INFORMATION SECURITY MANAGEMENT POLICY

XYNOMIX

CONFIDENTIAL

This Policy sets out Xynomix's (the organisation's) strategic commitment to information security management. It is the policy of the organisation to ensure the confidentiality, integrity and availability of information owned by both the organisation and clients is maintained to:

- Ensure continued quality of service
- Meet the organisation's contractual, legal, and regulatory obligations
- Meet the needs and expectations of other interested parties.

Information security management shall be treated as an integral part of management activities and will be pursued in the same manner and with the same vigour as other managerial objectives.

Xynomix is committed to:

- Taking appropriate action to ensure the confidentiality and integrity of the organisation's and client-owned information held by and managed by the organisation
- Developing, maintaining and exercising business continuity plans to ensure the availability of information and information systems
- Treating information security as a business-critical issue
- Ensuring that legislative, regulatory and contractual requirements are met
- Protecting and respecting the intellectual property rights of the organisation and others
- Creating a security-positive culture within the organisation
- Establishing and maintaining an effective Information Security Forum
- Ensuring information security risks are managed to an acceptable level
- Identifying and implementing controls for information assets that are proportionate to levels of risk
- Communicating this Policy and supporting arrangements to all employees, relevant clients, contractors, and other stakeholders
- Achieving individual accountability for compliance with this Policy, related policies and supporting procedures
- Ensuring all breaches of information security, actual or suspected, are reported and investigated in line with published policies
- Developing, implementing, and maintaining an information security management system (ISMS) in accordance with the best practice contained within ISO/IEC 27001:2022

With support from the organisation's Technical Director and Heads of Department, the Managing Director has overall responsibility and authority to ensure that this Policy is effectively implemented and delivered. All internal personnel and suppliers must play an active role in protecting the organisation's assets and must treat information security appropriately to achieve this purpose.

To support this Policy, subject-specific policies and supporting procedures will be produced in response to changes in risks faced by the organisation, legislation, regulation, contractual obligations, and operational working practices.

Information security objectives, which are aligned with the organisation's strategic business objectives, are agreed on an annual basis, supported by a set of key performance indicators (KPIs) and are monitored by the Managing Director.

The organisation recognises the need for continual improvement. The information security management system will be constantly reviewed, and any changes will be communicated to all relevant employees and interested parties.

Failure to comply with this policy, subject-specific policies and supporting procedures may result in disciplinary action being taken.

INFORMATION SECURITY MANAGEMENT POLICY

XYNOMIX

CONFIDENTIAL

This Policy and the organisation's performance in meeting its requirements will be monitored and reviewed by the Management Team, as a minimum, on an annual basis.