Information Security Policy

The Policy of MiCiM is, on a continuing basis, to exercise due care and due diligence to protect Information Systems from unauthorised access, use, disclosure, destruction, modification, disruption or distribution.

This will ensure that our reputation with our clients is maintained through confidentiality, integrity and availability.

Management will ensure business, legal, regulatory requirements and contractual security obligations are taken into account.

Risk Assessments against agreed criteria is continually undertaken.

The Management Team bears the responsibility for establishing and maintaining the system and undertakes to ensure its integrity is maintained through instruction and training of its personnel and that each employee has a proper understanding of what is required of them.

Equally, every employee has a personal responsibility to maintain this integrity.

Further, the Management will ensure any subcontractor employed for a particular function will meet the requirements specified and accept responsibility for their actions.

The Organisation has a Policy of Continuous Improvement and Objective setting in line with the ISO 27001:2013 Standard.

The Information Security Management System will be monitored regularly under the Top Management's ultimate responsibility with regular reporting of the status and effectiveness at all levels.

All of MiCiM's information security measures try to address at least one of the following three goals:

- Protect the confidentiality of data
- Preserve the integrity of data
- Promote the availability of data for authorised use

These goals form the confidentiality, integrity, availability (CIA) triad:

Confidentiality protocols are primarily intended to ensure that no unauthorised access to information is permitted and that accidental disclosure of sensitive information is not possible. Examples of MiCiM's confidentiality controls are the use of user IDs and passwords.

MiCiM's **Integrity** model keeps data pure and trustworthy by protecting system data from intentional or accidental changes. Integrity models have three goals:

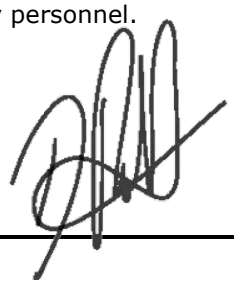
- Prevent unauthorised users from making modifications to data or programs
- Prevent authorised users from making improper or unauthorised modifications
- Maintain internal and external consistency of data and programs

An example of MiCiM's integrity protocols are the controlled access of certain files, defined for certain roles and levels of seniority.

Availability keep data and resources available for authorised use, especially during emergencies or disasters. Information security professionals usually address three common challenges to availability:

- Denial of service (DoS) due to intentional attacks or because of undiscovered flaws in implementation (for example, a program written by a programmer who is unaware of a flaw that could crash the program if a certain unexpected input is encountered)
- Loss of information system capabilities because of natural disasters (fires, floods, storms, or earthquakes) or human actions (bombs or strikes)
- Equipment failures during normal use

An Example of MiCiM's Availability controls include; applying encryption to information that will be stored on digital media (accessible only to MiCiM Hardware), periodically testing computer system security to uncover new vulnerabilities, building software defensively, and developing a disaster recovery plan to ensure that the business can continue to exist in the event of a disaster or loss of access by personnel.



Daniel Potter

Commercial Director
MiCiM Ltd

Date: 14th February 2021