archived.

Step 9 – Subscription Payment

Customer selects subscription.

Payment options:

- UPI
- Debit Card
- Credit Card
- Net Banking
- Wallet
- Other supported payment methods

Payment confirmation is automatically generated.

Invoice is issued.

Step 10 – KYC Verification

Customer uploads:

- Identity Proof
- Address Proof
- PAN
- Photograph
- Other required documents

Compliance Team reviews:

- Identity
- Authenticity
- Risk Indicators

Status:

- Approved
- Pending
- Rejected

Step 11 – Account Activation

Upon successful completion of:

- Registration
- OTP
- PAN
- Payment
- Agreement
- KYC

System activates account.

Customer receives:

- Welcome Email
- Login Confirmation
- Dashboard Access

---

5. Partner Journey

Partner onboarding follows similar workflow with additional steps:

- Business Verification
- GST Validation
- Bank Verification
- Agreement Execution
- Commission Profile Creation
- Hierarchy Mapping
- CP/DP Approval
- Training Completion (where applicable)

Partner becomes Active only after Compliance approval.

---

6. Backend Approval Flow

Workflow:

Registration

↓

OTP Verification

↓

Profile Submission

↓

PAN Verification

↓

GST Verification (if applicable)

↓

Bank Verification

↓

Agreement Acceptance

↓

Payment Confirmation

↓

KYC Review

↓

Compliance Approval

↓

Operations Approval

↓

Finance Validation (where applicable)

↓

System Activation

↓

Customer Notification

Applications may be returned for correction if documentation is incomplete or verification fails.

---

7. Administrative Rights

System Administrators shall have role-based access.

Typical roles include:

Super Administrator

- System configuration
- User management
- Role assignment
- Audit access

Compliance Administrator

- KYC review
- AML review
- Risk decisions

Finance Administrator

- Payment verification
- Refund approval
- Commission approval

Operations Administrator

- Onboarding approval
- Customer management
- Escalations

Customer Support

- Ticket management
- Limited profile updates
- Complaint handling

Access shall follow the principle of least privilege and be reviewed periodically.

---

8. Suspension Process

Accounts may be suspended for:

- Fraud
- KYC failure
- Policy violation
- Payment default
- Regulatory instruction
- Security concerns

Process:

Investigation

↓

Temporary Suspension

↓

Customer Notification

↓

Review

↓

Reinstatement or Termination

---

9. Renewal Flow

Prior to expiry:

System sends reminders.

Customer:

↓

Receives renewal notification

↓

Reviews subscription

↓

Completes payment

↓

Invoice generated

↓

Subscription renewed

↓

Confirmation issued

If payment fails:

↓

Retry

↓

Grace Period (if applicable)

↓

Subscription expiry

↓

Restricted access

---

10. Refund Flow

Customer submits refund request.

↓

Support verifies request.

↓

Finance validates payment.

↓

Operations verifies eligibility.

↓

Approval or rejection.

↓

Refund initiated.

↓

Customer notified.

Refund records retained for audit purposes.

---

11. Complaint Flow

Customer submits complaint.

↓

Ticket generated.

↓

Support reviews.

↓

Department assignment.

↓

Investigation.

↓

Resolution.

↓

Customer informed.

↓

Ticket closure.

Escalations follow the Customer Grievance Policy.

---

12. Termination Process

Accounts may be terminated due to:

- Customer request
- Fraud
- Compliance failure
- Extended inactivity
- Legal requirements
- Serious policy violations

Termination Process:

Verification

↓

Data retention review

↓

Account deactivation

↓

Access revoked

↓

Audit record maintained

↓

Customer notification

↓

Data retained or deleted according to the Data Retention Policy

---

13. Version Control

All changes to Platform workflows, agreements, policies, and system configurations shall be documented.

Version records shall include:

- Version Number
- Change Description
- Author
- Reviewer
- Approval Authority
- Effective Date

Previous versions shall be archived securely.

14. Audit Trail

The Platform shall automatically record significant events, including:

- Registration
- Login attempts
- OTP verification
- PAN verification
- GST verification
- Bank verification
- Agreement acceptance
- eSign completion
- Payment transactions
- KYC actions
- Administrative approvals
- Profile updates
- Suspensions
- Renewals
- Refunds
- Complaint handling
- Account termination

Audit logs shall include:

- User ID
- Date and Time
- IP Address
- Device Information
- Action Performed
- Administrator (where applicable)

Audit logs shall be protected against unauthorized modification.

15. Security Controls

The Platform shall implement appropriate security measures, including:

- Multi-factor authentication for administrators.
- Encryption of sensitive data in transit and at rest.
- Role-based access controls.

- Secure API integrations.
- Session management.
- Password policies.
- Regular vulnerability assessments.
- Security monitoring and incident response.
- Backup and disaster recovery procedures.

---

16. Monitoring and Review

This SOP shall be reviewed at least annually or whenever there are:

- Regulatory changes.
- New product launches.
- Technology upgrades.
- Security enhancements.
- Business process changes.

All amendments shall follow the Company's version control and approval process.

---

17. Approval Authority

This SOP shall be approved by:

- Chief Executive Officer (CEO)
- Chief Operating Officer (COO)
- Head – Compliance
- Head – Technology
- Head – Operations

---

18. Document Control

Version	Effective Date	Description	Approved By
1.0	[Insert Date]	Initial Release	Management