ICT Information Management and Security Policy

1. Introduction:

This document sets out the procedures for ICT Information Management and Security Policy.

2. Purpose:

To outline the direction, scope, and approach to the secure management of Information Assets and Information Systems within ITM ICT environment. The intent is to protect Information Assets, and any ICT Assets which create, process, store, view or transmit Information against unauthorised use or accidental modification, loss or release.

3. Scope:

This policy applies equally to all Users who have access to the ITM's Information Assets and related Information Systems.

4. Procedure:

ITM is committed to the management of risks associated with Information and Communications Technology (ICT) Assets and Information Systems and the reduction of ICT security incidents. This policy provides the governance framework for Information management and security within the building and defines the policy in all aspects of Information Security.

4.1. Information Security activities are concerned with the protection of Information from unauthorised use or accidental modification, loss or release. Information Security is based on the following five elements:

- **Confidentiality -** ensuring that information is only accessible to those with authorised access
- **Integrity -** safeguarding the accuracy and completeness of information and processing methods
- **Availability -** ensuring that authorised users have access to Information when required
- **Compliant Use -** ensuring that users meet all legal and contractual obligations.
- **Responsible Use -** ensuring that appropriate controls are in place so that users have access to accurate, relevant and timely Information

4.2. ITM will apply measures to ensure that the level of physical controls implemented will minimise or remove risk of equipment or Information being rendered inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation.

5. Access Management:

ITM will put in place control mechanisms based on business requirements, assessed/accepted risks, Information classification and legislative obligations for controlling access to all Information Assets and ICT Assets. At a minimum will ensure:

- Authentication requirements, including on-line transaction and services must be appropriate for the security classification of the information.
- Access to the ITM network and Information Systems requires specific authorisation and each User must be assigned an individually unique personal identification code and secure means of authentication

6. Incident management:

ITM will apply methods to ensure that effective management and response to Information Security incidents is critical to maintaining secure operations within the premises. ITM at a minimum will:

- establish and maintain an Information Security incident and response register and record all incidents
- Ensure all Information Security incidents are reported and escalated (where applicable) through appropriate management channels and/or authorities. Ensure that these incidents are investigated and if it is found that a deliberate Security violation or breach has occurred, apply formal disciplinary processes

7. Business continuity management:

ITM will ensure that a managed process including documented plans are in place to enable Information and ICT Assets to be restored or recovered in the event of a disaster or major security failure. There will be plans and processes to asses the risk and impact of the loss of information an ICT assets in the event of a disaster or security failure. Further develop methods for reducing known risks to ITM Information and ICT assets. Ensure business continuity Information and ICT Asset disaster recovery plans are maintained and tested to ensure Systems and Information are available and consistent with service level requirements.

8. Compliance management:

ITM will implement practices to ensure compliance with, and appropriate management of, all legislative and reporting obligations relating to Information Security. All Information Security policies, processes and requirements including contracts with ICT third parties, are reviewed for compliance on a regular basis. All reasonable steps are taken to monitor, review and audit Information Security compliance, including the engagement of internal and /or external auditors and specialist organisations where required.

9. Disclaimer:

ITM makes no warranty, explicit or implied, regarding the ICT services offered. Similarly, no responsibility can be accepted by ITM or its Employees, for any damage arising directly or indirectly from the use of these services. The responsibility for protecting ICT resources and services resides with all Users, who use these services. ITM will make all reasonable efforts to protect from possible ICT and computer-related dangers but advises that it cannot always protect from all potential threats. ITM cannot guarantee to protect an individual against exposure to material that may be offensive to them, as such ITM staff are warned that they may traverse or receive material that they find offensive.

10. Policy, monitoring and review:

The ICT Manager, or their delegate, is responsible for the review of this policy. This manager shall ensure that this policy is reviewed at least once each calendar year. Compliance with this policy is monitored/audited on a regular basis, as determined by risk assessment.