



# Information Security Policy Statement

Issue No:	F1006-4
Issue Date:	25/01/2024
Last Review:	25/01/2024
Classification:	Public

The Information Security Policy statement of Synthotech Limited is to determine, agree and conform to our partner's needs and expectations whilst fulfilling the requirements of relevant policies, standards, legal, regulatory, and contractual requirements.

Synthotech Limited recognises that to be competitive and maintain good security performance in turn-key innovation engineering industry, we must continually improve the management system, including the security of our information and our partners, employees, and other Interested Parties. As part of this, we recognise that we have a responsibility to protect all the data we hold or process, regardless of the owner. By protecting this data, we can ensure that we maintain our reputation as a trusted employer and partner, enabling us to grow as a business and deliver exceptional service to our customers.

To demonstrate our commitment to information security within the turn-key innovation engineering we will implement industry best practice security controls and ensure the effectiveness of these controls through certification to ISO 27001:2022, the global standard for managing information security and that it provides a framework for:

- Incorporating senior representatives from all Synthotech Limited departments with the management and approval functions associated with the ISMS.
- Continually improving the ISMS.
- Setting objectives and establishing an overall sense of direction of principles for actions about security.
- Establishing processes which will provide risk evaluation criteria that are aligned with current Synthotech Limited corporate strategic risk management procedures and policies.
- Listing all information assets and the security risks that may arise for each. The resultant information will inform Synthotech Limited of prospective mitigation priorities.
- Periodically review Synthotech Limited's current processes, policies, and guidance documents and recommend any changes or improvements to ensure we apply appropriate security measures.

It is the responsibility of all our employees, regardless of grade, to become familiar with our security management processes and to comply with all information security and privacy policies and the procedures that underpin them.

In turn, we commit to ensuring that our security management systems and processes are efficient and effective, and continuously improving the protection of our data assets while avoiding the reputational, legal, and financial harm that would result from a data breach.

This policy will be provided to our interested parties on request, to ensure ongoing compliance is attained.

**Name**            Mark Tindley  
\_\_\_\_\_  
  
**Signed**            \_\_\_\_\_  
**Position**        Managing Director  
\_\_\_\_\_  
**Date**              25/01/2024  
\_\_\_\_\_