ACCESS MERCANTILE SERVICES

INFORMATION & CYBER SECURITY POLICY

Information and Cyber Security Policy

At **Access Mercantile Services**, we recognise that information security is integral to our operations. It is our information security objective that the information we manage shall be appropriately secured to protect against breaches of confidentiality, failures of integrity or interruptions to the availability of that information and to ensure appropriate legal, regulatory and contractual compliance. To uphold this commitment, we have established and maintain an **Information Security Management System (ISMS)** in accordance with the **ISO/IEC 27001:2022** standard. This framework ensures that our information security practices are systematic, risk-based, and continuously improved

According to the above direction all **Access Mercantile Services** and staff are committed to these objectives:

- Use of all reasonable, appropriate, practical and effective security measures to protect our important processes and assets in order to achieve our security objectives.
- Protecting and managing our information assets to enable us to meet our contractual, legislative, privacy and ethical responsibilities and satisfy applicable IS requirements and legal requirements
- Protect the confidentiality, integrity and availability of information to guarantee that regulatory, operational and contractual requirements are fulfilled;
- Implement and conduct Information and Cyber Security risk management to protect information and related assets from all threats, whether internal or external, deliberate or accidental;
- Encourage personnel to stay up to date with the latest security trends, regulations and procedures and conduct effective training;
- Availability, security and reliability of all the services we provide for our clients even if security incidents occur;
- Maintain and test business continuity plans;
- Review and re-evaluation of Information and Cyber Security management system annually and/ or based on any system changes;
- Protect the system against unauthorized access;
- Report and investigate Information and Cyber Security breaches by Chief Information and Technology Officer
- Set, monitor and continuous improvement of Information and Cyber Security objectives.

Elliott Morey
Chief Executive Officer

Date of Issue: 29th February 2020
Last Reviewed: 12th March 2026