INFORMATION SECURITY POLICY

CAPITALFIELD INVESTMENT GROUP LIMITED
& SUBSIDIARIES

Our Policy Statement

CIGL's leadership is committed to establishing and complying with Information Security Management System (ISMS) requirements applicable to its business and will continually improve the management system for the protection of its asset and that of stakeholders in its custody. The leadership has authority to sanction any stakeholder, who breaches or compromises its information security policy.

Roles and Responsibilities

a. The GMD of CIGL has the responsibility for information security and has authority to sanction any violation. He may delegate it to any direct report for oversight and enforcement.
b. The Head of IT oversees the company's information, cyber, and technology security.
c. All employees of CIGL shall comply with information security procedures including the maintenance of data confidentiality and integrity.
d. All those assigned information system assets of CIGL shall be responsible for their operational security.
e. Each information system user shall comply with the security requirements that are in force at anytime, and shall ensure that the confidentiality, integrity and availability of the information or data in use is maintained to the highest standard.

See the detailed policy on the intranet.

Signed: 

For: The GMD