CCI Information Security Policy

In CCI, all Employees and Third Parties share in the responsibility of safeguarding the information used to support our business operations. Our information can be viewed as a form of currency. We exchange this currency thousands of times and like other forms of currency, we have to protect against loss or theft, including loss or theft by parties who try to gain access to our information through the unsuspecting actions of our employees, through backdoor channels, or through illegal methods.

The following are basic principles of the Information Security Policy:

1. The Policy is global and applies to all Employees and Third Parties with access to CCI information.
2. The Policy applies to information in any form, including data that is electronic, hard copy or verbal; sent in an email; uploaded to a website; saved to a USB drive, or accessed on a smartphone or tablet computer.
3. Regardless of where information is located, CCI information must be properly protected against unauthorized access and disclosure.
4. Employees are responsible for the protection of CCI information collected, transmitted, stored, or processed by Third Parties.
5. Violation or disregard of the Policy may be considered a violation of the CCI Code of Ethics and may result in disciplinary action up to and including termination.

The following are high-level objectives of Information Security Policy:

1. Assure confidentiality, integrity, and availability of information assets
2. Compliance with related laws, standards, and regulations
3. Establish an information security management system(ISMS) and continual improvement of ISMS
4. Augment awareness of all employees and third parties
5. Define an information security risk management approach/process and conduct regular assessments/treatment as defined in the Information Security Risk Assessment Procedure.