CYBERSECURITY
BEST PRACTICES
FOR CO-OPERATIVE BANKS

Stronger security. Safer banking. Greater trust.

01 IMPLEMENT MULTI-FACTOR AUTHENTICATION
Implement Multi-Factor Authentication for employees, administrators, and critical banking applications.

02 CONDUCT REGULAR SECURITY ASSESSMENTS
Conduct Regular Security Assessments including vulnerability scans, penetration testing, and compliance reviews.

03 MAINTAIN EFFECTIVE PATCH MANAGEMENT
Maintain Effective Patch Management to ensure timely remediation of security vulnerabilities.

04 ADOPT ROLE-BASED ACCESS CONTROL (RBAC)
Adopt Role-Based Access Control (RBAC) to restrict access to sensitive systems and customer information.

05 ENCRYPT SENSITIVE DATA
Encrypt Sensitive Data both at rest and in transit using industry-standard encryption mechanisms.

06 ESTABLISH CONTINUOUS SECURITY MONITORING
Establish Continuous Security Monitoring through log management, intrusion detection, and anomaly monitoring.

07 PROVIDE CYBERSECURITY AWARENESS TRAINING
Provide Cybersecurity Awareness Training for all employees to reduce phishing and social engineering risks.

08 IMPLEMENT SECURE BACKUP & RECOVERY PROCEDURES
Implement Secure Backup and Recovery Procedures and periodically test disaster recovery capabilities.

09 DEVELOP AN INCIDENT RESPONSE FRAMEWORK
Develop an Incident Response Framework to effectively manage and contain cybersecurity incidents.

10 ENSURE REGULATORY COMPLIANCE
Ensure Regulatory Compliance with applicable banking, privacy, and cybersecurity standards.

SECURE TODAY. RESILIENT TOMORROW.
Together, let's build a safer and stronger banking ecosystem.