



Head Office
 WALTHAM HOUSE
 RIVERVIEW ROAD
 BEVERLEY
 EAST YORKSHIRE
 HU17 8DY



ADMINISTRATION INSTRUCTION 42

TITLE:	Data Management Policy
AIM:	To outline the principles for Data Management
RELATED POLICIES & PROCEDURES:	Information Management and Technology Assets – IT Equipment & Furnishings
APPROVED BY:	Directors
DATE OF APPROVAL:	April 2010
DATE OF NEXT REVIEW:	April 2011
DISTRIBUTION:	All staff via Intranet

INTRODUCTION

- This document constitutes the Data Management Policy (DMP) for the DEFLOG VQ Trust & TIR Training Services Ltd (referred to herewith as the "Company") IT systems. All personnel using the systems are to comply with this DMP and no departure from or amendments to it are permitted unless prior authorization is obtained from the ICT Department.

ADMINISTRATION AND ORGANISATION OF SECURITY

- Breaches of these orders may render the offender liable to disciplinary action.
- Access to systems is limited to those personnel authorised by the appropriate Director as being approved users, who must have signed the user details sheet as having read and understood this DMP before commencing processing, and must subsequently sight them at least twice annually.

- The term user throughout these orders refers to the Authorised User of the equipment who is cleared to see and process any information on their own equipment.
- The highest protective marking of material which may be held or processed on this System is RESTRICTED.
- Systems are only approved for the processing sessions and protective markings of RESTRICTED material.

PHYSICAL SECURITY

- The system may only be used where the Company have approved locations, including the UK, Germany and Northern Ireland.
- When not in use all workstations must be securely locked by the user.
- Printers must always be checked and cleared of any printed output before the office is left unattended.
- Monitors and printers are to be situated so that no sensitive or confidential data can be overlooked from either outside the area, especially from outside the building, or by persons within the area who are not authorised users. PCs are to be shutdown and switched off when left unattended. The only exception is when the equipment is located in a locked room.

USER SECURITY

- Visitors to Company sites are not allowed to use the system with the exception of maintenance engineers who must be strictly controlled and supervised at all times.
- Each user is responsible for the security of their equipment and any electronic media associated with it or any output produced by the equipment in either paper or electronic form and the protection of any password.

DOCUMENT SECURITY

- • All unwanted printed material is to be disposed of by the use of a shredding machine.

HARDWARE SECURITY

- All equipment is to be checked before use for obvious signs of tampering. Any suspected problems are to be reported to the ICT Department without delay and the equipment is not to be used until checked and cleared.
- All sensitive or confidential material is, where possible, to be removed from the equipment before maintenance engineers are allowed access to the equipment. Engineers must be supervised whilst they are working on the equipment.
- All removable media introduced to the system must be checked for viruses first.
- All hardware failures must be reported to the ICT Manager who will arrange for the necessary maintenance and maintain the records of system failures.
- No equipment (e.g. terminal, PC modem, printer or fax) of whatever description is to be attached to any equipment covered by this DMP without approval of the ICT Manager. No attempt whatsoever should be made to introduce unauthorised equipment to the system.
- All access to network servers is to be strictly controlled via passwords; users must not disclose their passwords to other users. Workstations should not be left unattended without the user logging off or locking the screen so that user's password has to be re-entered to re-gain access. (During the period that the screen is locked no sensitive or confidential data should be visible).

SOFTWARE SECURITY

- All software used on the system is to be from authorized sources and properly licensed. Software may only be installed after the authorization has been given by the ICT Department. Under no circumstances

should users install or attempt to install any software off their own accord. Under no circumstances should users change or attempt to change any of the software or hardware settings on any equipment.

- All users are to be aware of the Computer Misuse Act 1990 and the law covering the unauthorised modification of computer data. Below are details of the offences that can be committed under the act. All offences or suspected offences are to be reported to the ICT Manager immediately.
- Computer Misuse Act 1990

1 Unauthorised access to computer material

(1) A person is guilty of an offence if—

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;

(b) the access he intends to secure is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function that that is the case.

(2) The intent a person has to have to commit an offence under this section need not be directed at—

(a) any particular program or data;

(b) a program or data of any particular kind; or

(c) a program or data held in any particular computer.

(3) A person guilty of an offence under this section shall be liable on summary conviction to imprisonment for a term

not exceeding six months or to a fine not exceeding level 5 on the standard scale or to both.

2 Unauthorised access with intent to commit or facilitate commission of further offences

(1) A person is guilty of an offence under this section if he commits an offence under section 1 above

("the unauthorised access offence") with intent—

(a) to commit an offence to which this section applies; or

(b) to facilitate the commission of such an offence (whether by himself or by any other person);

and the offence he intends to commit or facilitate is referred to below in this section as the further offence.

(2) This section applies to offences—

(a) for which the sentence is fixed by law; or

(b) for which a person of twenty-one years of age or over (not previously convicted) may be sentenced to imprisonment for a term of five years (or, in England and Wales, might be so sentenced but for the restrictions

imposed by section 33 of the [1980 c. 43.] Magistrates' Courts Act 1980).

(3) It is immaterial for the purposes of this section whether the further offence is to be committed on the same occasion as the unauthorised access offence or on any future occasion.

(4) A person may be guilty of an offence under this section even though the facts are such that the commission of the

further offence is impossible.

(5) A person guilty of an offence under this section shall be liable—

(a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the

statutory maximum or to both; and

(b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

3 Unauthorised modification of computer material

(1) A person is guilty of an offence if—

(a) he does any act which causes an unauthorised modification of the contents of any computer; and

(b) at the time when he does the act he has the requisite intent and the requisite knowledge.

(2) For the purposes of subsection (1)(b) above the requisite intent is an intent to cause a modification of the contents

of any computer and by so doing—

(a) to impair the operation of any computer;

(b) to prevent or hinder access to any program or data held in any computer; or

(c) to impair the operation of any such program or the reliability of any such data.

(3) The intent need not be directed at—

(a) any particular computer;

(b) any particular program or data or a program or data of any particular kind; or

(c) any particular modification or a modification of any particular kind.

(4) For the purposes of subsection (1)(b) above the requisite knowledge is knowledge that any modification he intends to cause is unauthorised.

(5) It is immaterial for the purposes of this section whether an unauthorised modification or any intended effect of it of a kind mentioned in subsection (2) above is, or is intended to be, permanent or merely temporary.

(6) For the purposes of the [1971 c. 48.] Criminal Damage Act 1971 a modification of the contents of a computer shall not be regarded as damaging any computer or computer storage medium unless its effect on that computer or computer storage medium impairs its physical condition.

- (7) A person guilty of an offence under this section shall be liable—
- (a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; and
 - (b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

- The system and any new systems will be registered with the Data Protection Act (1984). All users are to be aware of the main provisions of the Data Protection Act and should protect personal data accordingly. Any data held on the system must be used only in connection with official business.
- Back-up copies should be made of any software or data essential to the operation of the system. These should be kept in a different location to the working copies of the software and data files or a fire proof safe. Back-up copies should be made frequently and an annual test should be conducted to verify that the back-up copies are usable. Disks used for backing up data must be checked for malicious software before use. Once backup disks have been made, they are to be stored at a location away from the PC location or a fire proof safe.

ACCOUNTING AND AUDIT

- Information held on the IT systems is to be subject to the same degree of audit as that held by other means. Individual staff are responsible for the confidentiality of any data held on their systems.

LOSSES AND BREACHES

- Any incident involving a breach of personnel, hardware, software, document, or physical security is to be reported immediately to the ICT Manager.

EMERGENCY AND BACKUP PROCEDURES

- Backups. Individual users are responsible for ensuring that backup copies of any data files essential to their work are adequately maintained. Users of Domain network will be able to secure files on a networked drive held on a server. Users without access to the Domain network are to maintain backups of any essential files on removable media (e.g. Encrypted Memory Sticks, Floppy Disk, LS120, Zip, CD\DVD).
- The network servers will have an automated backup system that will perform backups on a daily basis. The backup media will be stored in a fireproof safe in a lockable room. The backups will be held for at least 7 days. The backup will enable the relevant server to be rebuilt to a known state, renewed or replaced, and will have all user data available as at the time of the backup.
- Emergency, Fire and Evacuation. In the event of any other incident requiring the evacuation of the area, the equipment is to be, if possible, secured, but not at the expense of personal safety.

VIRUS PROTECTION

- Anti-virus software must be used when data is input to the system. A Company approved anti-virus software must be used. All media from outside the organization is to be checked for viruses before being used on the system. The anti-virus software must be kept up to date.
- If a virus attack is suspected the following actions must be taken:
 - Contact the ICT Department
 - Do not switch off or re-boot the system until being given permission to do so by IT.
 - Locate and isolate all disks and other i/o media which may have been used on the infected workstation.
 - Identify and isolate any workstation that may have been infected.
 - Identify and warn any users that may have been sent infected files.
 - Recovery of data must not be started until the ICT Department is satisfied that any investigation will not be compromised and gives explicit permission to begin.