Information Security Policy

1. Purpose

Metro Assist is committed to managing information security in accordance with the organisational policies, and relevant contractual requirements, laws and regulations.

This policy outlines how Metro Assist will manage and mitigate security risks to safeguard the confidentiality, integrity and availability of Metro Assist information, communications, technology assets and business environment.

2. Scope

This policy applies to Metro Assist directors, employees and volunteers, students on placement and extends to contractors, entrusted third party service providers and other members of the Metro Assist's supply chain who are provided access to Metro Assist's systems or data in the delivery of their services.

The networks, devices and data that is stored, accessed, transmitted, displayed, relayed and/or processed by Metro Assist and other systems supporting service delivery are included in the scope of the policy. This includes the assessment and treatment of information security risks documented in the Information Asset Risk Register.

It is the responsibility of each person in scope to ensure compliance with this policy.

Definitions

Term	Definition
Digital Data	Non tangible information assets
ICT asset	Any hardware or data used for or related to information technology or communication.
Information	The term "information" is used to refer to any data (both structured and unstructured), irrespective of its file format and/or its storage medium.
Information assets	Any information that is of value to the organisation. This term also includes the underlying supporting infrastructure such as business processes, hardware, networks, storage, applications, third-party providers and storage amongst others.
Information security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information Security System	That part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security

IT Infrastructure	For the purposes of this policy, the term "IT infrastructure" applies to (but is not limited to) the following infrastructure components owned by, leased to, and/or managed on behalf of Metro Assist: All components of the network (including the communications infrastructure linking the components of the network); Server class systems, mid-range and/or mini-computer(s) upon which Metro Assist information is managed and/or processed; Personal computing devices, laptops, desktops, mobile devices including smart phones; Gateways, firewalls and all other network related devices that control interconnectivity between the Metro Assist IT infrastructure and external systems; and peripheral devices connected to the Metro Assist network together with the: System software; and Information necessary for implementing, operating, managing and/or monitoring components of the infrastructure and their use (including audit log files) used in conjunction with the physical components of the IT infrastructure
Physical assets	Tangible information assets (paper documents, backup tapes etc.)

3. Policy Statement

Metro Assist is committed to the secure management of information and systems utilising a policy framework based on the international standard for security management systems - ISO 27001. Metro Assist will manage information security risks and controls to the extent that there are clear benefits from the control measures.

4. Information security principles

Metro Assist has adopted the following high-level Information security principles to establish a sound foundation for information security policies, procedures and practices.

These principles are:

1. Information, in whatever form whether they are paper-based or stored in internal or external ICT systems or devices, is of fundamental importance to Metro Assist, and the organisation will manage information security within a framework based on ISO 27001.
2. Information security risks will be managed taking into account broader organisational objectives, strategies and priorities.
3. A risk management approach will be used to identify, evaluate and mitigate risks for Metro Assist systems and information assets. This approach is supported by Metro Assist Risk Management Policy and Risk Management Framework.
4. In line with the requirements of the ISO 27001 Standard, this policy is based on the following three elements of information security:
    - **Confidentiality:** ensuring that information will be accessible only to those authorised to have access
    - **Integrity:** safeguarding the accuracy and completeness of information and processing methods, and

- **Availability:** ensuring that authorised users will have access to information and associated assets when required.

5. Metro Assist's management will actively support information security within the organisational culture through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities. This will ensure information security management is embedded in operational activities and processes.
6. Continuity of operations will be heavily dependent upon the confidentiality, integrity and continued availability of information and the means by which it is gathered, stored and processed, communicated and reported.

5. Classification of information
   Metro Assist's treatment of all personal and health information, whether it relates to a customer or client, an employee or another person (such as a contractor) is considered sensitive and thus Metro Assist only collects, holds, uses and discloses personal and health information for the purpose of carrying out its functions.

6. Responsibilities

Board of Directors

Metro Assist Board establishes information security policy and assume oversight responsibility in managing information security risks.

CEO

Operational responsibility for information security rests with the Metro Assist CEO, however responsibility for the management of information security within the system is also delegated to the Managers within their area of program/function responsibilities.

The CEO is responsible for the business's protective security and security practices (both physical and information based), and to make determinations in relation to ICT investment within the delegated authority.

Corporate Service Manager

The Corporate Service Manager acts as Information Security Officer (ISO) and has responsibility to implement appropriate information security controls processes and technologies to protect Metro Assist from cyber security threats and information security incidents. The specific responsibility includes:

- Align business and security objectives with contractual requirements
- Set up information security system and maintain and review the information security policy and associated procedures, and ensure that the policy is readily available to staff
- undertake risk-assessments of the information assets in coordination with the Program/Department Managers and advise on information security risks and controls
- deliver security awareness activities to raise awareness and understanding of the obligations identified in this policy and educate users on how to reduce the risks of information security incidents.
- Coordinate cyber incident response
- Ensure that security measures and efforts are undertaken in a coordinated manner

External ICT contractor/System Administrators

The external ICT service providers contracted to manage Metro Assist's network and system is responsible for

- implementing logical, physical and environmental controls to secure information processing facilities and data
- identifying and complying with relevant information security and privacy regulatory frameworks, relating to technology and data use, storage and transmission
- designing and implementing controls to minimise the risk of unauthorised access, disclosure, modification, or destruction of information, whether accidental or malicious
- ensure the employees of the service providers are adequately inducted and trained in information security management
- ensure system logs, including audit, access, activity and performance logs are captured and retained according to regulatory and Metro Assist's operational needs.
- Provide technical advice on security environment and system need/performance

ICT Coordinator

The ICT Coordinator is responsible to ensure:

- implementing logical, physical and environmental controls to secure information processing facilities and data as delegated
- administer and manage Metro Assist network and system access control
- Manage the day–to–day information security of the system
- Coordinate the technical efforts of Information Technology Security Officers
- undertake risk-assessments of the technology control environment and advise on information security risks and controls in consultation with the external ICT service providers

Site Managers/Administrators

Responsible for the day-to-day physical protective security measures at the site.

Managers

Managers are responsible for

- undertaking risk-assessments of the information assets within their area of operation in set up information security controls
- ensuring staff are inducted and trained on information security requirements and controls set to manage risks for both paper based and digital information assets.
- ensuring compliance with this policy and monitor IT security performance of the team
- reporting any information security incident to the Corporate Service Manager and fulfil the responsibility of the response team member (if required)

Employees, Contractors and volunteers

All staff, contractors and volunteers must:

- read, understand and adhere to their obligations in relation to this information security policy and associated plan and procedures in the context of their relevant area of expertise
- report and respond to any suspected or actual security breaches or and respond to the breaches

- ensure the security and protection of information assets. Non-compliance with these responsibilities may lead to disciplinary and/or legal action.
- Keep user IDs password secure, active and registered
- ensure ITS endorsement is obtained for all software installed on the Metro Assist network,
- engage Corporate Service Manager and ICT coordinator for all technology-related asset procurement, including IT hardware, software, and cloud services, to ensure alignment with Metro Assist IT strategy, policies, standards and the Metro Assist's risk appetite

Staff members are responsible for ensuring they undertake appropriate security measures to protect Metro Assist information assets. Non-compliance with these responsibilities may subject to appropriate measures ranging from disciplinary to legal action.

24. Document Review and Approval

This document shall be submitted to the Metro Assist Board or (or delegate) for review and approval in any of these conditions:

- Prior to initial release for circulation
- Upon receipt of any revision on Metro Assist internal policies or procedures that may affect the integrity of this document
- On an annual basis, where there are changes to this document or not