INFORMATION SECURITY POLICY STATEMENT

1. Purpose
Information is an important asset to **Taclus Confidential** and it is the policy of **Taclus Confidential** that information used for **Taclus Confidential's** activities must be protected from threats which may result in significant financial loss, reputational damage or legislative exposure.

This will be achieved through implementing controls and responsibilities which are readily identifiable by external regulatory bodies, business partners, as being in line with recognised information security standards and which support compliance with relevant legislation.

This includes measures to ensure:

- Confidentiality – information must be protected from unauthorised access and disclosure throughout its lifecycle, from creation to final disposal.
- Integrity – the accuracy and completeness of information must be safeguarded and unauthorised amendment or destruction prevented.
- Availability – information and associated services must be available to authorised users in line with business requirements.
- Legislative compliance – all staff of **Taclus Confidential** must be aware of and comply with UK and EU Law which applies to the processing of information. Personnel data in particular will only be processed, disclosed, shared and retained in accordance with applicable data protection laws and good practice and will only be stored, transferred, copied or communicated when the confidentiality and integrity of the data can be reasonably assured throughout the process.

  To determine the appropriate level of security measures to be applied, a risk assessment must be carried out to identify the probability and impact of security failure. Such risk assessment must be integrated throughout information handling, processes and must be embedded within normal working practices.

2. Scope

This Policy applies to:

- All information created or received in the course of TaclusConfidential business which must be protected according tosensitivity, criticality, and value, regardless of the media on which it isstored, the location of the data, the manual or automated systems thatprocess it or the methods by which it is distributed.
- All approved users of Taclus Confidential information.
- All contractors, suppliers, Taclus Confidential partners and visitorswho may be authorised access to Taclus Confidential information.
- All locations from which Taclus Confidential information is accessedincluding home and off- site/remote use.Information entrusted to Taclus Confidential will be safeguarded inaccordance with this policy.

3.Responsibilities and compliance

Everyone has a responsibility to make informed decisions to protect confidential or personnel information and keep it safe.

All personnel and other approved users of Taclus Confidential information:
- Must be able to demonstrate competence in the understanding of dataprotection laws and good practice applicable to the performance ofTaclus Confidential responsibilities, as described in this policy andguidelines established to protect information and must seek advice andguidance if clarification is required.
- Must report any actual or suspected breach in information security,“near misses” or working practices which jeopardise the security ofTaclus Confidential information.

Non-compliance with this policy is subject to Taclus Confidential’s disciplinary procedures for personnel.

Signed:....*David Lovatt*..... Date: 09/2017

David Lovatt, Managing Director

Next Review Date: 30/10/2019