INTEGRATED MANAGEMENT SYSTEM POLICY STATEMENT

Coronation Merchant Bank (Coronation MB) is committed to ensuring the continuity of its business in the face of information security breaches and impactful incidents, the quality of its products and services, and enhancing customer satisfaction.

Coronation MB has implemented an Integrated Management System (IMS) that comprises of Information Security Management System (ISMS), Information Technology Service Management (ITSM) and Business Continuity Management System (BCMS) with the international Standard for the respective management systems. To consistently meet and exceed our customers' expectations, Coronation Merchant Bank has set the following business objectives:

- Customer satisfaction
- Operational excellence
- World-class Technology Platforms
- Optimize Security Management

As a forward-looking organization, we are also committed to the effective implementation, maintenance, and continual improvement of the management systems to support the achievement of our business goals.

The Executive leadership is dedicated to the following objectives for the Certified Integrated Management System implemented by the bank:

1. **ISO 22301 – Business Continuity Management System (BCMS)** is implemented for the entire Coronation MB, with special attention paid to activities identified during Business Impact Analysis (BIA) as critical areas.

2. **ISO 27001 – Information Security Management System (ISMS)** covers the management, operation and maintenance of the information assets and information systems and the associated processes that enable the safety of Coronation MB data and customers' financial information.

3. **ISO 20000 – Information Technology Service Management System (ITSMS)** applies to the entire lifecycle of IT services delivered by the Coronation MB IT department to all business units and branches in the bank.

4. All employees of Coronation MB and related parties identified in the IMS are expected to comply with this policy.

5. Coronation MB is committed to aligning its processes, operations, products, and services to the ISO 27001:2022, ISO 22301:2019, ISO 20000:2018 and NDPA requirements to ensure cyber resilience, integrated service management system and protection of its information assets.

6. The IMS is subject to continuous and systematic review with improvements, where necessary

This policy is publicly available to all interested parties and is reviewed periodically to take account of applicable local, statutory, regulatory, and customer requirements and any changes in business activity.

This policy applies to all Bank employees, its contractors, its consultants, and other individuals affiliated with Third Parties who have access to the Bank's information or business interests.

Breach of this policy or any security mechanism may warrant disciplinary actions.