ABC BANK – MASTER POLICIES DOCUMENT

Version 1.0 | Prepared for Internal & Regulatory Compliance

---

1. INTRODUCTION

1.1 Purpose

This document defines the core policies governing ABC Bank's operations, security, compliance, customer service, risk management, and technology usage. The purpose is to ensure:

- Regulatory compliance (RBI, SEBI, NPCI, PCI-DSS, ISO 27001, GDPR as applicable)
- Confidentiality, integrity, and availability of bank data
- Customer protection and service excellence
- Operational risk reduction
- Standardization across employees, systems, and processes

---

2. GOVERNANCE POLICIES

2.1 Corporate Governance Policy

- Establishes board responsibilities, executive oversight, ethical conduct, and decision-making practices.
- Mandates quarterly review of financial, operational, and risk indicators.
- Ensures transparency, accountability, and stakeholder protection.

2.2 Ethics & Code of Conduct Policy

All employees must adhere to:

- Integrity, honesty, and professional behavior
- Prevention of insider trading
- Strict confidentiality of customer information
- Avoiding conflicts of interest
- Mandatory reporting of unethical behavior (Whistleblower Procedure)

2.3 Whistleblower Protection Policy

- Employees may report fraud, misconduct, or unethical behavior anonymously.
- The bank ensures full confidentiality and prohibits retaliation.

---

3. INFORMATION SECURITY POLICIES (ISO 27001 ALIGNED)

3.1 Information Security Policy

- Protects bank information assets against threats, internal or external.
- Defines roles of CISO, SOC, IT Ops, Risk & Compliance.
- Mandatory for all employees, contractors, and partners.

3.2 Data Protection & Privacy Policy

- Customer data must be collected on lawful purpose only.
- Sensitive personal data must be encrypted at rest & in transit.
- Data access based on least privilege with MFA.
- Data retention based on regulatory guidelines.
- Customers can request data access, updates, or deletion (where applicable).

3.3 Access Control Policy

- Role-based access (RBAC) only.
- Mandatory annual access review.
- Immediate removal of access on employee exit.
- Privileged Access Management (PAM) required for admin accounts.

3.4 Password & Authentication Policy

- Minimum 12 characters, complexity required.
- Password rotation every 90 days.
- MFA mandatory for all banking applications.
- No sharing, writing down, or storing passwords insecurely.

3.5 Network & Infrastructure Security Policy

- Firewalls, IDS/IPS, and network segmentation mandatory.
- Zero Trust Architecture implementation roadmap.
- All internet-facing systems must undergo quarterly penetration testing.

3.6 Cyber Incident Response Policy

- Defines incident identification, escalation matrix, containment, recovery, and RCA.
- All incidents must be reported to the SOC within 15 minutes.
- Major incidents require reporting to regulatory bodies within stipulated timelines.

---

4. IT & OPERATIONS POLICIES

4.1 Change Management Policy

- All changes must be reviewed, tested, approved by CAB before deployment.

- Emergency changes require post-implementation review within 48 hours.
- Detailed documentation required for every change.

4.2 IT Asset Management Policy

- Inventory of all hardware, software, licenses must be maintained.
- Unauthorized devices or software strictly prohibited.
- End-of-life assets must be decommissioned securely.

4.3 Backup & Recovery Policy

- Daily incremental and weekly full backups.
- Backups stored in encrypted offsite/DR location.
- Annual Disaster Recovery (DR) drill mandatory.

4.4 Vendor Management Policy

- Mandatory due diligence, NDA, and risk rating before onboarding vendors.
- Third-party systems must meet security compliance equal to bank standards.
- Annual vendor audit required.

---

5. CUSTOMER SERVICE POLICIES

5.1 Customer Grievance Redressal Policy

- Complaints must be acknowledged within 24 hours.
- Resolution timelines:
    - General issues: 7 days
    - Payment disputes: 3 days
    - Fraud: 48 hours
- Escalation matrix up to Ombudsman.

5.2 Fair Usage & Transparency Policy

- Customers must be informed clearly about product terms, fees, interest, charges.
- No hidden charges allowed.
- Transparent communication in all banking channels.

5.3 Anti-Money Laundering (AML) & KYC Policy

- Mandatory KYC for all customers (Aadhaar, PAN, Address, Photo).
- Suspicious transactions must be reported to FIU-IND.
- Risk-based customer classification (Low, Medium, High Risk).

---

6. RISK MANAGEMENT POLICIES

6.1 Operational Risk Management

- Identification, assessment, tracking of risks (KRI monitoring).
- Incident reporting and loss event database maintenance.

6.2 Business Continuity Policy

- BCP activation during system outages, disasters, or crises.
- Alternate site operations must begin within defined RTO/RPO.
- Quarterly BCP simulation exercises.

6.3 Fraud Risk Management Policy

- Robust fraud detection, prevention, and response mechanisms.
- Real-time monitoring for suspicious activity.
- Employee awareness and anti-fraud training mandatory.

---

7. HR & STAFF POLICIES

7.1 Recruitment & Onboarding Policy

- Background verification mandatory (criminal, employment, education).
- Employees must sign confidentiality and acceptable use agreements.

7.2 Employee Conduct & Discipline Policy

- Defines disciplinary actions for violations of policies, misconduct, fraud, negligence.

7.3 Remote / Hybrid Work Policy

- Secure VPN usage required.
- Work from home devices must meet security standards.
- No unauthorized data transfer allowed.

7.4 Exit Policy

- Exit interview mandatory.
- Access removal within 2 hours of resignation/termination.
- Return of all bank assets.

---

8. COMPLIANCE & AUDIT POLICIES

8.1 Regulatory Compliance Policy

- Adheres to RBI Master Directions, FEMA, IT Act, Payment and Settlement Act, PCI-DSS, ISO 27001.
- Mandatory reporting timelines followed strictly.

8.2 Internal Audit Policy

- Annual audits covering financial, operational, compliance, and IT security areas.
- All departments must cooperate fully with auditors.
- Remediation plans required within 30 days.

8.3 Record Management Policy

- All financial records must be retained for a minimum of 8 years.
- Secure storage and destruction procedures must be followed.

---

9. PHYSICAL SECURITY POLICIES

9.1 Branch & Office Security

- CCTV coverage required for entrances, teller counters, vaults, ATMs.
- Access control via biometric or smart cards.

9.2 Data Center Security

- Restricted zone with authorized entry only.
- 24/7 monitoring, fire suppression systems, and environmental controls.

9.3 Asset Protection

- All physical assets must be tagged and inventoried.
- Secure disposal of electronic devices after data wiping.

---

10. POLICY ENFORCEMENT & VIOLATIONS

- Non-compliance may result in disciplinary action: warnings, suspension, termination.
- Serious breaches may lead to legal prosecution.
- Regular refresher training mandatory for all employees.

---

11. REVIEW & MAINTENANCE

- All policies must be reviewed annually or after major incidents.
- Updates approved by Board of Directors / Senior Management.
- Latest version accessible on the Bank's intranet.