Information Security Policy

1 Purpose

An effective Information Security Policy provides a sound basis for defining and regulating the management of information systems and other information assets. This is necessary to ensure that information is appropriately secured against the adverse effects of failures in confidentiality, integrity, availability and compliance which would otherwise occur.

2 Scope

The documents in the Information Security Policy set apply to all information assets which are owned by Reddan Group PLC, used by Reddan Group PLC for business purposes or which are connected to any networks managed by Reddan Group PLC. The documents in the Information Security Policy set apply to all information which Reddan Group PLC processes, irrespective of ownership or form. The documents in the Information Security Policy set apply to all employees and any others who may process information on behalf of Reddan Group PLC.

3 Policy Statement

3.1 Principles

- Information will be protected in line with all relevant policies and legislation, notably those relating to data protection, human rights and freedom of information.
- Each information asset will have a nominated owner who will be assigned responsibility for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect the asset.
- Information will be made available solely to those who have a legitimate need for access.
- All information will be classified according to an appropriate level of security.
- The integrity of information will be maintained.
- It is the responsibility of all individuals who have been granted access to information to handle it appropriately in accordance with its classification.
- Information will be protected against unauthorised access.
- Compliance with the Information Security policy will be enforced

3.2 Governance

Responsibility for the production, maintenance and communication of this top-level policy document and all sub-policy documents lies with Reddan Group PLC's Chief Information Officer. Substantive changes may only be made with the further approval of the CIO. Each of the documents constituting the Information Security Policy will be reviewed annually. It is the responsibility of the Chief Information Officer to ensure that these reviews take place. It is also the responsibility of the Chief Information Officer to ensure that the policy set is and remains internally consistent. Changes or

additions to the Information Security Policy may be proposed by any member of staff to the Chief Information Officer. Any substantive changes made to any of the documents in the set will be communicated to all relevant personnel.