

## Client Data Security Policy

**Date Approved:** July 25 2011

**Next Review Due:** Annually

### 1 Introduction

Information security is the ongoing process of exercising due care and due diligence to protect information, and information systems, from unauthorised access, use, disclosure, destruction, modification, disruption or distribution. The never-ending process of information security involves ongoing training, assessment, protection, monitoring & detection, incident response & repair, documentation, and review. This makes information security an indispensable part of all the business operations across different domains.

Datastor Technology Ltd (DTL) has an obligation to ensure that appropriate security management arrangements are in place for the protection of client information during the provision of data recovery services in order to meet the statutory requirements set out within the Data Protection Act 1998.

The information systems, equipment, software and data handled by DTL represent a considerable investment and are valuable assets for the client, sometimes essential to their effective and continuing operation.

Much of the data held in these systems is of a confidential nature, and it is necessary for all information systems to be protected against any events, accidental or malicious, which may put at risk the activities the client or its investment in information.

This policy applies to all information systems given into the care of DTL. 'Information systems' include both computer-based systems and non-computer based systems. All staff, contractors, temporary staff and third parties are required to adhere to this policy.

Without effective security, information assets may become unreliable and untrustworthy, may not be accessible where or when needed, or may be compromised by unauthorised third parties.

## 2 Policy Statement

The purpose of this policy is:

- To bring to the attention of all staff the need to improve and maintain security of information systems, and to advise clients of the approach being adopted to achieve the appropriate level of security.
- To ensure that DTL complies with current legislation and EU Directives, meets statutory obligations and observes standards of good practice.
- To minimise the risk of security breach and prosecution
- To define the requirements for connection to the DTL network.

## 3 Policy

DTL is committed to maintaining and developing an information systems infrastructure, which has an appropriate level of security and data protection.

Sharing of information with other organisations is subject to specific agreement between the client and the Director of DTL.

The purpose of information systems security is to ensure an appropriate level of: -

- Confidentiality
- Integrity
- Availability

Information Systems are comprised of three main portions, hardware, software and communications. The purpose of information security industry standards, as mechanisms of protection and prevention, is to apply procedures and policies to tell people (administrators, users and operators) how to use products to ensure information security within the organisations.

Information is obtained, held and disclosed lawfully and data access is confined to those with specified authority to view and/or change the data.

All system assets are operating according to specification and the accuracy of data is maintained.

Systems and data are available when required and the output from it delivered to the user who needs it, when it is needed.

### 3.1 Passwords and Access Control

Access to electronic information systems is controlled on the basis of service requirements, and managed through the use of protocols for allocating and controlling access, secure logins and passwords. Each individual is responsible for keeping their own password secure and must ensure it is neither disclosed to, nor used by, anyone else under any circumstances. Staff must only access systems using their own login and password. All staff are accountable for any activity carried out under their login and password and this is audited. **Failure to comply with these protocols may lead to**

**disciplinary action.**

### **3.2 Management and Staffing Arrangements**

Lead responsibility for information security management rests with the IT Manager and the Director. These individuals, together with all line managers, are responsible for implementing, monitoring, documenting and communicating information security policies throughout DTL

Information security is addressed at recruitment stage for all staff, and all contracts of employment and job descriptions include a confidentiality clause

### **3.3 Training and Awareness**

All staff are aware of their responsibilities for information security at the commencement of employment. Managers will ensure that all staff they are responsible for are aware of, and adhere to this policy.

Training will be provided or commissioned to ensure that staff, whether technical or administrative, are fully aware of their personal responsibilities in respect of information security, and are competent to carry out their designated duties. This should include training for staff in the use and protection of both paper and electronic records systems.

### **3.4 Risk Analysis**

Effective information security management is based upon the core principle of risk assessment and management. In order to make the best use of resources, each Information system should be secured to a level appropriate to the measure of risk associated with it. Measures will be put in place to ensure each system is secured to an appropriate level.

Once identified, information security risks must be managed on a formal basis. Risks will be recorded within the risk register and action plans put in place to demonstrate effective management of the risks.

### **3.5 Network Connection**

All in-laboratory and on-site handling of client data takes place on equipment that is connected neither to the DTL network nor to the internet.

### **3.6 Security of Assets**

Any client information systems that are not being actively worked on during the course of data recovery services are locked in the DTL fire resistant safe.

During the course of the data recovery process, as the first step, a copy of the data is made. This copy is used as the donor source for the recovery and is handled in the same secure way as the original.

When the recovery is complete, the recovered data is saved to data DVD for return to the client, and a copy is held for three months in the recovered data store. This is kept locked in the safe at all times when not in use. The copy that was made as part of the process is securely destroyed in line with the Data Destruction Policy.

### **3.7 Legal Requirements and Regulations**

DTL and all staff are directed by laws & regulations including, but not limited to:

- Data Protection Act 1998.
- Data Protection (Processing of Sensitive Personal Data) Order 2000
- Copyright, Designs and Patents Act 1990.
- Computer Misuse Act 1990.
- ISO/IEC 27001

Only licensed and/or legal software is permitted on DTL equipment. It is expressly forbidden for any user to load or operate software gained from the Internet, magazine, gifts or other sources unless authorised by the Director.

### **3.8 Business Continuity Planning**

DTL has processes in place to develop and maintain appropriate plans for the speedy restoration of all critical IT systems. All systems will have threats and vulnerabilities assessed to determine how critical they are to DTL. Individual work areas have procedures in place to maintain essential services in the event of IT system failure.

### **3.9 Computer “Owners”**

Each PC (including notebooks, laptops, palmtops, and portables) shall have a designated system owner responsible for overall security on the system. PCs shall be specified and purchased in accordance with current recommendations on software and hardware.

Precautions are taken to prevent and detect computer viruses.

If sensitive information is present on the PC, then the advice and agreement from DTL should be obtained before the PC is taken off site or used outside of a secure area.

### **3.10 Personal Use**

Personal use of IT equipment is not permitted on any machine used for client data recovery.