**Regulatory Guidelines for Customer Data Management, Record Retention, and Financial Eligibility**

**Section 1: Customer Data Privacy and Retention**

1.1 **Data Retention Period**

All customer Personally Identifiable Information (PII) must be retained for no longer than **7 years** from the date of account closure, unless required by legal obligations.

1.2 **Data Encryption Standard**

All customer data must be stored using at least **AES-256 encryption** both at rest and in transit.

1.3 **PII Access Control**

Only authorized personnel with **role-based access control (RBAC)** are permitted to access PII. Access logs must be retained for a minimum of **2 years**.

1.4 **Third-Party Disclosure**

No customer data may be shared with external vendors unless a signed **Data Processing Agreement (DPA)** exists and customer consent has been explicitly recorded.

**🔹 Section 2: Financial Eligibility for Credit Products**

2.1 **Minimum Income Threshold**

Applicants for personal loans must have a **verifiable monthly income of at least ₹25,000**, or equivalent foreign currency if residing abroad.

2.2 **Asset Declaration Requirement**

All applicants must disclose **movable and immovable assets**, including real estate, mutual funds, equity, and gold holdings.

2.3 **Debt-to-Income Ratio**

Approved applicants must maintain a **DTI ratio less than 40%** at the time of loan sanctioning.

2.4 **Loan Eligibility Blacklist**

Applicants who have defaulted on any credit obligation in the last **3 years** are **not eligible** for personal or unsecured loans.

**🔹 Section 3: Record-Keeping and Audit Guidelines**

3.1 **Document Archival Policy**

All financial transaction records must be stored for **a minimum of 10 years**, preferably in immutable format (e.g., blockchain or WORM storage).

3.2 **Audit Frequency**

Internal compliance audits must be conducted at least **once every 6 months**. Findings must be submitted to the central compliance system.

3.3 **Tamper Detection**

All logs must support tamper-evident features. Manual override of logs without audit trace is prohibited.

**🔹 Section 4: Customer Consent and Communication**

4.1 **Marketing Opt-In**

Customers must **opt-in explicitly** for all marketing communications. Pre-ticked checkboxes do not qualify as consent.

4.2 **Policy Updates**

Any changes in data usage or retention policy must be communicated to customers **at least 30 days prior** to enforcement.

4.3 **Grievance Redressal SLA**

All customer grievances must be acknowledged within **48 hours** and resolved within **7 working days**.

**🔹 Section 5: Regulatory Reporting and Escalation**

5.1 **Reporting Obligations**

Suspicious financial activities exceeding ₹10,00,000 must be reported to **FIU-IND** within **24 hours** of detection.

5.2 **Escalation Matrix**

Any regulatory breach must follow a **3-level escalation protocol**:  
→ Level 1: Internal Compliance Officer  
→ Level 2: Chief Compliance Officer  
→ Level 3: Independent Regulator (e.g., RBI, SEBI)

5.3 **Whistleblower Protection**

Employees reporting regulatory violations shall be protected under the **Bank’s Whistleblower Policy** and no punitive action may be taken against them.