Information Security Policy

We are committed to preserving the confidentiality, integrity, and availability of our information assets:

- For sound decision-making
- To deliver quality services to our customers
- To comply with the law
- To meet the expectations of our customers and
- To protect our reputation as a professional and trustworthy Company

Damage to any information we hold can cause problems for our business, customers and third parties. We have identified information management as one of our key risks and are putting in place measures that help us to manage it. Information security is everyone's responsibility.

We all need to make sure that we know how to use information safely and securely. This policy sets out what we all need to know. Whilst it is an important policy document, it is readable and full of practical help - please read it and ask yourself if you are doing everything you can to protect our reputation.

Definition Of Information Security

Information security means safeguarding information from unauthorised access or modification to ensure its:

- Confidentiality – ensuring that the information is accessible only to those authorised to have access;

- Integrity – safeguarding the accuracy and completeness of information by protecting against unauthorised modification
- Availability – ensuring that authorised users have access to information and associated assets when required

The Company is committed to preserving the confidentiality, integrity, and availability of our information assets:

- For sound decision making
- To deliver quality services
- To comply with the law
- To meet the expectations of our customers
- To protect our customers, staff, partners, and our reputation as a professional and trustworthy organisation

The purpose of our Information Security Policy is to protect the Company's information and that of our partners, to manage information risk and reduce it to an acceptable level, while facilitating reasonable use of information in supporting normal business activity and that of our partners.

This policy applies to all employees, contractors and agents of the Company (i.e. users) who use or have access to Company information, computer equipment or ICT facilities. The policy applies throughout the lifecycle of the information from creation, storage, and use to disposal. It applies to all information including:

- Information stored electronically on databases or applications e.g. email
- Information stored on computers, PDAs, mobile phones, printers, or removable media such as hard disks, CD rom, memory sticks, tapes and other similar media
- Information transmitted on networks
- Information sent by fax or other communications method
- All paper records
- Microfiche, visual and photographic materials including slides and CCTV
- Spoken, including face-to-face, voicemail and recorded conversation

Legal And Regulatory Requirements

Users of the Company's information assets will abide by UK and European legislation relevant to information security including:

- Data Protection Act 1998
- Computer Misuse Act 1990
- Electronic Communications Act 2000
- Copyright, Designs and Patents Act 1988
- Human Rights Act 1998 Regulation of Investigatory Powers Act 2000
- Telecommunications (Lawful Business Practice) Regulations 2000
- Civil Contingencies Act 2004
- Copyright Citation Ltd Version 1.0 35
- Freedom of Information Act 2000 and any specific information protection standards relevant to Company business such as the Payment Card Industry Data Security Standard (PCI DSS)

This list is not exhaustive and may change over time. Employees should seek guidance about the legal constraints of using information in their work and the Company will provide appropriate guidance and training to its staff.

Roles And Responsibilities

The Company's Senior Information Risk Officer (SIRO) has responsibility for managing information risk on behalf of the Management Team, setting strategic direction and ensuring policies and processes are in place for the safe management of information. Directors have responsibility for understanding and addressing information risk within
their service area, assigning ownership to Information Asset Owners and ensuring that within their service area appropriate arrangements are in place to manage information risk, and to provide assurance on the security and use of those assets.

Information Asset Owners undertake information risk assessments, implement appropriate controls, recognise actual or potential security incidents and ensure that policies and procedures are followed.

Action In The Event Of A Policy Breach

All employees, and anyone who delivers services on the Company's behalf e.g. contractors, partners, agents or other third parties with access to the Company's information assets have a responsibility to promptly report any suspected or observed security breach; further details are provided at Security breaches that result from a deliberate or negligent disregard of any security policy requirements may, in the Company's absolute discretion, result in disciplinary
action being taken against that employee. In the event that breaches arise from the deliberate or negligent disregard of the Company's security policy requirements by a user who is not a direct employee of the

Company, the Company shall take such punitive action against that user and/or their employer as the Company in its absolute discretion
deems appropriate.

The Company may, in its absolute discretion refer the matter of any breach of the Company's security policy requirements to the police for investigation and (if appropriate) the instigation of criminal proceedings if in the reasonable opinion of the Company such breach has or is likely to lead to the commissioning of a criminal offence.

Data Protection Policy

The Company is registered under the Data Protection Act 1998 and aims to operate in a professional and responsible manner at all times and to be open and accountable for the data it stores.

Access To Data

Employees have the right to access all their data if it is stored in a "relevant filing system" provided they give notice in writing at least seven days in advance of their wish to do so.

The Company has the right to charge a fee, up to a maximum of £10, for allowing employees to view their files. A further charge may be applicable should they wish to Copyright Citation Ltd Version 1.0 36 copy any information from their records. The amount of the fee and the decision to charge will be at the Company's discretion.

The personal information held by the Company in relation to any particular employee can be diverse and may include, for example, information relating to:

- employment, i.e. home address, bank details, emergency contact numbers, tax information, references, etc.
- attendance
- sickness, including medical certificates, etc.
- disciplinary matters

Note that some of this information is time limited and will be destroyed after a period.

Data Not Available To Scrutiny

Items of data are exempt from disclosure under the act and will not be available for employees to see. These include, for example, the name and address of individuals giving a reference to the Company or the content of a reference given by the Company where that is a confidential reference.