Southeast Bank Limited
a bank with vision

Information Security Management System Policy

In the widely digitized world, Southeast Bank Ltd. heavily depends on its ability to use Information and Communication Technology, for its banking operations. All its information is exchanged, archived, used, and processed using Information Technology hardware and software.

Any compromise of its information asset, in terms of Confidentiality, Integrity, and Availability (CIA), may cause serious disruption of services and legal non-compliance. Hence, SEBL is committed to ensure cyber security, protect its information asset and manage its IT infrastructure in a safe and secure manner.

For achieving the desired level of protection, SEBL plans and implements its Information Security Management System based on Risk Assessment, Resource Allocations, and Operational Controls. It also maintains a level of emergency preparedness for its Business Continuity and Disaster Recovery, so that, under all circumstances, the operation of SEBL is continued.

Vulnerability Assessment is used as a means of understanding the possible future information security that may challenge the system's robustness.

Complying with the applicable legal requirements is an essential ingredient of its overall Information Security Management System and it is committed to continually improve its Information Security Performance.

SEBL takes into account the views of its stakeholders in strengthening the reliability of its Information Security Management System so that, as a bank, SEBL can excel, fostering growth and prosperity for the country as a whole.

This policy is endorsed by the highest level of Management of SEBL and communicated to all parties relevant to its Information Security.

Endorsed By:

(.....)

Managing Director

Southeast Bank Limited