MCFM GLOBAL ACADEMY POLICIES

2024-2025

Cyber Security Policy

Effective Date: 21st March 2024

Revision Due Date:20th March 2025

MCFM Global Academy is committed to maintaining the confidentiality, integrity, and availability of information assets and ensuring the security of our digital infrastructure against cyber threats and vulnerabilities. The following policies and procedures guide our approach to cybersecurity:

1. **Information Security Governance:**
    a. We establish and maintain an information security governance framework that defines roles, responsibilities, and accountability for information security management.
    b. Senior management provides oversight and support for information security initiatives and ensures alignment with organisational goals and objectives.

2. **Risk Management:**
    a. We conduct regular risk assessments to identify, evaluate, and mitigate information security risks associated with the confidentiality, integrity, and availability of data and systems.
    b. Risk mitigation strategies are implemented to address identified vulnerabilities and safeguard against potential cyber threats.

3. **Data Protection and Privacy:**
    a. We implement measures to protect the privacy and confidentiality of personal and sensitive data in compliance with applicable data protection laws and regulations.
    b. Access to confidential information is restricted to authorised personnel only, and data is encrypted, anonymised, or pseudonymised as appropriate to mitigate privacy risks.

4. **Information Security Policies and Procedures:**
    a. We develop and enforce information security policies, standards, and procedures to govern the use, handling, and protection of information assets.
    b. Employees, contractors, and third-party vendors are required to adhere to established security policies and procedures and undergo training on cybersecurity best practices.

5. **Incident Response and Management:**
    a. We maintain an incident response plan and procedures to effectively detect, respond to, and mitigate cybersecurity incidents and breaches.
    b. An incident response team is designated and trained to coordinate response efforts and minimise the impact of security incidents on operations and stakeholders.

6. **Security Awareness and Training:**
    a. We provide ongoing security awareness and training programs to educate employees and stakeholders about cybersecurity threats, best practices, and their roles and responsibilities in maintaining information security.
    b. Regular phishing simulations and security drills are conducted to assess and improve employee awareness and preparedness for cyber threats.

7. **Continuous Monitoring and Improvement:**
    a. We implement mechanisms for continuous monitoring of information systems, networks, and infrastructure to detect and prevent unauthorised access, malicious activities, and other security incidents.
    b. Regular security audits, vulnerability assessments, and penetration testing are conducted to identify and address security gaps and weaknesses in our digital environment.

MCFM Global Academy is committed to fostering a culture of cybersecurity awareness, resilience, and vigilance to safeguard our information assets and protect against evolving cyber threats.

Maxcene Crowe

CEO, MCFM Global Academy