IT Code of Practice

a. Purpose

The IT Code of Practice of Constance Hotels Services Ltd ('Company') incorporates the Information Technology Policies recommended by the National Code of Corporate Governance for Mauritius.

The purpose of the IT Code of Practices is not meant to restrict the general openness experienced in a creative organisation, but merely to safeguard certain essential activities of the Company with focus on the governance of information-related technologies.

b. Scope of Application

The IT Code of Practice applies to computing facilities:

- Controlled by Constance Hotels, Resorts & Golf; or
- Owned by the Company; or
- Situated on any of the hotel premises of the Constance Hotels, Resorts & Golf.

c. Structure and Content

The IT Code of Practice is structured in 19 distinct sections as follows:

Section	Description
1. Regulations about the use of Computing Facilities	• Requirements for the use of computing facilities and possible actions in the case of a breach of the IT Code of Practice.
2. Access to Facilities	• Authorisation to be obtained for the use of computing facilities. • Misuse of computing facilities should be brought to the attention of the IT Department. • Offensive materials may not be displayed or printed.
3. Passwords	• A password is the key to the security of information, and more generally the integrity of the network system. • A user is responsible for all activities and possible misuse originating from his/her account. • Guidance with regard to the selection and change of passwords.
4. Information Storage & Publication	• Users must recognise that the resources of the Company's network are limited and take due account of this in any use of the system.
5. Data Protection	• Users who process personal data must strictly comply with the Company's Data Protection Policy.
6. Publication of Information	• No user may create, store, exchange, display, print, publicise or circulate offensive or illegal material in any form.
7. Copyright Material	• A user must not copy any copyright material without the written permission of the owner of the copyright.
8. Electronic Mail	• A user is responsible for all electronic mails sent from his/her account. • Any misuse of electronic mail should be reported to the IT Department.
9. Backups and Storage	• Regular backups are recommended. • Backup media should be stored away from the equipment they protect, in case of machine failure, fire or catastrophe.
10. Information Systems Implementations	• All information systems projects, whether big or small, should go through the IT Department prior to deployment.
11. Virtual Private Network	• Employees with VPN privileges are responsible for ensuring that unauthorised users are not allowed access to the internal networks.
12. Equipment Decommissioning	• Equipment which is no longer of use should be fully decommissioned.
13. Misuse of Facilities	• No user may seek or secure unauthorised access to any program or data held in any computer wherever located; a user must not attempt to decrypt system or user password or copy system files. • No user may effect unauthorised modification of the contents of any computer.
14. Discipline	• Use of computing facilities in breach of this Code of Practice may lead to the restriction of access to or the withdrawal of computing facilities.
15. Company Liability	• The Company accepts no responsibility for the malfunctioning of any computing facility, loss of data, or the failure of any computer security system, or any losses while using company systems. • The Company does not guarantee the continued availability of any IT facilities and accepts no liability for any loss or damage cause by the temporary or permanent withdrawal thereof.
16. Usage Monitoring and Inspection of Files	• IT administrators may monitor the activities and inspect the files of specific users on their computers and network.
17. System and Network Administration Access	• An IT administrator may access other users' files for the maintenance of network computer and storage systems.
18. Document Printing	• Users should abide by the communicated printing guidelines, except for printouts related to guest usage namely registration card, welcome/departure letters, etc.
19. Energy Saving	• Team members should adopt energy-saving behaviours.