Information Security Policy

PBS Utility Services Ltd are committed to preserving the confidentiality, integrity, and availability of all physical and electronic information assets throughout the organisation to preserve its competitive edge, profitability, legal, regulatory, contractual compliance, and commercial image.

Information and information security requirements will continue to be aligned with the company's objectives and the Information Security Management System (ISMS) is intended to be an enabling mechanism for information sharing, electronic operations, and reducing information-related risks to acceptable levels.

The company's existing strategic business plan and risk management framework provides the context for identifying, assessing, evaluating, and controlling information-related risks through the establishment and maintenance of an ISMS. The Risk Assessment, Statement of Applicability and Risk Treatment Plan identify how information-related risks are controlled. The Information Security Project Manager is responsible for the management and maintenance of the risk treatment plan. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks.

Business continuity and contingency plans, data backup procedures, avoidance of viruses and hackers, access control to systems and information security incident reporting are fundamental to this policy. Control objectives for each of these areas are contained within the Information Security Manual and are supported by specific documented policies and procedures.

The company is committed to achieving certification of its ISMS to ISO 27001:2022 and retain thereafter.

This policy will be reviewed annually and is available to all Interested Parties.

Our key objectives are to:

- Establish and maintain an effective and efficient information security management system, planned, and developed in conjunction with other management functions.
- To continually improve our communication and management systems ensuring that we deliver the best possible service to our clients and other interested parties.
- Ensure that the information security management system is an integral part of our business culture by communicating the policy to all employees.
- Conform to contractual, statutory, and regulatory requirements.
- Strive to ensure that all stakeholders are aware of the requirements of our business.
- Ensure the ISMS is subject to continuous, systematic review and continuous improvement through annual internal audits and management review meetings.
- Ensure that employees and other stakeholders are made aware of their individual responsibilities contained within our Management Systems.
- Ensure that the relevant needs and expectations of Interested Parties are considered and met.
- Ensure the integrity of the Management Systems are maintained when changes are planned and implemented.
- Provide leadership towards continual improvement.
- Ensure all employees and certain external parties have the appropriate training.

Signed:

P. Bebb – Director **A. Jones – Director** **S. Piggott – Director** **R. Jones – Director**

Date: 21/08/2026