IT Information Security Policy

a. Purpose

Constance Hotels Services Ltd ('Company') considers information as critical for its operations and long-term growth.

The IT Information Security Policy incorporates the information and information-security policies recommended by the National Code of Corporate Governance for Mauritius and aligns with the Data Protection Act 2017 as well as the European Union General Data Protection Regulations (EU GDPR). It relates to both computer-based and paper-based information.

The purpose of the IT Information Security Policy is to:

- Define the responsibilities of individuals with regard to the use of information; and
- Define the responsibilities of individuals with regard to the provision and use of information processing systems.

b. Scope of Application

This Policy applied to information held by the Company and its subsidiaries, and used by employees, students, volunteers and outside affiliates.

c. Structure and Content

The IT Information Security Policy is structured in 6 distinct sections as follows:

Section	Sub-Section	Description
1. Principles	N.A	▯ Principles adopted by the Company in respect of information security. ▯ Definition of Information Security and Key Terms.
2. Risk Management	N.A	▯ Thorough analysis of all information networks and systems on a periodic basis to document the threats and vulnerabilities to stored and transmitted information.
3. Information Security Responsibilities	N.A	▯ Identification of responsibilities for each participant type in the information security framework, namely: Information Security Officer, Information Owner, Custodian, User Management and User.
4. Information Classification	N.A	▯ Information to be classified according to four levels, namely: public, open/business, confidential and strictly confidential.
5. Computer and Information Control	Ownership of Software	▯ All computer software developed by the Company's employees or contract personnel on behalf of the Company or licensed for the Company use is the property of the Company.
	Installed Software	▯ All software packages that reside on computers and networks within the Company must comply with applicable licensing agreements and restrictions, and the Company's acquisition of software policies.
	Virus Protection	▯ Virus-checking systems approved by the Information Security Officer and Information Services must be deployed using a multi-layered approach to ensure all electronic files are appropriately scanned for viruses. ▯ No user is authorised to turn off or disable virus-checking systems.
	Access Controls	▯ A comprehensive range of security measures and mechanisms has been deployed by the Company to ensure physical and electronic access to open, confidential and strictly confidential information and computing resources is controlled in accordance with each user's authorised level of access. ▯ Security measures include precautions to be taken with respect to data transfer, printing and oral communications, the implementation of audit controls, periodical evaluations and contingency planning, data leakage prevention and protection of mobile devices.
6. Compliance	N.A	▯ Failure to comply with this Policy may result in disciplinary action up to and including dismissal in accordance with the Company's applicable procedures or, in the case of outside affiliates, termination of the affiliation.