ACC Limited('**ACC**') recognizes the importance of cyber security and data privacy in ensuring sustainable growth and business continuity across the organisation. Information systems and data resources of ACC are critically important assets for its business operations and effective customer services.

ACC is committed to establishing and improving cyber security preparedness and minimizing its exposure to associated risks to safeguard ACC assets. All ACC businesses and functions will implement adequate security policies, processes, and controls to protect confidentiality, maintain integrity, and ensure availability of all information assets.

This policy requires all Businesses under ACC:

- To comply with the applicable national and international cyber security standards.
- Implementation of control and monitoring measures for all hardware and software assets in use throughout the organization.
- Implementation of management protocols for protection and security of stakeholder assets.
- Risks to information and cyber systems are identified and mitigated to acceptable level through a formal documented procedure.
- Critical information is protected from unauthorized access, use, disclosure, modification, and disposal, whether intentional or unintentional.
- The confidentiality, integrity and availability of such information acquired permanently or in transit, provided or created are always ensured.
- To conduct regular cyber-security audits following appropriate national and international standards to maintain compliance.
- To establish clear-cut reporting channels for any form of violation of the Cyber Security and Data Privacy policies and any other specific information security and management policy as the case may be.
- To protect ACC stakeholders, information and assets from threats that could potentially disrupt business and ACC brand and reputation.
- To communicate the importance of cyber security and to continually enhance information security capabilities to all the concerned.
- To collaborate with cyber security and data privacy experts to continually upgrade the information management infrastructure.

- All Business Heads/Department Heads are directly responsible for ensuring compliance with this policy in their respective business domains.

- All breaches of information security, actual or suspected, are reported, investigated by the designated personnel and appropriate corrective and preventive actions initiated.

This policy applies to all stakeholders who access ACC's information or networks: Full Time Employees, Off-roll employees, including but not limited to subsidiary staff, contractors, consultants, temporary staff affiliated with third parties, including system vendors and staff from outsourcing companies.

This policy also applies to all information, computer, and data communication systems owned, licensed, and administered by ACC or its service providers and covers manifestations of other ACC's information such as voice and data.

The content and robustness of implementation of this policy will be reviewed periodically and revised accordingly, as needed.