

**QP 01-02**

**DATA CONTROL**

<b>Contents</b>	<b>Page</b>
1. Introduction	2
2. Responsibility	2
3. Security	2
4. Backup	2

## **1. INTRODUCTION**

This procedure is designed to provide a degree of security for electronic records held by ourselves in order to ensure:

- a) that any sensitive data is at minimum risk of disclosure.
- b) that any loss of data from the office computers can be quickly restored.

## **2. RESPONSIBILITY**

All personnel who have access to computer records of a sensitive nature are fully responsible for their proper use and safeguarding. Note that improper disclosure may be a criminal offence.

The Office Manager is responsible for making backups and storage of disks in the safe.

The Office Manager is responsible for checking disks for viruses prior to use on the office machines.

## **3. SECURITY**

Access to information held on any computer is granted only to personnel who need the access in the normal course of their duties. This access does not automatically confer the right to add, alter, delete or copy any data except as defined within the quality system documentation. Any amendment or copying outside this definition will be performed only with the express permission of the Operations/Business Manager.

No software will be added to or deleted from any computer or its set-up amended in any way without the approval of the Operations/Business Manager.

No disks of any format (including CDs) except those obtained expressly for our use will be used on any office machine unless they have been checked for viruses by the designated member of staff.

## **4. BACKUP**

The current regime incorporates a daily backup onto the server and 10 tape cassettes used on rotation.

Because of the crucial nature of this data, the latest backup disks will be taken off site by the PA to the Managing Director.