Revision History:

Section	Description of Change	Date	Issue	Authorised
All	Information Security Policy	18/06/2021	1	P Davison
All	None – Review and re-baseline	04/01/2022	2	P Davison
All	Updated to reflect role changes within organisation	09/01/2023	3	P Davison
All	None – Review and re-baseline	17/01/2024	3	P Davison
All	None – Review and re-baseline	31/01/2025	3	P Davison

The confidentiality, integrity and availability of information are of great importance to the administration and operation of Serios Group Ltd. Failure in any of these areas can result in disruption to the services that we provide as well as loss of confidence in Serios Group Ltd by existing and potential customers. The security of our information and other assets is therefore regarded as fundamental to the successful operation of the organisation. The objective of the Information Security Policy is to ensure business continuity and minimise business damage by preventing and managing at an acceptable level the impact of information security incidents. Adherence to this policy will assist to protect ourselves and our customers from information security threats, whether internal or external, deliberate or accidental.

This Information Security Policy is used as a framework for Serios Group Ltd to set Objectives. These objectives will be reviewed during the Management Review process.

We are committed to good information security provision for customers and staff; hence it is the policy of Serios Group Ltd that we will:

- Ensure a commitment to continual improvement
- Ensure that information is accessible only to those authorised to have access
- Safeguard the accuracy and completeness of information and processing methods
- Ensure that authorised users have access to information and associated assets when required
- Ensure that we meet our regulatory and legislative requirements
- Address the security of all our services and processes to ensure that risks are identified, and appropriate controls are implemented and documented
- Provide a secure working environment for staff on our site
- Produce business continuity and incident response plans for strategic services which will be tested on a regular basis
- Promote security awareness and provide appropriate information security training for our staff

The Compliance Manager is responsible for the production of and the controls to enforce this policy as well as the provision of advice and guidance on its implementation and maintenance.

All breaches of information security must be reported to the Compliance Manager who will be responsible for the investigation and subsequent reporting of all security incidents.

It is the responsibility of all staff and visitors to adhere to this policy.

Serios Group Ltd reserves the right to inspect any data stored on a company computer or telecommunication system, or transmitted or received via our networks, in the cause of investigating security incidents or safeguarding against security threats. This policy shall be reviewed on a regular basis or if significant security changes occur to ensure its on-going suitability and effectiveness.

Mr. P Davison
Compliance Manager
31st January 2025 (Review Date January 2026)