MCB GROUP

INFORMATION, INFORMATION TECHNOLOGY AND INFORMATION SECURITY GOVERNANCE POLICY

CONTENTS

1. INTRODUCTION

The Board of MCB Group Limited oversees information governance within the organisation and ensures that the performance of information and information technology systems leads to business benefits and creates value.

The Board ensures that information assets are managed effectively and the implementation of a framework on information, information technology and information security governance.is carried out by its main banking subsidiary,The Mauritius Commercial Bank Ltd ('Bank').

This policy is posted on the organisation's website.

2. SUMMARY OF THE BANK'S INFORMATION SECURITY AND RELATED POLICIES

The Bank has put in place a set of policies which set forth its approach to information security for the protection of Private and Confidential information. In line with regulatory requirements (Bank of Mauritius Guidelines, Data Protection Act, Payment Card Industry Data Security Standard …), maintaining the confidentiality, integrity and availability of information stored, processed and transmitted is the responsibility of all Bank staff and is part of their contractual obligations.

The policies cover different spheres associated with information security, the information systems, the administration of logical and physical access to information processed and stored as well as the transmission of information.The policies and their related procedures are regularly updated to reflect current requirements and best practices adopted by the Bank.

The Bank also ensures that all the policies are made accessible to all its staff by publishing them on its intranet. It conducts regular training sessions to ensure common understanding of the policies and procedures in place and to enable their effective implementation. On regular basis, the Bank also conducts e-learning to train and assess the knowledge of its staff on the related policies.

There are also appropriate governance arrangements in place whereby the IT function and the function responsible for monitoring adherence to Information Risk and IT security are kept separate.The Bank has also established control functions in the Internal Audit and Compliance. Accordingly, the Internal Audit conducts regular audit to test the effectiveness of the policies. A close follow up of the implementation of remedial actions is undertaken by the "IORCC" (Information Risk, Operational Risk and Compliance Committee) composed of relevant members of Management. Findings and reports are communicated to the Board Audit Committee and to Senior Management.