Work From Home (WFM) Policy

Our bank is committed to supporting flexible work arrangements that balance employee needs with operational requirements and regulatory compliance. This policy outlines the standards and expectations for employees working remotely.

Key Elements:

- Employee Eligibility
  Remote work is available only to employees whose job functions are suitable for telecommuting and have received formal management approval. Employees are required to be physically present in the office for at least **three days per week** to maintain effective collaboration and team cohesion.
- Remote Work Agreements
  All remote work arrangements require a formal, signed Remote Work Agreement (RWA) documenting the terms, including the schedule (full-time, part-time, or episodic), location, and expected working hours. RWAs must be approved by supervisors and retained in employee personnel files.
- IT Security Compliance
  Employees must use bank-issued secure devices and connect via approved VPNs to protect sensitive information. Encryption, multi-factor authentication, and compliance with cybersecurity policies are mandatory. IT regularly monitors access logs and security incidents related to remote connections.
- Performance Monitoring
  Managers will regularly track employee productivity through agreed-upon metrics focused on outcomes and deliverables. This includes digital tools for task management, regular check-ins, and performance reviews to ensure accountability without intrusive surveillance.
- Cybersecurity Training
  All remote employees must complete bank-approved cybersecurity training annually. Training covers data protection, phishing awareness, secure use of devices, and procedures to report security incidents promptly.