Title document

EDP

SECURITY

RC 3 c

RECOMMENDATIONS FOR LOSS PREVENTION IN EDP AND SIMILAR INSTALLATIONS

Part 3: Protection of Data and Software

CONTENTS

In this document, the following data classifications are used:

1. Public
Information intended for distribution outside the organization, either to select groups of individuals or to the public at large.

2. Internal use
Information intended for use primarily within the organization. Unauthorized disclosure, compromise or destruction would not be expected to have a significant impact on the organization, its customers or employees.

3. Confidential
Information intended for within the organization. Unauthorized disclosure, compromise or destruction could have an adverse impact.

4. Restricted
Information intended for use within the organization.
Unauthorized disclosure, compromise or destruction could cause significant damage or penalties to the organization, its customers or employees.

5. Top Secret /Triple X
Information of an extremely confidential nature, such as that used for national security purposes.

INTRODUCTION

Business dependence on the computer has meant an increasing demand on management to ensure that Electronic Data Processing (EDP) installations are, as far as possible, protected against unwanted actions. The physical aspects of protection against fire or intruders have been covered in Parts 1 and 2 of this series.

Part 3 of the series identifies measures to be taken to minimize, with a view to eliminating, unauthorized access to data and the possibilities of data corruption and/or manipulation, the consequences of which may be devastating to that business. It should be used in conjunction with the other parts of the series to ensure a high level of business confidence.

Data should be protected to a degree appropriate to its importance to the organization. Staff vigilance and adherence to data security strategy are vital for achieving proper protection. In order to ensure this, management should appoint persons to be responsible for the maintenance of the strategy. Responsibilities related to other aspects of the strategy also need to be clearly defined.

Consideration should also be given to relevant legislation. The Computer Mis-use Act 1990 describes the constraints on use of computers with regard to data management and use. Personal data should also be protected as required by the Data Protection Act 1984. The Act is concerned with the threat to individuals (data subjects) that may result from a mis-use of computer stored data and is designed to regulate the use of automatically processed information relating to individuals and the provision of services in respect of such information. The Act applies to all data users who control the contents and use of data from within the United Kingdom irrespective of where the processing of their data is carried out.

SCOPE

This document gives guidance on the protection of data and software stored on computers against unauthorized access which can take the form of unauthorized viewing or manipulation for personal or corporate gain, or for malicious reasons.

This document is primarily intended for the protection of confidential and restricted data (classification levels 3 and 4), but can be selectively applied for other classifications, according to the level of risk. Restrictions for level 5 data and software are normally only imposed at a national security level although this document does include some recommendations.

1. Definitions

The definitions given in the "**RECOMMENDATIONS FOR LOSS PREVENTION IN EDP AND SIMILAR INSTALLATIONS - PARTS 1 AND 2**" apply together with the following:

1.1 **Application Software**

High level software such as word processing, spreadsheet and database packages enabling information to be entered, stored, viewed and manipulated on computers.

1.2 **Audit Trail**

A chronological record of system activities sufficient to enable the reconstruction, review and examination of the sequence of activities surrounding or leading to events in the path of an operation from its inception to output of final results. This should not be confused with a simple log.

1.3 **Communication Socket**

A permanently mounted socket enabling communication to a computer or computer network.

1.4 **Data**

Information stored on computer media (eg magnetic tape, disk, computer memory) and for input to computers.

1.5 **Malicious Coding**

Instructions or commands introduced intentionally into the computer system to cause interference or breakdown or for illicit purposes. Such coding includes intentionally introduced viruses, logic and time bombs (where a code is designed to cause interference or breakdown under pre-determined circumstances or at a predetermined time) or trojan horses (where information is retrieved or manipulated by an illicit program disguised as a legitimate one).

1.6 **Operating System**

Software that controls the execution of computer programs and that may provide scheduling, debugging, input/output control, accounting, compilation, storage assignment and data management.

1.7 **Operator**

A person involved in the running and maintaining of a computer installation.

1.8 **Password**

A keyed-in code enabling access to computer data at a specific level.

1.9 **Personal Data**

Computer controlled or stored information concerning a living individual.

1.10 **User**

A person using a computer to input, delete, view, manipulate or extract data.

2. Responsibilities

2.1 Senior management should take overall responsibility for the protection of data and should define the accountability and responsibilities of staff within the organisation. The definition should be in the form of a management authorized document clearly stating total security policy, objectives and commitment. The document should be in accordance with the recommendations of management responsibilities as covered in BS 5750 (eg clause 4.1 of BS 5750 Part 1) and should be available to all appropriate persons.

2.2 Responsibilities should be compatible with all other aspects of EDP fire and security measures, so that there is no conflict of interest with regard to overall security policy.

2.3 Those assuming responsibility in the event of disruption of the computer system or corruption of data as a result of introducing software or data into the computer system (eg via malicious coding or viruses), should be clearly identified.

3. User control

3.1 Access to Terminals

A computer terminal provides potential access to all information in the computer system. Although it may be desirable to limit the capabilities of the equipment to the functions required, eg by providing no local processing capability, no removable disc storage, or no printer facilities, in practice equipment capabilities are usually well in excess of the function for which it is used. Therefore it is necessary to ensure that terminal usage is properly authorized and controlled, using physical and/or software controls as outlined below.

3.2 Physical Access Controls

3.2.1 At each terminal location an individual must be responsible for authorizing access to the terminal. The traditional lock and key approach is still an effective method of securing a terminal from unauthorized access in most situations. In addition there are various physical forms of locking terminals, such as key-switches, which can switch off the power supply to a group of terminals.

3.2.2 Within communal areas, it may be desirable to locate terminals where supervisors can visually monitor usage.

3.2.3 Measures should be taken to avoid illicit viewing of confidential or restricted data. These should include installation of terminals in controlled areas and automatic screen clearing after a specified period of keyboard inactivity.

3.2.4 Communications lines, sockets, patch panels and switches should be physically secured and accessible only by authorized personnel.

3.2.5 Physical inventories of terminals (including personal computers), communication hardware and magnetic media should be carried out at all remote sites to check that only authorized equipment is linked in.

3.3 SOFTWARE ACCESS CONTROLS

3.3.1 Security software should include features which deny access to all or part of the system based on an unauthorized correlation of any of the following.

- User identification (Password)
- Transaction code
- File access function (read, amend, copy, create, delete)
- Database record or item
- Terminal identification
- Circuit identification
- Time of day and date

3.3.2 A unique identification code should be given to each individual authorized to access level 2, 3 4 or 5 data or authorized to change level 1 data. The identification code should be associated with a user profile which defines the transactions the user may enter, the information contained in computer files which the user is permitted to access and the nature of access allowed to those files and to data elements contained within those files. User identification codes and user profiles for new users should be authorized by management, and removed when users leave employment.

3.3.3 A password is a commonly used means allowing computer systems to recognize an authorized user. Passwords should be unique to each individual - group passwords should not be used.

3.3.4 Passwords should be of a complexity commensurate with the sensitivity of the access and should consist of at least 6 characters of an alphanumeric mix, where possible. Additional passwords may be necessary for data classifications 3, 4 and 5 to prevent access to specific directories or files

3.3.5 Proper names, dates, car registration numbers, national insurance numbers, etc should not be used when forming a password. It is recommended that software is included that can identify and eliminate the use of such numbers.

3.3.6 Passwords should be kept secret. In no cases should they be centrally displayed or details left beside terminals. They should not be displayed on terminals at any time, printed in any reports or logged in transaction logs. Personnel should be made aware that any disclosure of their password could result in disciplinary action.

3.3.7 Password data set should be protected from unauthorized read and write access as level 4 data. Encryption may be desirable.

3.3.8 Passwords should be changed as follows:

- at regular intervals, at least monthly, or after a specified number of log-ons
- when the user leaves employment or is transferred
- when the password has been revealed to others
- when user behaviour necessitates a change

Forgotten passwords should not be reissued.

3.3.9 Failed access attempts should be signalled at operator consoles as they occur. Security staff should investigate regular failures and denials.

3.3.10 Access authorization for engineers or outside maintenance persons should be cancelled on completion of their task.

3.3.11 During each log-on session, the user should be advised when last his password was used. This should alert the user of a potential security breach.

3.3.12 For data classification level 4 applications, a combination of appropriate additional security measures may be necessary, eg

user knowledge (eg password, encryption key) and user asset (eg key, token, security card)

Security level 5 data may warrant the addition of direct user identification techniques such as palm or finger prints, voice prints or signature analysis.

3.3.13 All terminals connected to a centralized system should have an appropriate recognition signal to confirm its legitimate connection to the system. Terminals at physically remote sites should be locked out of the network outside normal operating hours, except on specific authorization from management. Networking systems should incorporate facilities for barring communications where such communications are not necessary. Where dial-up networks are in use, additional measures may be necessary to verify the identity of the originating terminal.

3.3.14 It should be ensured that users log-off when leaving a terminal, even for relatively short periods. Where possible, terminals should log off automatically after a predetermined period of keyboard inactivity (eg 5 minutes).

4. Stored data

4.1 Procedures regulating access to stored data should minimize the possibility of unauthorized viewing, use and corruption, eg modifying manufacturer's standard file names.

4.2 All stored data should be deleted as soon as no longer required. There should be a periodic check on the number of files of a certain age (eg 1 year) still stored in the computer, such as on hard disk, to determine if continued storage is necessary. These checks should only be undertaken by persons with the appropriate authority. Redundant magnetic media should be destroyed (eg shredded or burned).

4.3 Data should be encrypted where considered appropriate to the sensitivity of the data and the consequences of disclosure. This is particularly appropriate when transmitting data to remote sites (see clause 5.1).

4.4 BACK-UP FILES

4.4.1 A procedure should be in operation to ensure that back-up copies of files, operating systems and application software are made together with any operating information and programme listings. Copies should be made at a frequency dependent on the value and nature of the data.

4.4.2 All back-up copies should be checked for validity and should be readily identifiable.

4.4.3 Short term off line back-up media, where a high level of availability is required, should be stored in security controlled areas.

4.4.4 Computer media containing long term back up files should be kept in securable and fire resistant cabinets or specially constructed storage rooms. These cabinets or rooms should preferably be located remote from the facility. If facilities for long term storage are shared with other organisations, it should be ensured that sufficient security measures are in place to prevent cross-access to data. Data should only be released to authorized personnel. All movement of data and transportation should be logged. Containers with an appropriate level of fire and security integrity and immunity to corruption, should be used to transport data carrying media.

4.5 PRINTED DATA

4.5.1 Where data is reproduced on paper, or where written data is to be presented for input to a computer, it should be afforded the same security precautions as for stored data. Sensitive printed data, for example, should be stored in security cabinets.

4.5.2 Printed data produced for drafting or information should be destroyed when no longer required. It is recommended that a shredder or similar facility is available. Operators without the appropriate authority to process information of a certain data classification level, should not be given the task of destroying printed data of that level.

4.5.3 Some printers may store data for printing in resident memory. It should be ensured that, for classification level 4 and 5 data, the memory is cleared as soon as the printing process is finished. Used printer ribbons should be disposed of in a controlled manner.

5. Monitoring data use

5.1 There are two main methods for monitoring data use, these are the audit trail (also known as the management trail) and the system log, system journal, or activity log.

5.2 AUDIT TRAIL

5.2.1 An audit trail is the predetermined route by which the processing of data can be traced through the application system. This is used to reconstruct and review the sequence of activities surrounding a transaction from its inception to the output of final results and to break down the final result into its constituent parts.

5.2.2 The audit trail should be an integral part of the information processing application. It should ensure that the records required to trace data backwards and forwards through the application are generated, identified and stored securely for an appropriate retention period.

5.2.3 Audit trail information should be stored as classification level 4 data.

5.2.4 Where high classification level data is being processed, it may be desirable to incorporate an on-line real time audit facility to notify system administrators of an imminent breach of security.

5.3 SYSTEM LOG

5.3.1 A system log is an automatic logging programme controlled by the operating system of a computer and designed to record its activities. Essentially the system log provides sufficient information to identify each job run on the computer together with a detailed breakdown of processing time and peripherals used. It will also identify the use of data files.

5.3.2 As a minimum, the creation, amendment and deletion of records and files should be logged with details of the user identification, time, date and source (eg terminal). This information should be stored securely for an appropriate retention period as classification level 4 data.

5.3.3 The System Log should be checked on a regular basis, preferably using a selective report of the logged parameters. Any unusual activity should be investigated. Circumstances demanding attention include:

- rejected access attempts
- unauthorized access to password details
- working excessive overtime or unusual hours
- repeated transactions of the same type made by one individual (which may indicate attempts to find a particular record by browsing).

5.4 Other methods to identify possible unauthorized access to data should be used where available and where considered by management to be appropriate. One method is by the use of file "fingerprinting" techniques. This is where files are marked with an identification of the user(s), if and when file access has been established.

6 Protection against remote interception

6.1 TRANSMISSION LINES

6.1.1 There is a possibility that data transmitted from one operating terminal to another will be intercepted, whether within the same building or to a remote site.

6.1.2 All transmitted data should be coded depending on its data classification, as given below

Data Classification	Method
1. Public	No coding necessary
2. Internal use	Simple non-sequential or coded transmission, eg transmission of data in a pseudo-random manner, using data packets transmitted in reverse order, multiplexing with other data, etc.
3. Confidential	Data scrambling or encryption*.
4. Restricted	Encryption* with high security algorithms. (eg, for synchronous transmission, any successive data pattern of more than 100 bits, should not be repeated within 1,000,000 successive bits).

** In accordance with appropriate encryption standard algorithms (for example, algorithms agreed by the American National Standards Institute (ANSI)).*

6.1.3 Where access is required over public telephone lines, then measures may be necessary to protect against external unauthorized users (eg, hackers). As well as the coding of data, identification and verification procedures for all communicating terminals should be incorporated. Open lines should not be used. Terminals should use ex-directory numbers. Diversions, changes or insertions to transmitted data should not be made unless the appropriate authority is given.

6.1.4 Every effort should be made to avoid the possibility of substitution or blocking of data during its transmission. The methods described above may be sufficient in some cases. However, there may be a need for more complex terminal remote end identification arrangements. Such methods could include the use of digital signatures, handshake arrangements, etc, to confirm the safe transmission and reception of data.

6.1.5 For level 4 classified data, transmission lines under the control of the organisation should incorporate tamper detection methods. Alternatively, routing data signals by fibre optic cable can prevent many cases of intercepting and analysing data.

6.2 EMANATION INTERCEPTION

(For consideration where high security level data is processed, such as that classified at level 5.)

6.2.1 Although not considered to be a common problem, it is possible to intercept data remotely by means other than connecting with communication lines. Such methods include the monitoring of radiated emanations. These may be in the form of acoustic or electromagnetic signals. Acoustic emanations can be suppressed by using sound screening.

6.2.2 Unprotected computer equipment such as VDUs can radiate readily detectable electromagnetic fields. Intelligible information can be derived from these fields. In view of this, measures should be taken to prevent this form of data access such as:

(a) *Electrical screening of the EDP facility (Note: Clause 7.4 of Part 2 of this series "Security Protection" also recommends screening, although this is for the purpose of protecting against outside electromagnetic fields).*

(b) *Filtering of secondary cabling that could carry induced electromagnetic information. The use of fibre-optic cables effectively eliminates this risk.*

(c) *Earthing of all metal conduit, etc that could possibly carry induced information derived from the electromagnetic fields.*

6.2.3 If it is deemed impractical to incorporate the above recommendations, then consideration should be given to the adoption of a "needle in a haystack" philosophy by processing sensitive data in short time spans between other data.

7 Use of software

7.1 All software should be approved for use by senior management before acquisition. This should include screening of any public domain/bulletin billboards brought up, for example, after log on. Computer games should be banned from use.

7.2 Acquisition procedures should ensure that the software used is reliable and from a reputable source. Acquired software should be fully checked on a stand alone machine with virus checking facilities before live use. Such checks should also, where possible, evaluate the software for the possibility of it containing malicious coding.

7.3 Software development, update and modification should follow a recognized, structured procedure in order to ensure that the software meets the requirements and contains no illicit code. Testing should not be carried out on live data and should preferably be carried out by personnel independent of those who developed the software. Acceptance for live use should be controlled by appropriate management procedures.

7.4 Wherever possible, and especially for applications involving sensitive data, users should not be involved in software development or testing except in defining requirements.

7.5 Authentication and virus checking procedures should be used to minimize the threat of external contamination of the software or data held in the computer system. It is recommended that such programs are automatically called up when software or data is introduced to the system by, for example, floppy disks. It should be noted that some forms of malicious coding may not be readily detectable. In view of this, users should be made aware of the possibilities of malicious coding. Contingency plans should be prepared to minimize loss and disruption in the event of contamination.

7.6 Software used for data security should have an appropriate level of sophistication to enable a unique security system to be operated, so that persons with knowledge of the software package will not be able to breach the security arrangements.

8. Personnel procedures

8.1 STAFF SELECTION

Staff to be employed for tasks involving processing of data, should be carefully selected. The selection procedure should be commensurate with the security level of data that would be processed (ie the vetting of general users need not be as thorough as for persons employed to process confidential data). Senior management, such as personnel managers should be directly involved in staff selection, temporary or permanent, to ensure consistency of staff selection procedures.

8.2 TRAINING

8.2.1 As well as general training in the use of computer hardware and software, staff should be trained in the security of data. Such training should include:

- knowledge of the security policy
- an understanding of the data classification level(s) the employee has responsibility for.
- an understanding of the procedures regarding breaches in security.
- details of the precise duties required.

8.2.2 After staff have undergone training, procedures should be included to monitor post training activity.

8.2.3 A register of those in sensitive roles should be kept, together with procedures to prevent them having the capacity to cause significant damage, and recovery procedures in the event that these fail.

8.2.4 It should be ensured that there are sufficient persons with the appropriate level of knowledge such that operations and security are not compromised if one key person becomes unavailable. Rotation of duties is a useful method of revealing illicit data manipulation.

8.3 TERMINATION

When staff leave, it is important that data security arrangements are updated so that the staff members' knowledge on access to data is redundant. Leaving staff should be fully debriefed with regard to the security arrangements and made aware of the consequences of attempting to breach such arrangements. Procedures should be in place to ensure that computer managers are informed of staff selections and terminations before the event.

9. Inspection

9.1 A full inspection should be carried out of the data security measures when they are first implemented. This inspection should examine the capabilities of each of the methods of data security to check whether they are fully functional and fit for purpose.

9.2 The initial inspection may require the acting out of test scenarios to check the effectiveness of the systems. Such scenarios would attempt to breach any or all of the data security measures adopted.

9.3 In addition, a procedure of regular follow up inspections should be implemented to check the continued effectiveness of the systems. Systems operation inspections should review procedural controls to ensure that these are working as anticipated, are adequate and that audit trails exist. Systems and development inspections should ensure that development is adequately controlled, systems are properly designed and auditable with adequate controls, and that systems are properly tested and documented before use.

9.4 It is important that any corrective actions required as a result of inspections are quickly implemented since failure to do so may jeopardize future security arrangements, and result in loss of business confidence.

9.5 A fully planned catastrophe response procedure should be in place to allow rapid response in the pre-planned and correct manner.

BIBLIOGRAPHY

Loss Prevention Council, "Recommendations for loss prevention in EDP and similar installations":

Part 1: Fire Prevention

Part 2: Security Protection.

British Standard BS 5750: Quality Systems

Part 1: 1987: Specification for design development, production, installation and servicing

The Data Protection Act 1984

The Computer Mis-Use Act 1990

Published by the Loss Prevention Council, 140 Aldersgate Street, London EC1A 4HY

Printed in Great Britain by Chelmer Printing & Stationery Company Limited 392/5