Mauritius Telecom Data Centre – Information Security Policy Statement

Objective

The objective of this policy is to establish the necessary policies, procedures and an organizational structure that will protect Mauritius Telecom Data Centre's information assets and critical activities from all appropriate threats and to ensure regulatory, contractual and legislative requirements are met.

Policy

- Information assets and information processing facilities shall be protected against unauthorized access
- Information shall be protected from unauthorized disclosure
- Confidentiality of information assets shall be a high priority
- Integrity of information shall be maintained
- The management of the supply chain shall ensure appropriate information security and business continuity measures are included in contracts, where possible, so that the supplier is able to deliver acceptable levels of service
- Business continuity plans shall be produced, maintained and tested
- Use of information assets and information processing facilities shall be in accordance with policies and procedures
- All incidents actual or suspected, shall be reported and investigated in line with Data Centre policies and procedures
- Controls shall be implemented to manage the risks faced by the Data Centre
- Adhere to the requirements of ISO27001:2013

The Data Centre Management team commit to continual improvement through a process of management review, regular internal/external audits and security incident reporting.

The policy will be reviewed as and when required to ensure that it continues to be appropriate to the needs of the business.

Name: Yagianath Rosunee

Signature: ....

Position: Chief Technical Officer   Date: 20th December 2022