INFORMATION SECURITY POLICY STATEMENT

Purpose

This Information Security Policy Statement defines the commitment made by Burgoynes to meet, and where possible exceed, the requirements of ISO 27001:2022. It also sets out our commitment to upholding Information Security best practice across our logical domains and physical sites in scope.

Policy Statement

The Burgoynes leadership team recognise the importance of securing our clients' and our own information. Our objective is to maintain the highest standard of confidentiality, integrity and availability of internal, client and supplier information, and to maintain and develop that system through the processes of staff training, incident recording, audits and reviews. We have implemented an Information Security Management System (ISMS) that includes governance of Information Security, to protect our information assets from all threats, whether internal or external, deliberate or accidental.

Information Security is controlled through the preservation of:

- **Confidentiality**: ensuring that information is accessible only to those authorised to have access;
- **Integrity:** safeguarding the accuracy and completeness of information and processing methods;
- **Availability**: ensuring that authorised users have access to information and associated assets.

Client and corporate information are critical business assets. These assets are identified and managed in accordance with the risk assessment methodology that endorses the acceptable risk levels. The success of Burgoynes business is dependent upon the company's ability to store information securely and retrieve and process it as and when required. Such information and the way it may be processed is subject to applicable legislation.

Our Information Security Policy is achieved and implemented through a stringent set of controls, including policies, processes, procedures and software and hardware functions. These controls

are continuously monitored, reviewed, improved and approved by Burgoynes Senior Management to ensure that specific security objectives are met.

A robust system is in place to continually improve the ISMS to:-

- Take account of changes to business requirements and priorities;
- Consider new threats and vulnerabilities
- Confirm that controls remain highly effective and appropriate

The overall effectiveness of the ISMS is reviewed via a formal Management Review process. This strategic review is conducted with representation and approval from the Board.

Security awareness is incorporated in our induction process and training program and our policy is readily accessible internally and presented to existing and prospective clients upon request.

In addition to employees, Burgoynes suppliers, contractors and sub-contractors are required to adhere to our Policy. All staff are empowered to take responsibility for Information Security and a robust process for identifying and reporting security risks and incidents is in place and is regularly reviewed.

Through maintaining our certification to ISO27001, and on-going compliance to regulatory, legal and other applicable contractual requirements, Burgoynes will demonstrate confidence, integrity and credibility both internally and externally to our ISMS.

Monitoring
This policy will be monitored to ensure its continued applicability to Burgoynes.