Southeast Bank PLC.
a bank with vision

Information Security Management System Policy

In today's widely digitized world, Southeast Bank PLC. relies extensively on Information and Communication Technology to carry out its banking operations. All its information is communicated, stored, utilized, and processed through IT hardware and software systems.

This policy will commit to fulfilling all relevant requirements related to information security and will commit to continual improvement of the information security management system.

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, SEBPLC is committed to ensure cyber security, protect its information assets and manage its IT infrastructure in a safe and secure manner.

For achieving the desired level of protection, SEBPLC 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 SEBPLC is continued.

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

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

SEBPLC considers the views of its stakeholders in strengthening the reliability of its Information Security Management System so that, as a bank, SEBPLC can excel, fostering growth and prosperity for the country.

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

Endorsed By:

.....

Managing Director (Current Charge)
Southeast Bank PLC.