Statement of Commitment to Information Security

Statement of Commitment to Information Security

Canacol Energy ("Canacol") is committed to the protection of its information and has zero tolerance for any form of criminal or illegal behavior relating to the company´s information and data security. Efforts are directed and based on ISO27001 - Information Security Management.

Canacol is critically dependent on information and information systems. Thus, the reputation that the company enjoys is also directly linked with the way it manages such information. So, in case important information is disclosed to third parties (which could result in inappropriate or illegal actions) or information systems were compromised, Canacol could suffer serious losses or go out of business.

All employees, contractors, consultants, temporary staff, and personnel affiliated with third parties engaged by Canacol are expected to behave in a manner that promotes the best practices in cybersecurity, protecting themselves, associates, and corporate assets from cyber-attacks. In addition, they are expected to understand that privacy will be limited when using company´s equipment and cyber systems are not provided for personal use.

In this sense, Canacol's security programs rely on the diligence of its employees and affiliates. As such, it is required that they act in accordance with our security programs and comply with all cyber security laws in all countries of operation, in addition to Canacol's Security and Data protection policy.

In compliance with the applicable laws and internal regulations and policies, Canacol may terminate its contractual relation with any employee or contractor who violates the company´s security policies. In this event, Canacol may also initiate and conduct legal proceedings to the full extent of the law, against the employee or contractor.

Finally, considering Canacol´s management, direction and responsibilities, and acknowledging the right to Habeas Data, the company will regularly assess security vulnerabilities and threats to business operations and manage the identified risks through mitigation actions. This, in order to minimize the probability of a material impact due to a cybersecurity breach.

Charle Gamba

CEO

Nov, 2021