INFORMATION SECURITY POLICY

1. Purpose

The purpose of this document is to define the role that 12d Synergy's management takes in ensuring commitment to information security, the development and propagation of this policy, and the assignment of appropriate information security roles, responsibilities, and authorities to protect 12d Synergy's assets from all relevant threats, whether internal or external, deliberate, or accidental.
This policy operates in conjunction with the 12d Synergy IT policy handbook, and specifically the Confidential Data policy, Network and Authorisation policy and the Cloud Access and Authentication Policy.
Information on specific encryption and procedures for our cloud service is available in the 12d Synergy Cloud Security Statement, which is available on request.

2. Objective

12d Synergy, which provides data management software and data management software hosting, is committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets (information assets include data or other knowledge stored in any format on any system that has value to an organisation, and should be logged) throughout the organisation in order to compete in the marketplace and maintain its legal, regulatory and contractual compliance and commercial image.

3. Roles and responsibilities

- The management team is responsible for setting and approving the Information Security Policy.
- The CTO is responsible for ensuring that roles, responsibilities and authorities are appropriately assigned, maintained and updated as necessary.
- All employees are responsible for adhering to the requirements of the Information Security Policy and for fulfilling any duties related to assigned roles, responsibilities or authorities. The consequences of breaching the Information Security Policy are set out in 12d Synergy's disciplinary policy and in contracts and agreements with third parties.

4. Policy objectives

It is the policy of 12d Synergy that:

- Information is made available to all authorised parties with minimal disruption as required by 12d Synergy business processes.
- The integrity of this information is maintained, as per the 12d Synergy IT policy handbook.
- The confidentiality of information is preserved, as per the 12d Synergy IT policy handbook.
- The organisation ensures compliance with all legislation, regulations and codes of practice, and all other requirements applicable to its activities.
- Appropriate information security education, awareness and training is available to staff and relevant others working on the organisation's behalf. All staff are required to undergo training regarding best security practices, and read and sign relevant security policies when joining the company. This training is updated on as needs basis and staff undergo this training annually.

- Breaches of information security or security incidents, actual or suspected, are reported and investigated through appropriate processes, in accordance with our Cyber Incident Response Plan.
- Appropriate access control is maintained and information is protected against unauthorised access, as per the 12d Synergy IT Policy handbook.

This policy is approved by senior management and is reviewed at regular intervals or upon significant change.

This policy is communicated to all staff within 12d Synergy and is available to customers, suppliers, stakeholders and other interested parties upon request.

Document control
The CTO is the owner of this document and is responsible for ensuring that this procedure is reviewed.

A current version of this document is available to all members of staff in our corporate 12d Synergy instance and is published at 12d Synergy/12dS Asset Library/10 Policies and Legal. This policy was approved by the CEO and is issued on a version-controlled basis.

Change history record

Issue	Description of change	Approval	Date of change
1.0	Initial draft	CTO	01/07/2021
1.1	Updated with latest policies	CTO	25/10/2021