Information Security Policy

MiCiM is committed to the ongoing protection of its Information Systems through the application of due care and due diligence in accordance with our ISO 27001:2022 management system and Cyberessentials accreditation. Our objective is to safeguard against unauthorised access, use, disclosure, destruction, modification, disruption, or distribution of information. This commitment ensures the confidentiality, integrity, and availability of data, thereby preserving our reputation and trust with clients.

Governance and Responsibility

Management Commitment: MiCiM's management is responsible for ensuring that all business, legal, regulatory, and contractual security obligations are identified and met.

Risk Management: Risk assessments are conducted continuously against defined criteria to identify and mitigate potential threats.

System Integrity: The Management Team is accountable for establishing, maintaining, and improving the Information Security Management System (ISMS). This includes providing appropriate training and guidance to ensure all personnel understand their responsibilities.

Employee Responsibility: Every employee is personally responsible for upholding the integrity of the ISMS.

Third-Party Assurance: Subcontractors engaged by MiCiM must meet defined security requirements and accept accountability for their actions.

Continuous Improvement

MiCiM is dedicated to continuous improvement and objective setting in alignment with the ISO 27001:2022 standard. The ISMS is regularly reviewed and monitored under the oversight of senior Management, with performance and effectiveness reported across all levels of the organisation.

Information Security Objectives

MiCiM's information security measures are designed to achieve the following core objectives, known as the CIA Triad:

- Confidentiality: Ensuring that information is accessible only to those authorised to have access.
- Integrity: Safeguarding the accuracy and completeness of information and processing methods.
- Availability: Ensuring that authorised users have access to information and associated assets when required.

Implementation of the CIA Triad

Confidentiality

Confidentiality controls are in place to prevent unauthorised access and accidental disclosure of sensitive information. Examples include:

- Use of unique user IDs and secure passwords
- Role-based access controls

Integrity

Integrity protocols ensure data remains accurate and trustworthy. These include:

- Restricting modification rights to authorised personnel
- Preventing improper changes by authorised users
- Maintaining consistency across systems and data sources

Example: Controlled access to specific files based on role and seniority.

Availability

Availability measures ensure data and systems remain accessible during normal operations and emergencies. These include:

- Protection against denial-of-service (DoS) attacks
- Disaster recovery planning
- Regular system testing and vulnerability assessments
- Encryption of data stored on digital media accessible only via MiCiM hardware

Asset Management

- All IT assets will be recorded in an asset register, including information on serial number, maintenance and repairs, asset owner (responsible) and if and when an asset is issued to a user.
- All company assets will be recorded in an asset register including information on purchase date, value, maintenance (PAT, MOT), asset owner (responsible) and if and when an asset is issued to a user.
- Assets issued to a user will be subject to an acceptable usage policy and be signed/dated by the receiving user and issuer.
- The asset register shall be securely stored, accessible only by authorised personnel.
- The asset lifecycle will be tracked, including procurement, issuance, maintenance, and retirement/disposal stages.
- A quarterly audit will be conducted to reconcile the register with physical assets and usage logs.

Company and Mobile Devices

- All company devices must be enrolled in MiCiM's Mobile Device Management platform and comply with baseline security profiles
- Only company issued devices may be used to conduct business
- Issuance of devices will be recorded on the asset register.
- Devices must be encrypted to a minimum of AES128, AES256 is preferable, and where possible a Trusted Platform Module chip should be utilised (laptops)
- All devices must be secured by means of a PIN or secret password.
- Users may not (and should not be able to) install any unapproved apps/programs.
- All devices operating system and programs should be kept fully up to date and patched.
- Access through unsecured internet services must be via the MiCiM VPN.
- All devices are subject to remote management by the company (remote control, wipe, disablement)
- Company data may be accessed, but must be saved on the relevant company drive. It should not solely be stored on the device itself.
- Sharing of company assets, and passwords with any third party is strictly prohibited.
- Only MiCiM approved devices should connect to the MiCiM Network. All other devices must use the guest Wifi.
- Users are not permitted to take personal backups of company information, if there is a requirement for an issued device to be backed up, the company will provide a solution. Third party backup software is also prohibited.
- Only licensed, genuine software should be installed on devices. Illegitimate software is not permitted. Office licences are assigned to users as part of their 365 subscription.
- Where applicable, devices will have a corporately managed antivirus/malware product installed, which should be configured for regular scans or on-access scanning. Webroot Secure Anywhere or other approved software.
- Two factor authentication should be used where possible (such as smartcard & password for laptop)
- Users should not have admin privileges on their issued devices or other assets. Authorisation for changes and requests should be sought from the line manager.
- Upon offboarding or return, all devices must undergo IT-controlled data removal before reassignment or disposal.
- Company-issued devices are monitored in accordance with our Acceptable Use and Privacy Policy.

Removable Media

- Consumer removable media will be unavailable for users unless it has been fully encrypted by corporate approved software and included on the asset register.
- Data Loss Prevention software will be leveraged to reduce the risk of data theft and loss.
- Any removable or offsite backup medium should also be fully encrypted with a secret key.

- Storage in servers at the hardware level should also be encrypted (encryption at rest)
- All removable medium should be included on the asset register and an audit log of any actions kept (Create, Use, Update & Destroy).
- Any transporting of storage medium should only be undertaken by a defined list of trusted, reliable couriers and in tamper proof packaging.
- Directors and Senior Members of Staff can be considered.
- Data must be encrypted on the medium and encryption keys may not be transported in the same manner as the medium.
- Verification of courier identification is required before transfer of the medium.
- Chain of custody is required to be kept in the asset register.
- All medium should be thoroughly wiped before re-issue, re-use, or destruction.
- USB ports on all endpoints will be disabled by default and only enabled through IT exception processes

Networks and Network Access

- MiCiM operates a Zero Trust model: all access requests must be explicitly verified and granted based on device, user, and context.
- All SharePoint sites must be configured according to business need, with access permissions reviewed quarterly.
- All data packets on the network should be traceable to an individual user or terminal.
- "New" devices on the network will need to be manually approved/verified before access is granted.
- Where possible access to a network should be validated by a user verification mechanism such as LDAP lookups (RADIUS)
- Edge network firewalls will be used to restrict inbound/outbound traffic to those defined in the corporate policy. Data through the firewall should also be subject to inspection – such as IPS and packet verification.
- Networks will be segregated based on network requirement and function.
- Default firewall rule will be to block inbound traffic and outbound traffic not on corporately agreed ports (80, 443, 25, 53 etc)
    - All firewall rules will be subject to review for necessity
    - Subscription services should be up to date
- Remote access will be limited to defined group of people, all connections will require a unique username/password.
    - It is suggested that user authentication is made against an on-site LDAP/AD server to reduce account littering.
- Remote access services will be limited to use via a company asset such as laptop or phone, personal devices are not permitted to be connected to the corporate network in any circumstance.

Information Security and Controls

- Office 365 is leveraged in a number of ways across the business, the most utilised being Sharepoint and Exchange.
    - SharePoint in Office365 is leveraged for cloud-based file access and shares. Multiple distinct sites exist with separate permissions. There is a subset of permissions for the business share.
    - Exchange in Office365 is leveraged for user mail flow. All users have their own mailboxes.
- All users of Office 365 are required to setup an additional authentication token when they first login to their account. All administrative users in Office 365 are required to use two factor authentication.
- Users in Office 365 are synchronised against an on-prem active directory server for single sign on authentication and permissions.

Cryptography

- Cryptographic mechanisms will be implemented across the business. These mechanisms should be AES256 where possible, but where not AES128 should be used.
- All secret keys and key pairs used for administrative access to systems will adhere to a corporate standard and changed regularly.
- Secret keys must be a minimum of 8 characters, may not be a dictionary word, and contain: uppercase, lowercase, numbers and symbols.
- The recording system should keep an audit log of whom and when created a key, who has accessed it and when, when the key should be removed from production and destroyed.

Access Control and Physical Security

- Defined access groups should be created to limit user access to software functions they do not need.
- Physical access to all servers should be secured.
- Access to the system should be discussed and agreed with SMT
- Access to systems should be periodically reviewed, and unnecessary access revoked.
- Accounts should be issued to all those that require access to a system, the sharing of accounts is not permitted.
- Company IT equipment should be physically separate to that managed by external parties.
- Company equipment and medium should not be left unattended in public.
- A clear desk policy should be enforced.
- Users should terminate or disconnect (lock) devices when not in use or if being unattended.
- Confidential information should only be printed on the approved printers and carried out securely so that the job is only printed when the user is at the printer.

- Site security perimeter should be clearly defined and there should be no gaps or breaks, all external doors should be alarmed.
- Access should be granted to areas only on a requirement basis.
- Unsupervised access in secure areas should be avoided.

Security Event/Incident Management

- All security events and incidents, be they physical or virtual, resulting in breach or not should be immediately reported to the IT Team and escalated to Daniel Potter.
- IT Team will log the incident and audit the events that took place before the incident.
- Where any evidence of device tampering is found the device will be subject to a full diagnostic.
- In the event of breached credentials an immediate block will be enforced on the domain controller and thus office 365. All users will be required to reset their passwords.
- In the event of an information breach, IT Team will investigate and attempt to find the source, destination, classification and extent of the breach and advise the business whether or not the information in question requires them to notify authorities.
- All security events will be discussed at the SMT meeting and any notifications to relevant authorities will be actioned through the SMT.

Daniel Potter

Director

July 2025