

1.0 PURPOSE AND SCOPE:

- 1.1** Lignacite Ltd is fully committed to protecting all of its information against any loss of confidentiality, integrity and availability that could impact our finances, operations, legal or contractual obligations or on its reputation.
- 1.2** As part of this commitment, the business has established an integrated management system (IMS) that has been designed to fully meet all requirements of ISO 27001:2022.
- 1.3** The business is fully committed to maintaining and continually improving this management system to ensure it remains fully compliant with the ISO 27001 standard.
- 1.4** This policy sets out the measures that will be taken to protect the company's computer systems, infrastructure and other information assets from damage and threats, whether internal, external, deliberate or accidental.
- 1.5** This policy is applicable to all personnel and to both the Brandon and Nazeing sites.

2.0 DEFINITIONS:

2.1 The following definitions are applicable to this policy:

- **Information security** is defined as the preservation of confidentiality, integrity and availability of information and associated information processing facilities.
 - **Confidentiality** refers to ensuring that information is not made available or disclosed to unauthorised individuals, entities or processes.
- Integrity** refers to safeguarding the accuracy and completeness of assets.
Availability refers to information being accessible and usable upon demand by an authorised entity.

3.0 POLICY:

- 3.1** Top level and senior management are responsible for maintaining and monitoring this policy, along with all associated processes, systems and procedures, along with providing guidance and support for their implementation.
- 3.2** Top level and senior management are responsible for ensuring that appropriate resources are provided to permit managers, team leaders and supervisors to both implement and adhere to this policy and all other associated systems and procedures.
- 3.3** All employees are responsible for fully adhering to this policy, associated systems and procedures, along with the key principles laid out within the IMS and associated policies and procedures.
- 3.4** The primary aim of this policy is to:
 - Reduce, so far as is reasonably practicable, the likelihood of an incident occurring which may affect the security of information held by the company.
 - In the event of an incident, ensuring that the business continuity is maintained and impact minimised.

Category: Information Security		Type: Policy		Reference: 1.25	
Page 1 of 3	Issue Date: 12/02/2025	Issue No.: 003	Author: Marvyn Candler		

3.5 The business will achieve these objectives by:

- The establishment, implementation, monitoring, and maintenance of an integrated management system that meets the requirements of ISO 27001:2022, the Data Protection Act 2018 and the UK General Data Protection Regulation (GDPR).
- Ensuring that any changes to the environment, technology employed, threats or legislation are identified and resulting measures reviewed and implemented.
- Understanding the threats posed to information held by the company, its partners and clients.
- Evaluating the threats posed to the data held and systems operated and ensuring that appropriate risk treatments are in place to minimise them.
- Ensuring that all employees understand and fulfil their obligations with respect to information security.
- Setting annual IMS objectives as a platform for ensuring that the IMS system as a whole is compliant with the standard, relevant to the organisation and ensures that the system is subject to continual improvement.
- Ensuring compliance with all legal and other requirements for information security and ensure that information users are aware of and comply with all current and relevant information security regulations and legislation.
- Ensuring suitable and effective training and supervision that provides employees with the knowledge and information to undertake their activities in accordance with specified requirements.
- Undertaking periodic audits on all systems, to ensure compliance and monitor performance.
- Protecting all of the company's assets against loss of confidentiality, integrity or availability.
- Providing a safe and secure information system working environment for employees and any other authorised users.
- Ensuring that all information users understand their own responsibilities for protecting the confidentiality and integrity of the information they handle.
- Protecting the organisation from liability or damage through the misuse of its information.

3.6 Any employee or other authorised user who suspects that there has been or is likely to be a breach of information security, has a duty to immediately inform the management. In the event of a suspected breach or actual security breach, the business may disable or remove any users, data or anything else necessary to secure its information systems.

3.7 Failure to comply with this policy and associated procedures may lead to disciplinary action being taken, which could include dismissal or prosecution.

3.8 Policy statements will be brought to the notice of employees. All Policy statements will be regularly reviewed, revised as necessary and any revisions brought to the notice of employees.

Category: Information Security		Type: Policy		Reference: 1.25	
Page 2 of 3	Issue Date: 12/02/2025	Issue No.: 003	Author: Marvyn Candler		

4.0 ASSOCIATED DOCUMENTATION:

4.1 The following documentation has applicability to this policy:

- Integrated Management System Policy
- Data Protection and GDPR Policy
- Company handbook
- Integrated management system manual

4.2 This policy is supported by additional procedures which can be found in section 6 of the policy and procedure manual.

Signed:..... *G. de Lotbiniere*
GAJ de Lotbiniere, Chairman

Date:..... *28 | 4 | 25*

Category: Information Security		Type: Policy		Reference: 1.25	
Page 3 of 3	Issue Date: 12/02/2025	Issue No.: 003	Author: Marvyn Candler		