Q002 INFORMATION SECURITY POLICY

The purpose of the Policy is to protect Medisort's information assets[1] from all threats, whether internal or external, deliberate or accidental. Medisort's Directors has approved the Information Security Policy

It is the policy of Medisort to ensure that:

- Information will be protected against unauthorised access
- Confidentiality of information will be assured[2]
- Integrity of information will be maintained[3]
- Regulatory and legislative requirements will be met[4]
- Information Security Training will be provided
- All breaches of Information Security, actual or suspected, will be reported and investigated
- Standards will be produced to support the policy. These include virus controls and passwords
- Business requirements for the availability of information and information systems will be met

The Operations Director has direct responsibility for maintaining the policy and providing advice and guidance on its implementation. All Managers are directly responsible for implementing the policy within their business areas, and for adherence by their staff. It is the responsibility of each employee to adhere to the Information Security Policy

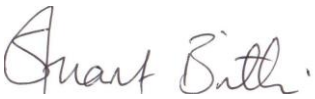
Notes

1. Information takes many forms and includes data stored on computers, transmitted across networks, printed out or written on paper, sent by fax, stored on tapes or diskettes or spoken in conversation or over the telephone.

2. The protection of valuable or sensitive information from unauthorised disclosure or intelligible interruption.

3. Safeguarding the accuracy and completeness of information by protecting against unauthorised modification.

4. This applies to record keeping and most controls will already be in place. It includes the requirements of legislation such as the Data Protection Act.



Stuart Brittle
Managing Director