Telecoms Advisor Ltd

Information and Security Policy

Review History			
Name	Role/Position	Date Reviewed	Signature

Approval History			
Name	Role/Position	Date Approved	Signature

1. Introduction

The confidentiality, integrity and availability of information, in all its forms, are critical to the on-going functioning and good governance of Telecoms Advisor Ltd. Failure to adequately secure information increases the risk of financial and reputational losses from which it may be difficult for the Company to recover. This information security policy outlines Telecoms Advisor Ltd's approach to information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of the Company's information systems. Supporting policies, codes of practice, procedures and guidelines provide further details.

Telecoms Advisor Ltd is committed to a robust implementation of Information Security Management. It aims to ensure the appropriate confidentiality, integrity and availability of its data. The principles defined in this policy will be applied to all of the physical and electronic information assets for which Telecoms Advisor Ltd is responsible. Telecoms Advisor Ltd is specifically committed to preserving the confidentiality, integrity and availability of documentation and data supplied by, generated by and held on behalf of third parties pursuant to the carrying out of work agreed by contract.

1.1 Objectives

The objectives of this policy are to:

1. Provide a framework for establishing suitable levels of information security for all Telecoms Advisor Ltd information systems (including but not limited to all computers, mobile devices, networking equipment, software and data) and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems. The resources required to manage such systems will be made available
2. Make certain that staff are aware of and comply with all current and relevant UK and EU legislation.
3. Provide a safe and secure information systems working environment for staff, and any other authorised users.
4. Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data that they handle, including satisfying the information security requirements of third party data providers.
5. Protect Telecoms Advisor Ltd from liability or damage through the misuse of its IT facilities.
6. Maintain confidential information provided by suppliers at a level of security commensurate with its classification, including upholding any legal and contractual requirements around information security.
7. Respond to feedback and update as appropriate, initiating a cycle of continuous improvement.

2 Policy

2.1 Information security principles

The following information security principles provide overarching governance for the security and management of information at Telecoms Advisor Ltd.

1. Information should be classified according to an appropriate level of confidentiality, integrity and availability
2. Staff with particular responsibilities for information must ensure they handle that information in accordance with its classification level; and must abide by any contractual requirements, policies, procedures or systems for meeting those responsibilities.
3. All users covered by the scope of this policy (see Section 1.2. Scope) must handle information appropriately and in accordance with its classification level.
4. Information should be both secure and available to those with a legitimate need for access.
5. Information will be protected against unauthorized access and processing in.
6. Breaches of this policy must be reported (see Sections 2.4. Compliance and 2.5. Incident Handling).
7. Information security provision and the policies that guide it will be regularly reviewed through the use of annual internal audits.

2.3 Information Classification

The following table provides a summary of the information classification levels that have been adopted by Telecoms Advisor Ltd and which underpin the 8 principles of information security defined in this policy.

1. Confidential – DPA - defined Sensitive Personal data

2. Restricted – DPA Defined Personal Data

3. Internal Use – Internal company correspondence

4. Public – Freely available on the web

2.4 Suppliers

All Telecoms Advisor Ltd suppliers and/or contractors will abide by this Policy when accessing or processing assets locally or remotely and when subcontracting to other suppliers.

2.5 Compliance, Policy Awareness and Disciplinary Procedures

Any security breach of Telecoms Advisor Ltd's information systems could lead to the possible loss of confidentiality, integrity and availability of personal or other confidential data stored on these information systems. The loss or breach of confidentiality of personal data is an infringement of the Data Protection Act (1998) and the EU General Data Protection Regulation, contravenes Telecoms Advisor Ltd's Data Protection Policy and may result in criminal or civil action against The company.

All current staff and other authorised users will be informed of the existence of this policy and the availability of supporting policies, codes of practice and guidelines.

Any security breach will be handled in accordance with all relevant Company policies .

2.6 Incident Handling

If a member of staff is aware of an information security incident then they must report it to the Service Desk at support@pcitelecom.co.uk
or by telephone 0330 022 0660.

2.7 Supporting Policies, Codes of Practice, Procedures and Guidelines

Supporting policies have been developed to strengthen and reinforce this policy statement. These, along with associated codes of practice, procedures and guidelines are published together and are available for viewing on the company intranet. All staff and any third parties authorised to access Telecoms Advisor Ltd's network are required to familiarise themselves with these supporting documents and to adhere to them in the working environment.