Document Title:	Security Management Procedures
Document Type:	Procedures
Abstract:	This document defines the new Information Security Management Procedures for use within ICL Pathway. They are based upon the (1999 revised) BS7799 "Code of Practice for Information Security Management".
Document Status:	Draft (Latest Approved is Version 1.0)
Distribution:	Horizon Library (FAO Bob Booth) ICL Pathway Library ICL Outsourcing (OSD) ICL Outsourcing (SMG)
Author/Editor:	Peter J Harrison
Comments To:	Author, copy to Martyn Bennett / Graham Hooper
Comments By:	-

SECURITY MANAGEMENT PROCEDURES

Foreword

These ICL Pathway Security Management Procedures are intended for use, as a reference document, by managers and employees responsible for initiating, implementing and maintaining information security within ICL Pathway.

These procedures are based upon British Standard BS7799, “A code of Practice for Information Security Management.” Whilst most of the controls described in BS7799 are relevant to ICL Pathway, it is necessary to take account of local environmental and technological constraints when applying generic controls. Consequently, this code of practice has been augmented by further guidance and set in the context of ICL Pathway’s organisation.

Contents

Annexes

SECTION 0. GENERAL

0.1 Document History

Version	Date	Reason
0.1	27/4/98	Initial Draft
0.2	28/9/98	Draft for internal review
0.3	15/12/98	Incorporates minor changes and corrections.
1.0	7/5/99	Approved
1.1	22/6/99	Removal of references to DSS/Benefits Agency relating to Contract changes.
1.2	17/9/99	Aligned with revised (1999) version of BS7799.

0.2 Approval Authorities

Name	**Position**	**Signature**	**Date**
John Bennett	Managing Director		
Tony Oppenheim	Director Commercial & Finance		
Terry Austin	Director Development		
Martyn Bennett	Quality & Risk Director		
John Dicks	Customer Requirements Director		

0.3 References

ICL Pathway documents:

[SECPOL]	RS/POL/002	ICL Pathway Security Policy
[AUDPOL]	RS/POL/005	ICL Pathway Audit Policy
[ACCPOL]	RS/POL/003	ICL Pathway Access Control Policy
[SFS]	RS/FSP/001	ICL Pathway Security Functional Specification
[TED]	TD/ARC/001	ICL Pathway Technical Environment Description
[CLASS]	*TBD*	ICL Pathway Security Classification Standards

Relevant legislation:

[1] Data Protection Act (1984)
[2] Computer Misuse Act (1990)
[3] Copyright, Designs and Patents Act (1988)
[4] Police and Criminal Evidence Act (PACE)
[5] Post Office and Telegraph Acts
[6] Official Secrets Act (1989)
[7] Companies Act (1985)

0.4 *Document Structure*

These Security Management Procedures are divided into ten main sections, corresponding to the main section of the BS7799 Code of Practice, as follows.

Section 1:	Security Policy.
Section 2:	Security Organisation.
Section 3:	Assets Classification and Control.
Section 4:	Personnel Security.
Section 5:	Physical and Environmental Security.
Section 6:	Communications and Operations Management.
Section 7:	Access Control.
Section 8:	System Development and Maintenance.
Section 9:	Business Continuity Management.
Section 10:	Compliance.

Within each section, the subsection headings are a close match to BS7799.

0.5 *British Standard 7799*

BS7799 gives recommendations for information security management. It is intended to provide a common basis for organisations to develop, implement and measure effective security management practice and to provide confidence in inter-organisational dealings.

0.6 *BS7799's Key Controls*

The original (1995) BS7799 identified ten "Key controls" that were viewed as either essential requirements (e.g. legislative requirements) or considered to be fundamental building blocks for information security (e.g. security education).

The key symbol (🔑) is no longer used, but BS7799 (1999) still highlights five of the controls as "common best practice", applying to most organisations and environments, as follows:

- information security policy document (section 1.1.1),
- allocation of information security responsibilities (section 2.1.3),
- information security education and training (section 4.2.1),
- reporting of security incidents (section 4.3.1), and
- business continuity management (section 9.1.1).

Controls considered to be essential to an organisation, from a legislative point of view, are:

- intellectual property rights (section 10.1.2),
- safeguarding of organisational records (section10.1.3), and
- data protection and privacy of personal information (section 10.1.4).

Whilst these controls also apply to ICL Pathway, they are not regarded as having any extra significance within these Security Procedures.

1. SECURITY POLICY

1.1 Information Security Policy

Objective:	To provide management direction and support for information security.

Top management shall set a clear direction and demonstrate their support for, and commitment to, information security through the issue of an information security policy across the organisation.

1.1.1 Information Security Policy Document

A written policy document shall be available to all employees responsible for information security policy across the organisation.

ICL Pathway's commitment to security is communicated throughout ICL Pathway, as evidenced by board level approval of ICL Pathway's Security Policy [SECPOL].The policy document, which should be available to all employees responsible for information security, includes the following guidance:

a) a definition of ICL Pathway's business, information security and legal objectives,

b) a definition of responsibilities for all aspects of information security,

c) a statement of management intention, supporting the goals and principles of information security,

d) an explanation of specific security policies, principles, standards and compliance requirements, including:

- compliance with legislative and contractual requirements,
- security education requirements,
- virus prevention and detection policy, and
- business continuity planning policy,

e) an explanation of the process for reporting suspected security incidents.

Responsibilities for maintaining the policy and the frequency of policy review are defined within the security policy document.

1.1.2 Review and Evaluation

The "owner" of ICL Pathway's Security Policy shall be responsible for ensuring that the policy is reviewed and maintained.

ICL Pathway's Security Policy is "owned" by the Director, Quality and Risk Management (see section 2.1) who would normally delegate documentation of the policy to the IT Security Manager (see section 2.1.3). The review period (typically every 12 months) is specified within the Security Policy.

2. SECURITY ORGANISATION

2.1 Information security infrastructure

Objective: To manage information security within ICL Pathway.

A management framework shall be established to initiate and control the implementation of information security within ICL Pathway.

The ICL Pathway management framework is defined within the ICL Pathway Security Policy ICL Pathway's Managing Director has ultimate responsibility for security. The responsibilities of the Director, Quality and Risk Management, include:

- overall control of security throughout ICL Pathway,
- provision of adequate resources for security,
- being Chairman of the ICL Pathway Security Board (see section 2.1.1),
- owner of ICL Pathway's Security Policy,
- approval authority for ICL Pathway's Security Policy,
- approval authority for ICL Pathway's Security Standards,
- overall control of risk management functions,
- establishing the security interface with POCL, and
- establishing the security interface with all subcontractors.

2.1.1 ICL Pathway Security Board

Management direction shall be provided through a suitable high level steering forum.

The ICL Pathway Security Board should provide management direction on Information Security.

The representatives on ICL Pathway's Security Board are nominated by the Director, Quality and Risk Management, and approved by the ICL Pathway Board. The Security Board participants, which will include the Horizon Security Liaison staff, represent a broad range of interests to ensure that alternative perspectives are considered.

Whenever necessary, the Security Board can commission independent specialists to undertake studies, investigations or audits.

Security Board responsibilities include:

- ownership of ICL Pathway's Security Strategy,
- determining the adequacy of ICL Pathway's Security Policy definition,
- formal review of all Security Policy documents,
- review of security incidents, on a regular basis, and
- liaison with external bodies and specialists.

2.1.2 Information Security Co-ordination

Information security measures shall, where appropriate, be co-ordinated through a cross-functional forum.

Within ICL Pathway the nominated representatives on the ICL Security Board (identified in section 2.1.1) provide cross-functional input, representing the views of ICL Pathway's organisation.

2.1.3 Allocation of Information Security Responsibilities

Responsibilities for the protection of individual assets and for carrying out specific security processes shall be clearly defined.

ICL Pathway's Security Policy [SECPOL] defines the security roles and responsibilities within the organisation. The board level responsibilities are summarized above, in section 2.1.The Security Manager is responsible for ensuring implementation of policy and standards, and maintaining "best practice", within the remit of ICL Pathway.

ICL Pathway's Security Manager's responsibilities include:

- physical and environmental security,
- monitoring compliance with ICL Pathway's Security Policy,
- providing the point of contact for reporting all types of security incidents,
- recording and investigating security incidents,
- ensuring that security relevant events are audited by the system,
- ensuring that audit trails are analysed on a regular basis,
- documentation of ICL Pathway's Security Policy,
- being the owner of ICL Pathway's Security Standards,
- documenting ICL Pathway's Security Standards,
- communicating security policy and standards throughout ICL Pathway,
- authorising and approving for system changes,
- coordinating the evaluation of all new security products proposed,
- specifying and arranging security education and training,
- devising and conducting security awareness programmes,
- liaising with POCL and suppliers' security personnel, and
- recruiting selection of security administration personnel.

The description "Security Administration" is used to describe ICL Pathway personnel assigned to roles with particular responsibility for security. ICL Pathway's Security Manager is the normal line manager for this group, hence many of the activities assigned to Security Administrators will be to support the functions listed above. Wherever possible, Security Administrators act in a supporting or monitoring role rather than as a Service Provider for the operational service. In this capacity they can:

- monitor compliance with ICL Pathway's Security Policy,
- implement ICL Pathway's Security Standards,
- conduct independent reviews of compliance to policy and standards,
- report security incidents, and
- recommend changes, to enhance ICL Pathway's security controls, to the Security Manager.

2.1.4 Authorisation Process for Information Processing Facilities

Installation of information processing facilities shall be technically approved and authorised.

A management approval process for new information processing facilities should be established to ensure that the installation of equipment is for a defined business purpose, will provide an adequate level of security protection, and will not adversely affect the security of the existing infrastructure.

Two levels of authorisation should be used, as follows.

a) **Business approval**. Each installation should have appropriate user management approval, authorising its purpose and use. Approval should also be obtained from the manager responsible for maintaining the local IT security environment, to ensure that it conforms to all relevant security policies and requirements.

b) **Technical approval**. Where necessary, it should be checked that all devices connected to communication networks or maintained by a particular service provider are of an approved device type.

2.1.5 Specialist Information Security Advice

Specialist advice on information security shall be sought whenever appropriate.

Experienced in-house information security advisers should, ideally, provide specialist security advice on all aspects of information security. The quality of their assessment of security threats and advice on countermeasures will determine the effectiveness of the organisation's information security programme. For maximum effectiveness and impact, they should be allowed direct access to IT and business managers throughout the organisation.

Although most internal security investigations will normally be carried out under business line management control, the information security adviser(s) may be called on to provide advice, lead or conduct the investigation.

2.1.6 Cooperation Between Organisations

Security specialists and organisations shall co-operate to combat general security threats.

Internal information security advisers should be encouraged to liaise with external security specialists (in industry or government) at their discretion. Such cooperation provides an opportunity to share experience and assessments of security threats and promote the development of consistent security practices across industry, helping to remove obstacles to inter-organisational dealings.

It is also important to maintain appropriate contacts with law enforcement authorities, IT service providers and telecommunications authorities, to ensure that appropriate contacts can be quickly established and advice obtained, in the event of a security incident.

Exchanges of security information should be restricted to ensure that confidential company information is not passed to unauthorised persons.

2.1.7 Independent Review of Information Security

Implementation of information security shall be independently reviewed.

The security policy document (see section 1.1.1) sets out responsibilities and policy for information security. The actual practice of information security should be reviewed independently to provide assurance that organisational practices properly reflect the policy, and that it is feasible and effective.

2.2 Security of Third Party Access

Objective:	To maintain the security of organisational information processing facilities and information assets accessed by third parties.

Access to company information processing facilities by (non-organisational) third parties shall be controlled.

Control of access to ICL Pathway's systems and data should be in accordance with ICL Pathway's Access Control Policy [ACCPOL], which is based upon analysis of security and business requirements.

2.2.1 Identification of Risks From Third Party Access

The risks associated with access to organisational information processing facilities by third parties shall be assessed and appropriate security controls implemented.

The ICL Pathway Security Functional Specification [SFS] defines the security functionality incorporated into the operational ICL Pathway system. It is based upon an analysis of risks to the ICL Pathway solution, including risks associated with access by third parties.

2.2.2 Security Requirements In Third Party Contracts

Contracts with third parties involving access to organisational information processing facilities shall specify security requirements.

Arrangements involving third party access to ICL Pathway's systems should be based on a formal contract containing, or referring to, all of the necessary security conditions to ensure compliance with the ICL Pathway's Security Policy and standards. The contract should be in place before access to the information processing facilities is provided. The following items should be considered for inclusion in the contract:

a) the general policy on information security,
b) permitted access methods, and the control and use of unique identifiers (User Ids) and passwords,
c) a description of each information processing service to be made available,
d) a requirement to maintain a list of individuals authorised to use the service,
e) times and dates when the service is to be available,
f) the respective liabilities of the parties to the agreement,
g) procedures regarding protection of organisational assets, including information,
h) responsibilities with respect to legal matters, e.g. data protection legislation,
i) the right to monitor, and revoke, user activity,
j) responsibilities regarding hardware and software installation and maintenance,
k) the right to audit contractual responsibilities,
l) restrictions on copying and disclosing information,

m) measures to ensure the return or destruction of information and assets at the end of the contract,

n) any required physical protection measures,

o) mechanisms to ensure that security measures are followed,

p) user training in methods, procedures and security,

q) measures to ensure protection against the spread of computer viruses (see section 6.3),

r) an authorisation process for user access,

s) arrangements for reporting and investigating security incidents,

t) involvement, by the third party, of subcontractors and other participants.

2.3 Outsourcing

Objective:	To maintain the security of information when the responsibility for information processing has been outsourced to another organisation.

Outsourcing arrangements shall address the risks, security controls and procedures for information systems, networks and/or desktop environments in the contract with third parties.

2.1.1 Security Requirements in Outsourcing Contracts

In addition to the security considerations for Third Party contracts (listed in section 2.2.2), Outsourcing Contracts should consider:

a) how legal requirements (e.g. data protection legislation) are to be met,

b) arrangements to ensure that all parties are aware of their security responsibilities,

c) maintenance of integrity and confidentiality of business assets,

d) how physical and logical access to sensitive business information is to be controlled,

e) how availability of services is to be maintained in the event of unplanned circumstances (e.g. disaster situations),

f) levels of physical security to be applied, and

g) auditor’s rights.

3. ASSETS CLASSIFICATION AND CONTROL

3.1 Accountability for Assets

Objective:	To ensure that IT assets are given protection in proportion to their value and the impact on the business of their loss or disclosure.

All major information assets shall be accounted for and have a nominated owner.

Owners should be identified for major assets and assigned responsibility for the maintenance of appropriate security measures. Responsibility for implementing security measures may be delegated, though accountability should remain with the nominated owner of the asset.

3.1.1 Inventory of Assets

Inventories shall be maintained of all significant information and IT assets.

Managers must ensure that up-to-date inventories are maintained including details of all significant component assets. Each significant asset must be clearly identified with its value, security classification (see section 3.2) custodian and location recorded.

Significant assets include:

a) **information assets**: databases and data files, system documentation, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements,

b) **software assets**: application software, system software, development tools and utilities,

c) **hardware assets**: computer and communications equipment, magnetic media (tapes and disks), other technical equipment (power supplies, air-conditioning units), furniture, accommodation, and

d) **services**: computing and communications services, other technical services (heating, lighting, power, air-conditioning) upon which the system is dependent.

3.2 Information Classification

Objective:	To ensure that information assets receive an appropriate level of protection.

Security classifications shall be used to indicate the need and priorities for security protection.

ICL Pathway should use the security classification system, described in [CLASS].

3.2.1 Classification Guidelines

Protection for classified information shall be consistent with business needs.

System Managers must ensure that their system information is protectively marked in line with Government rules (see Annex A) and that this is recorded and periodically reviewed.

Security classifications and associated protective measures for ICL Pathway's business information should take account of business needs for sharing or restricting information, and the business impacts associated with unauthorised access or damage to the information.

The responsibility for defining the classification of an item of information (e.g. a document, data record, data file or diskette) and for periodically reviewing the classification, should rest with the originator or nominated owner of the data.

3.1.2 Protective Marking

Printed output and removable media from systems handling classified data should carry an appropriate Protective Marking.

Output from information processing systems containing classified information, must carry the Protective Marking for the most sensitive information contained (in the output).

Items to be labelled include printed reports, magnetic media (tapes, disks, cassettes), electronic messages and file transfers.

Screen displays containing classified information need not be labelled.

Protectively Marked items must be handled and disposed of in line with Government instructions. In particular, such data held on redundant storage media or computers must be overwritten before disposal (see sections 5.2.6 and 1.1.1).

In addition to Government rules, the business needs for sharing or restricting information, and the business impacts associated with unauthorised access or damage to the information, must also be taken into account. In particular, consideration should be given to the following business needs:

a) **confidentiality**: the business need to share or restrict access to information with regard to confidentiality and the controls required to restrict access to the information,

b) **integrity**: the business need to control modifications to information and the controls required to protect the accuracy and completeness of the information, and

c) **availability**: the business need to have information available when required by the business and the controls required to achieve this.

4. PERSONNEL SECURITY

4.1 Security in Job Definition and Resourcing

Objective: To reduce the risks of human error, theft, fraud or misuse of facilities.

Security shall be addressed at the recruitment stage, included in job descriptions and contracts, and monitored during an individual's employment.

Managers should ensure that job descriptions address all relevant security responsibilities. Potential recruits should be adequately screened (see section 4.1.2), especially for sensitive jobs. All employees and third party users of information processing facilities should sign a confidentiality (non-disclosure) undertaking.

4.1.1 Including Security In Job Responsibilities

Job descriptions shall define IT security responsibilities where appropriate.

Line Managers should record specific security responsibilities in the Job Descriptions of their staff where appropriate.

These should include any general responsibilities for implementing or maintaining security policy, as well as any specific responsibilities for the protection of particular assets, or for the execution of particular security processes or activities.

All non-ICL Pathway personnel with access to ICL Pathway systems must have their obligations in relation to those systems recorded in Job Descriptions or contracts.

4.1.2 Personnel Screening

Applications for employment shall be screened if the job involves access to IT facilities handling sensitive information.

The following checks should be made on all such applications:

a) at least two satisfactory character references, one business and one personal,

b) a check (for completeness and accuracy) of the applicant's curriculum vitae,

c) confirmation of academic and professional qualifications,

d) an identification check, e.g. passport, and

e) a credit check for employment in particularly sensitive jobs, e.g. control of finance.

4.1.3 Confidentiality Agreements

Users of organisational information processing facilities shall sign a confidentiality undertaking.

Users of ICL Pathway information processing facilities should sign an appropriate confidentiality (non-disclosure) undertaking as part of their initial conditions of employment.

Agency staff and third party users not already covered by an existing contract (containing the confidentiality undertaking) should be required to sign a confidentiality agreement prior to connection to ICL Pathway information processing facilities.

Confidentiality agreements should be reviewed when there are changes to terms of employment or contract, particularly when employees are due to leave the organisation, or contracts due to end.

4.1.4 Terms and Conditions of Employment

Terms and conditions of employment should state the employee's responsibility for information security. The action to be taken if the employee disregards security requirements should also be stated.

4.2 User Training

Objective:	To ensure that users are aware of information security threats and concerns, and are equipped to support the ICL Pathway security policy in the course of their normal work.

Users shall be trained in security procedures and the correct use of information processing facilities.

Users should also be formally authorised in writing of the scope of their access (rights and restrictions).

4.2.1 Information Security Education And Training

Users shall be given adequate security education and technical training.

System Managers must ensure that users of their system are given adequate security education and training.

Users should receive appropriate training in ICL Pathway policies and procedures, including security requirements and other business controls, as well as training in the correct use of information processing facilities (e.g. logon procedure, use of software packages) before access to information processing services is granted.

This applies to employees of ICL Pathway and to third party users.

4.3 Responding to Security Incidents and Malfunctions

Objective:	To detect information security incidents at the earliest opportunity, in order to minimize the damage, correct the consequences and prevent reoccurrence.

Incidents affecting security shall be reported through management channels as quickly as possible.

All employees and contractors should be made aware of the procedure for reporting the different types of incident (security breach, threat, weakness or malfunction) that might have an impact on the security of ICL Pathway assets.

They should report any observed or suspected incidents as quickly as possible to the correct focal point.

4.3.1 Reporting Security Incidents

All security incidents shall be reported through management channels ,as quickly as possible, in accordance with formal procedures. For most users the ICL Pathway Help Desk will act as the incident reporting centre with the calls being routed to the ICL Pathway Security Manager for action.

A security incident is defined as any suspected or actual undermining, circumvention or failure of the normal confidentiality, integrity or availability of a computer system or any part of the ICL Pathway infrastructure.

Information security incidents include:

- suspected virus infection (see section 6.3.2),
- system failures and any loss or degradation of service,
- errors resulting from incomplete or inaccurate data,
- failures to follow correct operating procedures that undermine security arrangements,
- accidental or deliberate disclosure of protectively marked data to unauthorised persons or systems,
- improper addition, modification, removal or destruction of data software or hardware, and
- other misuse of the system by ICL Pathway or any other personnel.

Incident reports must be treated as RESTRICTED documents.

Documents relating to security incidents must be retained for at least 6 years following the incident report. After this period, the ICL Pathway Security Manager will determine whether the information needs to retained for a further period or securely disposed.

4.3.2 Reporting Security Weaknesses

Suspected security weaknesses shall be reported.

Users of information processing services should report any observed or suspected security weaknesses in, or threats to, systems or services. Reports should be directed to the ICL Pathway Help Desk or, if necessary, directly to the ICL Pathway Security Manager or a Security Administrator.

Users should not, in any circumstances, attempt to prove a suspected weakness.

4.3.3 Reporting of Software Malfunctions

Software malfunctions and other system faults shall be reported.

Users of information processing services should note and report any software that does not appear to be functioning correctly, or other system problems, to the ICL Pathway Help Desk.

The ICL Pathway Help Desk shall record the reported faults and, where appropriate, report them to the ICL Pathway Security Manager.

Users must not, under any circumstances, attempt to investigate or correct the fault. Appropriately trained and experienced staff should carry out recovery procedures.

4.3.4 Learning from Incidents

The types, volumes and costs of security incidents and malfunctions should be recorded, quantified and monitored, so that reoccurrence of high impact incidents can be prevented.

Enhanced or additional controls may be required to limit the frequency, damage and cost of future occurrences. Changes to the ICL Pathway Security Policy may also be necessary.

4.1.5 Disciplinary Process

Breaches of security, which may involve negligent or deliberate misuse by ICL Pathway personnel, shall be investigated in accordance with normal investigation and disciplinary procedures.

A formal disciplinary process will be invoked for employees who have violated ICL Pathway security policies and procedures. The disciplinary process shall be defined by the human resources function and approved by the ICL Pathway management team.

Disciplinary measures act as a deterrent to employees who might be inclined to disregard ICL Pathway's security procedures. Additionally, they should ensure correct, fair treatment for employees who are suspected of committing serious or persistent breaches of security.

5. PHYSICAL AND ENVIRONMENTAL SECURITY

5.1 Secure Areas

Objective:	To prevent unauthorised access, damage and interference to business premises and information.

Information processing facilities supporting critical or sensitive business activities shall be housed in secure areas.

Such facilities must also be physically protected from unauthorised access, damage and interference. They should be sited in secure areas, protected by a defined security perimeter, with appropriate entry controls and security barriers.

5.1.1 Physical Security Perimeter

Physical security protection shall be based on defined perimeters.

The physical protection measures used must be based upon risk assessment. This will depend upon the value of the assets and services to be protected, as well as the associated security risks.

Physical security protection shall be based on defined perimeters corresponding to the boundaries associated with the risk analysis. Each level of physical protection should have a defined security perimeter, around which a consistent level of security protection is maintained.

ICL Pathway Security Manager is responsible for ensuring that risk assessment is carried out in all areas for which ICL Pathway has responsibility.

The security measures used shall ensure that:

a) the security of the perimeter is consistent with the value of the assets (including services) under protection,

b) the security perimeter is clearly defined,

c) physical barriers are, wherever necessary, provided from floor to ceiling (extending into suspended ceiling/floor space whenever possible) to prevent unauthorised entry and environmental contamination,

d) other personnel are not to be made aware unnecessarily of the activities within a secure area,

e) prohibition of unsupervised lone working is considered, both for safety and to prevent opportunities for malicious activities,

f) ICL Pathway-managed computer equipment is housed in dedicated areas separate from third-party-managed computer equipment,

g) when vacated, secure areas are physically locked and periodically checked,

h) personnel supplying or maintaining support services are granted access to secure areas only when required and authorised, and

i) photography, recording or video equipment is not allowed, unless authorised, within the security perimeters.

5.1.2 Physical Entry Controls

Secure areas shall be protected by appropriate entry controls.

Secure areas shall be used to enclose IT assets that support business-critical and information assets with a high value. These areas must be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.

Wherever possible, low value assets that need to be used regularly (including printers and photocopiers) should not be located in secure areas. This will reduce the number of people who need to enter the area.

Protectively marked or business-critical systems that are not related should, wherever possible, be housed in separate secure areas. In particular, ICL Pathway managed assets should be located in separate secure areas from third-party managed assets. Each area shall have its own access rights such that personnel are only granted access to relevant secure areas.

Within all ICL Pathway secure areas.

a) visitors must be supervised,
b) date and time of entry and departure should be recorded,
c) visitors must only be granted access for specific, authorised purposes,
d) all personnel should be required to wear visible identification and encouraged to challenge strangers, and
e) access rights must be revoked immediately for staff who leave employment.

5.1.3 Security Of Data Centres and Computer Rooms

Data centres and computer rooms supporting business-critical activities shall have good physical and environmental security.

Data centres and computer rooms supporting ICL Pathway's business-critical activities must have good physical security.

The selection and design of the site should take account of the possibility of damage from fire, flooding, explosions, civil unrest, and other forms of natural or man-made disaster. Consideration should also be given to any security threats presented by neighboring accommodation.

Al all times:

a) key facilities should be sited away from areas of public access or direct approach by public vehicles,
b) where possible, buildings should be unobtrusive and give minimum indication of their purpose, with no obvious signs, outside or inside the building, identifying the presence of computing activities,
c) lobby directories and internal telephone books should not identify locations of computer facilities,
d) hazardous and combustible materials should be stored securely at a safe distance from the site,
e) computer supplies, such as stationery, should not be stored within the computer room until required,
f) fallback equipment and back-up media should be sited at a safe distance to avoid damage from a disaster at the main site,

g) appropriate safety equipment should be installed, such as heat and smoke detectors, fire alarms, fire extinguishing equipment and fire escapes,

h) safety equipment should be checked regularly in accordance with manufacturers' instructions.

i) employees should be properly trained in the use of safety equipment,

j) emergency procedures should be fully documented and regularly tested,

k) doors and windows should be locked when the area is unattended, and

l) external protection should be provided on all windows.

5.1.4 Working in Secure Areas

ICL Pathway personnel and third parties working in secure areas should be made aware that:

a) existance and knowledge of activities within the secure area should be on a need to know basis,

b) unsupervised working in secure areas should be avoided for safety and security reasons,

c) vacant secure areas should be kept locked and periodically checked,

d) all access to secure areas by third parties (e.g. essential service personnel) should be authorised and monitored, and

e) recording equipment (e.g. photographic, video, audio etc) should not be allowed unless explicitly authorised.

5.1.5 Isolated Delivery and Loading Areas

IT assets shall be protected from theft and damage during deliveries and removals.

IT assets are particularly vulnerable to theft and damage during delivery and removal. This applies to hardware, software and consumables (such as media and stationary).

Deliveries must be verified against the order placed with discrepancies reported to the person who placed the order. This person is then responsible for resolving any differences. Differences, which cannot be properly explained and corrected, are to be reported as an information security incident.

An isolated area for delivery and loading of supplies and equipment should be used wherever possible. This should reduce the opportunity for unauthorised access to computer rooms and office accommodation. The security requirements for such an area should be determined by a risk assessment, taking the local environment into account.

Packaging from valuable items should be discarded discretely after delivery to avoid drawing the attention of potential thieves to newly delivered items.

5.2 Equipment Security

Objective:	To prevent loss of, or damage to, IT equipment and the information that it holds.

Equipment shall be physically protected from security threats and environmental hazards.

Protection of IT equipment (including that used off-site) is necessary to prevent loss, damage or compromise to IT assets.

5.2.1 Equipment Siting and Protection

IT equipment shall be sited and protected to reduce the risks of theft and damage.

IT equipment should be sited or protected to reduce the risks from environmental hazards and opportunities for unauthorised access.

Wherever ICL Pathway's equipment is used:

a) Office Managers must ensure that IT equipment is held securely from the time of its delivery from the supplier,

b) where possible, IT equipment should be sited away from public and frequently used areas,

c) IT equipment should be made unobtrusive and give minimal indication of its purpose.

d) Workstations handling sensitive data should be positioned to reduce the risk of being overlooked,

e) all points of access must be made secure against breakage and forced entry. If the building or room cannot be adequately secured, then additional measures (e.g. physically protected equipment enclosures) should be used,

f) Office Managers should ensure that the environmental conditions (e.g. ventilation) recommended by the equipment manufacturer are maintained at all times,

g) smoking, eating and drinking must be prohibited close to IT equipment,

h) hazardous and combustible materials, including stationery, must not be stored alongside IT or other equipment,

i) used combustible material, including waste paper, should be cleared away regularly, and

j) consideration should be given to potential hazards from neighbouring floors as well as to those from the same floor.

It is the Site Managers responsibility to ensure that IT equipment is protected against potential environmental hazards, including

- fire,
- smoke,
- water,
- dust,
- vibration,
- chemical effects,
- electrical supply interference, and
- electromagnetic radiation.

All protection equipment (e.g. fire extinguishers) must be checked regularly and staff trained in its proper use.

Any loss or damage to IT equipment must be reported as a security incident (see section 4.3.1).

5.2.2 Power Supplies

IT equipment shall be protected from power failures or other electrical anomalies.

The electrical supply should be protected from fluctuations in power and other forms of interference.

All business-critical IT facilities should be provided with standby power supplies.

System Managers must ensure that standby and uninterruptable power supply (UPS) equipment is regularly tested in accordance with the manufacturer's recommendations.

5.2.3 Cabling Security

Power and telecommunication cabling shall be protected from interception or damage.

The following security measures should be applied to reduce these risks within an organisation's premises.

Within ICL Pathway premises, power and telecommunications cabling should, wherever possible, be protected from unauthorised interception or damage (using conduit or by avoiding routes through public areas). System Managers should ensure that power cabling, distribution points and ducting are not exposed to damage.

Outside ICL Pathway premises, power and telecommunications cabling into ICL Pathway facilities must be protected from unauthorised access. Service suppliers should be asked to provide resilience through alternative routing.

5.2.4 Equipment Maintenance

IT equipment shall be operated and maintained in accordance with manufacturers' recommendations. IT equipment and information assets shall be protected during maintenance.

System Managers should ensure that manufacturers' recommended environmental conditions and maintenance schedules are followed.

Where necessary, environmental conditions, including temperature, humidity and power supply quality, should be monitored and controlled to stay within manufacturers' guidelines.

Manufacturers' recommended maintenance should be carried out by users and suitably qualified engineers, as required.

Equipment must be maintained in accordance with the supplier's recommended service intervals and specifications. All maintenance and repair activity should be logged.

Maintenance visits should be arranged in advance, with all repairs and servicing of equipment carried out by authorised maintenance personnel.

Maintenance engineers should not be granted access to classified data, except where access is unavoidable for diagnosing faults. Any additional system access granted for fault rectification must be revoked as soon as the work is completed.

Security administrators shall check that security measures (e.g. power-on passwords) have not been modified or bypassed during maintenance.

5.2.5 Security of Equipment Off-premises

Equipment used outside ICL Pathway's premises shall be adequately protected.

All portable IT equipment should be indelibly marked to indicate that it is ICL Pathway property.

When travelling, equipment and media must not be left unattended in public places. Portable computers should be carried as hand luggage.

All portable equipment must have access controls, anti-virus software and encryption facilities installed. These measures shall be configured to:

- limit access to authorised users,
- log the activity of individual users,
- encrypt all stored data classified as RESTRICTED (or above), and
- provide anti-virus scanning of all imported files.

The Manager responsible for equipment ownership shall ensure that equipment users and custodians are formally authorised, held individually accountable for equipment on loan, and that equipment is not damaged or misused.

5.2.6 Secure Disposal or Reuse of Equipment

Data and software shall be thoroughly erased from equipment prior to disposal.

Hard disks and other media must be reformatted or completely erased to ensure that all data and software is removed or overwritten prior to disposal.

Damaged storage devices containing very sensitive data may need to be destroyed. The ICL Pathway Security Manager shall advise in such cases.

Upon disposal, ICL Pathway's asset registers should be updated. Software licences should be reused wherever possible. Disposal of media is addressed in section 6.6.4).

5.3 General Controls

Objective:	To prevent compromise of theft of information and information processing facilities.

Information and information processing facilities shall be protected from unauthorised disclosure, modification and theft.

5.3.1 Clear Desk and Clear Screen Policy

A clear desk policy shall protect information from unauthorised access, loss or damage.

ICL Pathway's clear desk policy should be applied to all information assets, in order to reduce the risks of unauthorised access, loss of and damage to information outside normal working hours.

In particular:

a) Papers and diskettes should be stored in cabinets when not in use, especially outside working hours.

b) Sensitive or business-critical information should be locked away (ideally in a fire-resistant cabinet) when not required, especially when the office is vacated.

c) Key locks, passwords or other controls, should be used to protect personal computers and computer terminals when not in use.

d) Consideration should be given to the need to protect incoming and outgoing mail points and unattended fax machines.

5.1.2 Removal of Property

Removal of property belonging to the organisation shall require authorisation.

Equipment, data or software, should not be taken off-site, without documented management authorisation.

Removals must be formally authorised in writing by the appropriate System Manager. The Security Guard (or equivalent) should check the approval document, which must be carried by the person removing the item, when the item is removed from ICL Pathway premises.

6. COMMUNICATIONS AND OPERATIONS MANAGEMENT

6.1 Operational Procedures and Responsibilities

Objective:	To ensure the correct and secure operation of computer and network facilities.

Documented procedures, for the management and operation of all computers and networks, shall be provided and kept up-to-date.

Appropriate operating instructions and incident response procedures shall be used. The principle of segregation of duties (see section 6.1.4) shall be applied, where appropriate, to reduce the risk of negligent or deliberate system misuse.

6.1.1 Documented Operating Procedures

Documented procedures shall be provided for the operation of all computer systems.

Clear, documented operating procedures should be prepared for all operational computer systems to ensure their correct, secure operation. Documented procedures should also be prepared for systems development, maintenance and testing work, especially if it requires the support or attention of other organisational functions (e.g. computer operations).

Documentation should specify, in detail, procedures for:

a) normal system operation, including the scheduling of regular tasks,

b) handling errors or other exceptional conditions which might arise during job execution,

c) detection and correction of system failures and security breaches, before they damage the integrity, confidentiality or availability of the system,

d) correct handling of files, storage media and printed output, with due regard to the classification of the information they contain,

e) copying and safe-keeping of system data for back-up purposes, and

f) system restart and recovery in the event of system failure.

Change control procedures should be enforced to ensure that amendments to operating procedures are properly considered and authorised. All changes to processing schedules should be subject to management approval.

Operating procedures should only be issued to authorised personnel. Similarly, restrictions should apply to the use of system utilities (see section **Error! Reference source not found.**).

6.1.2 Operational Change Control

Changes to information processing facilities and systems shall be controlled.

All changes to information processing systems and facilities should be subject to impact analysis and approval.

System Managers should ensure that all equipment, software, data and procedures that make up their system are recorded as configuration items in ICL Pathway's Configuration Management System. This should include the links between items so that the full impact of any change can be assessed.

Change Control procedures should be implemented as specified in section 8.5.1.

6.1.3 Incident Management Procedures

Incident management responsibilities and procedures shall be established.

Incident management procedures should ensure a quick, effective and orderly response to every security incident (as defined in section 4.3.1).

In addition to normal contingency plans, incident management procedures should cover:

a) all potential types of security incident (see section 4.3.1),
b) procedures for reporting incidents (see section 4.3.1),
c) collection of audit trails and similar evidence,
d) identification and analysis of the cause of the incident,
e) communication with business users and others affected by, or involved with, recovery from the incident,
f) orderly recovery from the incident, and
g) planning and implementation of remedies to prevent recurrence.

Audit trails and similar evidence should be collected and secured at the earliest opportunity. This must be done without modifying, or in any other way undermining, the evidence.

In addition to problem analysis, such evidence may be necessary to support charges of breach of contract, regulations or legislation, or to support negotiations for compensation from suppliers. It may also be used as evidence in the event of proceedings under computer misuse or data protection legislation (see section 10.1).

Action to correct and recover from security breaches and system failures should be carefully and formally controlled. During this period, the ICL Pathway Security Manager should ensure that:

1. only clearly identified and authorised staff are allowed access to live systems and data,
2. all emergency actions taken are documented in detail,
3. emergency action is reported to management and reviewed in an orderly manner, and
4. the integrity of business systems and security controls is confirmed with minimal delay.

6.1.4 Segregation of Duties

Segregation of duties shall be applied to minimise the risk of negligent or deliberate system misuse.

The management and execution of security-critical duties must be separated in order to reduce opportunities for unauthorised modification or misuse of data or services. In particular, the following functions should not be carried out by the same person:

a) business system use,
b) system administration, supervision or operation,
c) network management,
d) systems development and maintenance,
e) change management, and
f) security administration or audit.

Additional segregation constraints should be applied to systems supporting business-critical financial applications.

For small systems, where it may be impractical to achieve this degree of separation, the same principle should be applied with the System Manager responsible for allocation of responsibilities.

6.1.5 Separation of Development and Operational Facilities

Development and testing facilities shall be isolated from operational systems.

Development and testing activities may cause unintended changes to software and data sharing the same computing environment. In addition, the powers required by developers are inappropriate in an operational environment.

The following controls should be applied:

a) Development and operational software should, run on different processors, Where this is not possible, they must run in different domains or directories.

b) Developer's powers must be confined to the development environment.

c) Testing activities must take place in an environment that is isolated from the operational environment. Wherever possible, development and test/validation activities should also be separated.

d) Compilers, editors and other system utilities should not be stored in, or accessible from, operational environments.

e) Different logon procedures should be used for operational and development/test systems, to reduce the risk of confusion. Users should use different passwords for these systems.

f) Development and test systems should display appropriate identification messages.

6.1.6 External Facilities Management

Proposals to use an external facilities management service shall identify the full security implications and include appropriate security controls.

The use of an external contractor to manage computer or network facilities may introduce or increase some security risks whilst reducing others. These risks must be identified in advance with appropriate security measures agreed with the contractor and incorporated into the contract.

Particular issues that should be addressed include:

a) the need to retain in-house any particularly sensitive or critical applications or functions,

b) the need for approval of business application owners,

c) the implications for business continuity planning,

d) the process for measuring compliance with ICL Pathway's Security Policy, [SECPOL],

e) the security standards to be applied, and

f) the responsibilities and procedures for reporting and handling security incidents (see section 6.1.2).

Guidance on security conditions in third party contracts is provided in section 2.2.2.

6.2 System Planning and Acceptance

Objective:	To minimize the risk of systems failures.

Advance planning and preparation shall be used to ensure the availability of adequate capacity and resources.

Projections of future capacity requirements should be made, to reduce the risk of system overload. The operational requirements of new systems should be established, documented and tested prior to their acceptance. Fallback requirements for services supporting multiple applications should be coordinated and regularly reviewed.

6.2.1 Capacity Planning

Future information processing requirements shall be estimated to ensure that adequate processing, storage and network capacity is made available when needed.

Forecasts of future information processing capacity requirements should be made to ensure that adequate processing power, storage and network capacity remain available. These forecasts should take account of new system requirements and ICL Pathway's future system strategy.

Information system planners and network managers should use this information to provide adequate information processing facilities and infrastructure. System Managers and Security Managers should use this information to predict and avoid deficiencies that might threaten system security.

Mainframe computers require particular attention because of the greater cost and lead time for procurement of new capacity. Managers of mainframe services should monitor the utilization of key system resources, including processors, main storage, file storage, printers and other output devices, and communications systems. They should identify trends in usage, particularly in relation to business applications or management information system (MIS) tools.

6.2.2 System Acceptance

Acceptance criteria for new systems and system upgrades shall be established. Tests against these criteria shall be satisfied before the system or upgrade is accepted.

System managers should ensure that the requirements and criteria for acceptance of new computer systems are clearly defined, agreed, documented and tested. These should include:

a) performance criteria,

b) capacity requirements,

c) business continuity requirements,

d) testing criteria, and

e) training requirements.

Approval of criteria and requirements should include the ICL Pathway Security Manager and Managers of any other systems that are impacted.

For major new developments, the operations function should be consulted at all stages in the development process to ensure the operational efficiency of the proposed system design. Appropriate tests should be carried out to confirm that all acceptance criteria are fully satisfied.

6.3 Protection from Malicious Software

Objective: To protect the integrity of software and information.

Tools and precautions shall be used to minimise the risk of system failures through attacks by malicious software.

Malicious software is often given names such as computer viruses, macro viruses, network worms, Trojan horses and logic bombs. They all exploit the vulnerability of computer software to unauthorised or unknown modification.

6.3.1 Controls Against Malicious Software

Tools shall be used to prevent, detect and correct attacks by malicious software.

Since there are many anti-virus products available, the ICL Pathway Security Manager should provide up-to-date advice on which tools give the best protection for a given situation. The onus is on System Managers to seek advice on anti-virus protection and to obtain the necessary funding for tools.

Four types of tools should be considered:

- **Virus Recognition**: which scan files and disks searching for known types of malicious software.
- **Integrity Checking**: which check for spurious files and unauthorised amendments to existing files.
- **Device Controls**: which constrain risky user actions (e.g. booting a PC from a floppy disk).
- **E-mail Scanning**: which check electronic mail attachments for macro-based attacks.

Whatever tools are used, they must be updated regularly to ensure that they are capable of detecting new virus types.

Licence arrangements for anti-virus tools should include a commitment from the supplier to provide regular updates. These should be supplied and applied at least quarterly.

Before using anti-virus tools to scan a computer, the computer should be re-booted from a virus-free system disk. This will prevent the possibility of boot sector viruses concealing themselves in memory.

Anti-virus tools are insufficient in themselves to prevent, detect and correct attacks by malicious software. Procedures must be deployed to ensure that the tools are used correctly (see section 6.3.2).

The ICL Pathway Security Functional Specification [SFS] defines the virus protection measures that should be incorporated into the operational ICL Pathway system.

6.3.2 Anti-Virus Procedures

Precautions shall be implemented to help prevent, detect and correct attacks by malicious software.

Users should be kept aware of their role in preventing and detecting attacks by malicious software. This includes guidance in the use of anti-virus tools (see section 6.3.1).

No unauthorised software should be loaded onto, or stored in, any ICL Pathway system.

Anti-virus tools must be used to scan computers and storage media on a routine basis. All exchangeable disk media (e.g. floppy disks and CD ROMs) must be scanned on receipt. This includes new software from all sources and disks from other ICL Pathway sites. Similarly, all disk media that is to be dispatched must be scanned before it is sent.

Integrity checking software (see section 6.3.1) should be installed to protect business-critical systems and data. It should be used regularly to detect the presence of spurious files and unauthorised amendments.

When malicious software is detected the following steps should be followed immediately:

- Switch off the suspect computers and do not use them again until the outbreak has been investigated.
- Collect and "quarantine" suspected disks and all others that have been used on the suspect computer.
- Notify the ICL Pathway Help Desk who will notify the ICL Pathway Security Manager to arrange for a Security Administrator (or IT Specialist) to investigate and clear the infected computers and disks.
- Notify any other offices to which suspect disks or files have been sent.

All virus infections are security incidents, which should be reported as defined in section 4.3.1.

Management procedures and responsibilities should be established for reporting and recovering from virus attacks (see sections 4.3 and 6.1.2). Appropriate business continuity plans should be established for virus attacks, including all necessary data and software back-up and recovery arrangements (see section 9.1).

6.4 Housekeeping

Objective:	To maintain the integrity and availability of information processing services.

Good housekeeping and preventative maintenance shall be practised to maintain the integrity and availability of services.

Routine procedures should be established for taking back-up copies of data, logging events and faults and, where appropriate, monitoring the equipment environment.

6.4.1 Information Backup

Back-up copies of essential business data and software shall be taken regularly and stored securely. The process of restoring from back-up copies shall be tested regularly.

Back-up facilities must ensure that all essential business data and software can be recovered following a computer disaster or media failure. The back-up arrangements for individual systems should meet the requirements of business continuity plans (see section 9.1).

In all cases:

a) Back-up copies should be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the original site.

b) At least three generations of back-up data should be available, at the remote site, at any one time.

c) Additional copies, held close to the system for convenience, should be stored in a fireproof safe.

d) All back-up media should be clearly marked with:
   - the name of the system or system files contained,
   - the date and time the copy was taken, and
   - the version number (for software).

e) Accurate and complete records of the back-up copies should be stored securely.

f) Back-up data should be given an appropriate level of physical and environmental protection (see section 5) consistent with the standards applied at the main site.

g) The controls applied to media at the main site should be extended to cover the back-up site.

h) Back-up copies should be regularly tested to ensure that they can be relied upon for emergency use when necessary.

Recovery processes should be tested at least every 12 months and whenever there is a significant change to the system software or operating procedures. These tests should simulate recovery from a complete loss of data and software.

Where a third party provides back-up services, requirements must be specified in a Contract or Service Level Agreement.

System users should be informed when back-up data is used and advised of any remedial action (such as re-input) that they may need to undertake.

Data owners should specify the retention period for essential business data and any requirement for archive copies to be permanently retained (see section 10.1.3).

In the event of a real incident the Incident Management Procedures should be followed in line with business continuity plans (see sections 6.1.2 and 9.1).

Data owners should specify the retention period for essential business data in addition to any requirement for archive copies to be permanently retained (see section 10.1.3).

6.4.2 Operator Logs

Computer operators and other system administrators shall maintain a log of all changes they make to a system and all other significant system management events.

Wherever possible, the collection of system logs should be automated and it should not be possible to disable them. Log files must be protected from alteration, deletion and other forms of attack. Only authorised personnel must be allowed to read them.

System logs should include:

a) system start and finish times (including unplanned down time),

b) other scheduled events (e.g. data back-up),

c) changes made to the system configuration or reference data,

d) system errors and incidents (including corrective action taken), and

e) confirmation of the correct handling of data files and output.

System logs should be subject to regular, independent checks against operating procedures. They must be available for inspection by auditors, investigators and security personnel. They must be retained in accordance with the ICL Pathway Audit Policy [AUDPOL].

6.4.3 Fault Logging

Faults shall be reported and corrective action taken.

All faults with hardware, software and systems must be reported. For operational systems, the ICL Pathway Help Desk should be contacted (see section 4.3.3).

Faults which have affected the confidentiality, integrity or availability of the system should also be reported to the ICL Pathway Help Desk, which will log the fault and route it to the ICL Pathway Security Manager for action (see section 4.3.1).

Corrective action will be reviewed by the ICL Pathway Security Manager (or nominated Security Administrator) to ensure that security controls have not been compromised.

6.5 Network Management

Objective:	To ensure the safeguarding of information in networks and the protection of the supporting infrastructure.

The security management of computer networks, which span organisational boundaries, must conform to the ICL Pathway Security Functional Specification.

The ICL Pathway Security Functional Specification [SFS] specifies the security functionality used to protect the communications links used by ICL Pathway's operational system. This includes the cryptographic protection of "external" links to third party sites.

6.5.1 Management Responsibility for Networks

Management responsibility for all networks used by ICL Pathway shall be clearly defined.

All ICL Pathway's networks should have nominated Systems Managers with responsibility for safeguarding the confidentiality and integrity of data passing over their network. They also have responsibility for ensuring that connected systems are protected from unauthorised external access via their networks.

Operational responsibility for networks should be separated from computer operations, where appropriates (see section 6.1.4).

The type of protection required for ICL Pathway's operational system is specified in the Functional Specification [SFS] and Access Control Policy [ACCPOL].

6.5.2 Managing External Network Links

ICL Pathway uses the public Integrated Services Digital Network (ISDN) and leased lines to communicate with third party organisations. These connections are protected as specified in the ICL Pathway Security Functional Specification [SFS].

For external communication links, the network management responsibilities should be formally specified in the relevant Contract and/or Service Level Agreement. Such agreements should clearly define the boundaries of the network and responsibilities for remote equipment (including routers and encryption devices).

Network Access Control and Data Encryption are considered in sections 7.4 and 8.3.2, respectively.

6.6 Media and Documentation Security

Objective:	To safeguard the confidentiality, integrity and availability of information on storage media and system documentation.

Computer media and documentation shall be controlled and physically protected.

The controls described in this section are designed to protect computer media (e.g. tapes, disks, cassettes), input/output data and system documentation from damage, theft and unauthorised access.

6.6.1 Management of Removable Computer Media

Removable computer media shall be controlled and physically protected from damage, theft and unauthorised access or copying.

Media should be stored in a safe, secure environment in accordance with manufacturers' specifications.

Media that contains Protectively Marked data should be labelled accordingly (see section 3.2.2) and locked away when not in use.

Media containing important back-up data should be stored away from the computer site (see section 1.1.1).

For Data Centres supporting business-critical systems, the Operations Manager should appoint a media librarian. He/she should be responsible for the security of the media in the library and required to control all movement of media belonging to the data centre. Written authorisation should be required before media is removed. All media library procedures and authorisation levels should be clearly documented.

Storage media must be labelled to distinguish between that containing live, development, test, archive and back-up data. The data storage system used should avoid descriptive labels, so that the data stored is not identifiable from its label.

Any re-usable media that is no longer required should be erased.

6.6.2 Disposal of Media

Protectively Marked computer media shall be disposed of securely when no longer required.

Storage media containing Protectively Marked data must be erased completely before it is used for other purposes within ICL Pathway. If the media is damaged or no longer required by ICL Pathway, it should be physically destroyed (e.g. by incineration or shredding).

If the content of data storage media is unknown and there is a possibility that it may have contained Protectively Marked information, then it should be treated as if it does contain such data.

Secure disposal (and re-use) of computer equipment is defined in section 5.2.6.

6.6.3 Information Handling Procedures

ICL Pathway shall establish information handling procedures.

The booklet “Security of Information” issued by ICL Group Security provides practical guidelines for handling information that is sensitive.

Particular attention should be paid to:

a) handling and labelling of all media,
b) limiting access to documents and media to authorised personnel,
c) maintaining records of authorised recipients of information,
d) ensuring that input data is complete, processing is properly completed and that output validation is applied,
e) protection of spooled data awaiting output,
f) the environment used for media storage,
g) keeping the distribution of data to a minimum,
h) clearly identifying the intended recipient of the data, and
i) periodic review of distribution lists to check authorisation of recipients.

When disposing of information:

- redundant Protectively Marked documentation should be destroyed securely (e.g. shredded), and
- disposal of sensitive items should be logged, where possible, for future reference and to maintain an audit trail.

6.6.4 Security of System Documentation

System documentation shall be protected from loss and unauthorised access.

System documentation that contains sensitive information (e.g. descriptions of applications processes, procedures, data structures and authorisation processes) should be classified accordingly.

Protectively Marked system documentation should only be distributed to, and held by, those with a specific need and approval to use the information. Printed documents, when not in use, should be locked in sturdy cabinets.

An appropriate level of access control, as specified in [ACCPOL], must be used to protect computer held documents.

System documentation should be maintained under configuration control (see section 1.1.1). The distribution list for system documentation should be kept to a minimum and authorised by the application owner.

6.7 Exchanges of Information and Software

Objective:	To prevent loss, modification and misuse of information exchanged between organisations.

Exchange of information and software between organisations shall be controlled.

The Office Automation facilities (e.g. MS Office) and the electronic mail systems used by ICL Pathway need to be used with care, to maintain the integrity and confidentiality of information processed and exchanged.

6.7.1 Information and Software Exchange Agreements

Agreements for the exchange of data and software shall specify security controls.

Formal agreements, including software escrow agreements when appropriate, should be established for exchange of data and software (whether electronic or manual) between organisations. The security content of such an agreement should reflect the sensitivity of the business information involved. Agreements should specify appropriate security conditions including:

a) management responsibilities for controlling and notifying transmission, despatch and receipt,

b) procedures for notifying transmission, despatch and receipt,

c) minimum technical standards for packaging and transmission,

d) courier identification standards,

e) responsibilities and liabilities in the event of loss of data,

f) data and software ownership and responsibilities for data protection, software copyright compliance and similar considerations (see section 10.1.4),

g) technical standards for recording and reading data and software, and

h) any special measures required to protect very sensitive items, such as encryption keys.

6.7.2 Security of Media in Transit

Computer media shall be protected from damage, loss and misuse during transit.

The following controls should be applied to safeguard computer media being transported between sites.

Data storage media should be shipped in packaging that is sufficiently robust to protect the contents from physical damage and in accordance with manufacturers' specifications.

Known and trusted carriers should be used, with the identity of the individual courier being checked before packages are released to them. For Protectively Marked or other important data a formal acknowledgement of receipt should be obtained.

Special measures should be used to protect sensitive information from unauthorised disclosure or modification. Depending upon the sensitivity of the information, appropriate measures are:

a) the use of locked containers,

b) delivery by hand,

c) use of tamper-proof packaging (which reveals any attempt to gain access), and

d) splitting the consignment into more than one delivery and despatching by different routes.

Data storage media should be scanned for malicious software whenever it is sent to, or received from, another site (see section 6.3.2).

6.7.3 Electronic Commerce Security

Special security controls shall be applied to protect electronic data interchange.

Electronic Data Interchange (EDI) with trading partners is vulnerable to unauthorised interception or modification, hence special security controls should be applied.

Assurance and evidence of despatch or delivery should be provided.

The security controls applied to EDI transactions should be agreed with trading partners and value-added network (VAN) providers. Advice should be sought from EDI specialists to ensure compatibility with industry standards.

Guidance on the use of encryption and message authentication techniques is provided in sections 8.3.2 and 8.2.3 respectively.

6.7.4 Security of Electronic Mail

Security controls shall be established to minimise the business and security risks associated with electronic mail.

E-mail System mangers should implement controls to reduce business and security risks that may be presented by the use of electronic mail (e-mail). Issues that should be addressed include:

a) vulnerability of messages to unauthorised interception or modification,
b) the need for careful and selective e-mail addressing – to avoid misdirection and unnecessary circulation,
c) how to protect Protectively Marked e-mail attachments from unauthorised access,
d) reliability and availability of e-mail services,
e) legal considerations, such as the potential need for proof of origin, despatch, delivery and acceptance,
f) need for care over statements made – since e-mail is often treated as less formal than other correspondence but has the same status in law,
g) security implications of publishing directory entries,
h) need for security measures to control remote user access to e-mail accounts, and
i) precautions that must be taken to avoid importing e-mail borne malicious software (see section 6.3.

The ICL Pathway Classification Standards [CLASS] provide guidance on the use of e-mail to transmit information that is Protectively Marked.

6.7.5 Security of Electronic Office Systems

System and Security Managers shall ensure that users are kept regularly reminded of their security obligations in order to minimise security risks associated with electronic office systems.

Electronic office systems provide opportunities for fast dissemination and sharing of business information. User guidelines should, therefore, include:

a) the categories of staff, contractors and third-parties allowed to use the system,
b) the locations from which the system may be accessed (see section 2.2),
c) the need to restrict certain facilities and data areas to specific categories of users,
d) the conditions under which Protectively Marked information may be stored within the system,
e) the need to indicate the status of users in directories – to avoid user errors,
f) the effective use of anti-virus software (see section 6.3.2),
g) user and administrator responsibilities for data back-up and recovery (see section 1.1.1), and
h) fallback and business continuity arrangements (see section 9.1).

Whilst the ICL Pathway Security Manager has overall responsibility for devising and conducting security awareness programmes (see section 2.1.3), their effectiveness will be influenced by reinforcement of messages by System Managers.

In particular, users need to be reminded:

- to use anti-virus measures in the prescribed way,
- that unauthorised software must not be stored or used on ICL Pathway's systems,
- that all security breaches and system malfunctions must be reported (see sections 4.3.1 and 4.3.2), and
- that the system is to be used for ICL Pathway business purposes only.

The ICL Pathway Classification Standards [CLASS] provide guidance on the processing of information that is Protectively Marked.

6.1.6 Publicly Available Systems

ICL Pathway shall ensure that any material made publicly available is suitably protected.

Care should be taken to protect the integrity of electronically published material. This includes information published on web servers for access via the Internet or an Intranet.

Only authorised information should be made publicly available.

Electronic publishing systems which permit feedback (e.g. readers comments sent by e-mail) and direct entering of information (e.g. name and address information) require additional protection. Such systems must also be fully compliant with all relevant legislation, including the Data Protection Act.

6.1.7 Other Forms of Information Exchange

ICL Pathway shall ensure that information exchanged, by whatever means, is suitably protected.

The exchange of information through voice, facsimile and video conferencing facilities should be controlled. Controls should be provided to ensure that these facilities are only accessible by authorised personnel.

7. ACCESS CONTROL

7.1 *Business Requirement for Access Control*

Objective:	To prevent inappropriate and unauthorised access to ICL Pathway's systems.

Access to computer services and data shall be controlled on the basis of business requirements.

This should take account of policies for information dissemination and entitlement.

7.1.1 Access Control Policy

Business requirements for access control shall be defined and documented.

To provide effective control of system resources, ICL Pathway should produce and maintain a clearly defined Access Control Policy to identify all users who are authorised to access any part of the system and the access rights that are to be permitted.

The ICL Pathway Access Control Policy [ACCPOL] contains a detailed definition of roles and responsibilities for all personnel who have any kind of access to the services provided by ICL Pathway.

For practical reasons, the Access Control Policy is expressed in terms of roles rather than named individuals. All users will be associated with one or more roles so that all persons will be individually accountable for their actions. Roles have been broadly defined under category headings (e.g. Operational, Systems Management and Support).

7.2 *User Access Management*

Objective:	To prevent unauthorised access to ICL Pathway's systems.

Allocation of access rights to information processing services shall be controlled.

System Managers should ensure that all stages in the life-cycle of user access are covered, from the initial registration of new users to the final deregistration of users who no longer require access to information processing services. Special attention should be given, where appropriate, to the need to control the allocation of privileged access rights that allow users to override system controls.

7.2.1 User Registration

Access to all multi-user information processing services shall be controlled by formal user registration and deregistration procedures.

Access to multi-user information processing services should be controlled through a formal user registration process that should:

a) check that the user has authorisation from the system owner for the use of the service,

b) check that the level of access granted is appropriate for the business purpose,

c) give users a written statement of their access rights,

d) for systems holding classified data, require users to sign undertakings to indicate that they understand the conditions of access,

e) ensure service providers do not provide access until all necessary authorisation procedures have been completed,

f) maintain a formal record of all persons registered to use the service,

g) immediately remove the access rights of users who have changed roles or left the organisation,

h) periodically check for, and remove, redundant User Ids and accounts that are no longer required, and

i) ensure that redundant User Ids are not re-issued to another user.

Users in some roles will be required to use user Ids with additional "tokens", as described in section 7.2.5.

7.2.2 Privilege Management

The use of special privileges shall be restricted and controlled.

The allocation of privileges on multi-user systems should be controlled through a formal authorisation process, which should:

a) identify the privileges associated with each system component (e.g. operating system, database management system) and the categories of staff to which they need to be allocated,

b) allocate privileges to individuals on a "need-to-use" basis (i.e. the minimum privilege needed for that role),

c) maintain an authorisation process and a record of all privileges allocated,

d) ensure that privileges are not granted until the authorisation process is complete,

e) promote the development and use of system routines to avoid the need to grant privileges to users, and

f) ensure that users assigned high privileges for special purposes use a different User Id for normal business use.

7.2.3 User Password Management

The allocation of user passwords shall be securely controlled.

ICL Pathway should use passwords as the principal means of validating a user's authority to access a computer service. In some cases (see section 7.2.5) the use of additional tokens will also be required.

The allocation of passwords should be controlled by a formal management process, which should:

a) require users to sign an undertaking to keep personal passwords confidential and work group passwords solely within the members of the group,

b) ensure that users are provided, initially, with a secure temporary password which they are obliged to change immediately,

c) ensure that replacement passwords (for users who have forgotten their password) are only issued to users who can prove their identity, and

d) require users to acknowledge receipt of passwords.

7.2.4 Review User Access Rights

User access rights shall be reviewed at regular intervals.

ICL Pathway's Security Manager should ensure that the access rights of all users are reviewed, at regular intervals, in order to maintain effective control over access to data and information processing services.

This review process should ensure that:

a) users' access capabilities are reviewed at least every 6 months,
b) authorisations for special privileged access rights (see section 7.2.2) are reviewed every 3 months, and
c) privilege allocations are checked every 3 months to ensure that unauthorised privileges have not been obtained.

7.2.5 Token Management

The allocation of tokens shall be securely controlled.

ICL Pathway should use passwords as the principal means of validating a user's authority to access a computer service (see section 7.2.3).

The Security Administrator(s) responsible for tokens (see section 7.2.5) should ensure that:

a) unallocated devices are held securely, and
b) an inventory of all allocated and unallocated devices is maintained.

Loss of a token must be reported immediately to the relevant System Manager who should ensure that the system rights associated with the use of the lost token are removed immediately. The loss must also be reported as a security incident (see section 4.3.1).

7.2.6 Use of Tokens

The ICL Pathway system should use tokens when the protection provided by passwords alone is not considered to be sufficient. In general, token use should be limited to system management personnel and management operations conducted from, or at, remote sites, as defined in the ICL Pathway Access Control Policy [ACCPOL].

ICL Pathway's Security Functional Specification [SFS] specifies that

a) tokens should be allocated to named individuals for their sole use,
b) the identity of users who have been issued with tokens should be made known to the system and the authentication processes must enforce their use,
c) the system should be capable of selectively revoking the validity of tokens,
d) smart tokens should be used in all cases where a password alone is not considered to be sufficient,
e) each user should be obliged to prove that he/she posses the token at the time of logon,
f) tokens which generate a one-time password, thereby protecting against password replay, should be used,
g) each token will have an associated PIN which must be used to activate the device,
h) personnel who are authorised to access the ICL Pathway system from remote locations[1] should be required to identify themselves using hand held tokens,
i) personnel who are authorised to access the ICL Pathway system using UNIX root privilege should be required to identify themselves using hand held tokens, and
j) personnel who are authorised to access the ICL Pathway system as a database administrator (DBA) should be required to identify themselves using hand held tokens.

[1] This group should comprise selected system administrators authorised to use remote access for system management activities.

7.3 User Responsibilities

Objective: To prevent unauthorised access to ICL Pathway's systems.

ICL Pathway shall seek the cooperation of authorised users in its quest for effective security.

Users should be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment.

7.3.1 Password Use

Users shall follow good security practices in the selection and use of passwords.

Passwords provide the principal means of validating a user's authority to access a computer service.

The following rules apply when allocating and managing their passwords. All users should:

a) change temporary passwords (allocated to new users) at the first logon,

b) choose an individual password (not one shared with others) to maintain accountability,

c) keep their passwords confidential,

d) avoid keeping a paper record of passwords, unless this can be stored securely,

e) change passwords whenever there is any indication of possible system or password compromise,

f) select passwords with a minimum length of six characters.

g) avoid basing passwords on any of the following:
- dictionary words,
- all-numeric or all-alphabetic groups,
- family names, initials or car registration numbers,
- company names, identifiers or references,
- months of the year, days of the week or any other aspect of the date,
- telephone numbers or similar all-numeric groups,
- User Id, user name, group ID or other system identifier, and
- more than two consecutive identical characters.

h) change user passwords at least every 30 days, and more frequently for privileged accounts (e.g. system administrators),

i) avoid re-using or "cycling" old passwords, and

j) never include passwords in any automated logon process (e.g. stored in a macro or function key).

Guidance on the design or selection of password management systems is given in section 7.5.4.

7.3.2 Unattended User Equipment

Users shall ensure that unattended equipment is secured against unauthorised access when it is left unattended.

IT equipment installed in public areas can be particularly vulnerable to unauthorised access. In particular, confidential information may be output to printers or displayed on workstations.

Users should, therefore, take appropriate precautions whenever equipment is left unattended.

For printers, printout should be removed, with personal and classified information locked away. Printers left unattended for an extended period should be switched off.

Portable IT equipment must never be left unattended in public areas or in other situations where theft is likely, such as visible inside an unattended vehicle (see section 5.2.5).

7.4 Network Access Control

Objective:	To protect networked services from damage, interference or disclosure resulting from unauthorised access.

All connections to networked services shall be controlled.

ICL Pathway should have well defined interfaces between networked services, with effective authentication mechanisms for remote users, in order to control access to networked information processing services

7.4.1 Policy on Use of Networked Services

Users shall only be able to gain access to the services that they are authorised to use.

The ICL Pathway Access Control Policy [ACCPOL] defines the level of system and network access permitted for users assigned to particular roles (see section 7.1.1). In particular, users should only be provided with direct access to the services that they have been specifically authorised to use.

7.4.2 Enforced Path

Where appropriate, the route from user terminals to the computer service(s) shall be restricted to an enforced path.

Where appropriate, ICL Pathway should implement controls to restrict the route between each user terminal and the computer services that its user is authorised to access (i.e. creating an enforced path).

The objective of such an enforced path is to prevent any undesirable “straying” by users outside the route between the user terminal and the services that the user is authorised to access. This should be achieved by limiting the routeing options at each point in the network path, using predefined choices.

ICL Pathway should consider:

a) allocating dedicated lines or telephone numbers,

b) automatically connecting ports to specified application systems or security gateways,

c) limiting menu and submenu options for individual users, and

d) preventing unlimited network “roaming”.

The requirements for an enforced path should be based on the ICL Pathway Access Control Policy [ACCPOL], outlined in section 7.1.1.

7.4.3 User Authentication for External Connections

Connections by remote users via public (or ICL Pathway) networks shall be authenticated using passwords and, where appropriate, tokens.

External connections to ICL Pathway's computers provide a route for unauthorised access to business applications. The identity of remote users must, therefore, be verified (authenticated) by a method that is stronger than a password.

Users who require remote access to an ICL Pathway system should use tokens (see section 7.2.5) in addition their password.

Dial-up access to ICL Pathway's systems must be strictly controlled in accordance with the ICL Pathway Security Functional Specification [SFS] and Access Control Policy [ACCPOL].

7.4.4 Node Authentication

All connections with remote computer systems should be authenticated.

All connections between ICL Pathway's computer Systems and other remote computer systems should be protected as specified in the ICL Pathway Security Functional Specification [SFS].

For most links, strong cryptographic mechanisms must be used to provide data integrity and data confidentiality protection.

7.4.5 Remote Diagnostic Port Protection

Third-party access for remote diagnostic or maintenance purposes shall be allocated only where it is necessary.

Many computers have a dial-up remote diagnostic facility for use by maintenance engineers. These diagnostic ports potentially provide a means of unauthorised access. Authorised ICL Pathway personnel should, therefore, only enable these dial-up facilities when needed.

Dial-up access should be subject to the controls described in section 7.4.3, with access only being granted on a case-by-case basis as authorised by the System Manager.

As soon as diagnostic or maintenance activity is complete, the dial-in facility should be disabled. The Security Administrator should then check that only legitimate diagnostic or maintenance activity has taken place.

7.4.6 Segregation In Networks

ICL Pathway's networks shall be divided into separate domains.

ICL Pathway's networks should be divided into domains, each with a clearly defined user community and security perimeter. Several domains may be classed as a single "system" for security policy and management purposes.

Domains should be connected by managed gateways or firewalls which filter traffic on the basis of pre-determined rules or tables.

The ICL Pathway Access Control Policy document [ACCPOL] is structured in terms of the domains defined in the ICL Pathway Security Functional Specification [SFS]. This does not, however, exclude the introduction of other boundaries (e.g. Windows NT Domains) added by the Technical Environment Description [TED].

7.4.7 Network Connection Control

ICL Pathway shall control the access capability of users from other organisations in accordance with the ICL Pathway Access Control Policy.

ICL Pathway should incorporate controls to restrict the connection capability of the users to support the access policy requirements of specific business applications.

Such controls should be implemented through network gateways that filter traffic by means of pre-defined tables or rules. The restrictions applied should be based on the Access Control Policy [ACCPOL] that takes into account the requirements of the business applications.

Examples of such restrictions are:

- electronic mail only,
- one-way file transfer,
- both-ways file transfer,
- interactive access, and
- network access linked to time of day or date.

7.4.8 Network Routeing Control

Where appropriate, ICL Pathway shall use network routeing controls on shared networks.

Shared networks, especially those extending across organisational boundaries, may require the incorporation of routeing controls to ensure that computer connections and information flows do not breach ICL Pathway's Access Control Policy requirements.

Routeing controls should be based on positive source and destination address checking mechanisms. They can be implemented in software or hardware.

7.4.9 Security of Network Services

The risks associated with the use of network services shall be established.

Whilst ICL Pathway's use of external networked services may, initially, be very low, increased usage is to be expected.

A wide range of public or private network services is available, some of which offer value-added services. Such services may have unique and possibly complex security characteristics that need careful consideration.

ICL Pathway should ensure that their network provider gives a clear description of the security attributes of all services used, and should establish the security implications for the confidentiality, integrity and availability of business applications.

7.5 Operating System Access Control

Objective:	To protect ICL Pathway's systems from damage, interference or disclosure resulting from unauthorised access.

Access to all ICL Pathway information processing facilities shall be controlled.

All access to ICL Pathway's systems should be restricted to authorised users in specific roles, as specified in the ICL Pathway Access Control Policy [ACCPOL].

7.5.1 Automatic Terminal Identification

Automatic terminal identification should be used, where appropriate, to authenticate connections to specific locations.

Automatic terminal identification is a technique that can be used for applications in which it is important that the session can only be initiated from a particular location. An identifier in, or attached to, the terminal can be used to indicate whether a particular terminal is permitted to initiate or receive certain transactions. It may be necessary to apply physical security protection to the terminal, to maintain the security of the terminal identifier.

7.5.2 Terminal Login Procedures

Access to information processing services shall be controlled by a secure logon process.

The procedure for logging into a computer system (logon) should be designed to minimize the opportunity for unauthorised access. The logon procedure should, therefore, disclose the minimum of information about the system, in order to avoid providing an unauthorised user with unnecessary assistance.

The logon processes used by ICL Pathway should:

a) begin by displaying a notice warning that the system must only be used by authorised users,
b) not provide help messages that would aid an unauthorised user,
c) not display system or application identifiers until the logon process has been successfully completed,
d) not indicate which logon components were incorrect after an unsuccessful attempt to logon,
e) limit the number of unsuccessful logon attempts to no more than 3 retries, and
f) where appropriate, display the following information on completion of a successful logon:
    - date and time of the previous successful logon, and
    - details of any unsuccessful logon attempts since the last successful logon.

The action taken in the event of an unsuccessful logon will depend upon the environment. It may be appropriate to disable either the user or the terminal device. Recovery may be on a time elapsed basis or could require action by a system administrator.

7.5.3 User Identification and Authentication

Computer activities shall be traceable to individuals.

User Ids should be for the sole use of one person so that individuals can be held accountable for their actions. Used Ids should not give away any indication of the user's privilege (e.g. "manager" or "supervisor").

In exceptional circumstances (e.g. for external Audit purposes) a User Id may need to be shared by a group of users for a specific task. Such cases must be approved by the Security Manager who will specify the additional controls to be used (e.g. recording names of individuals and times of access).

7.5.4 Password Management System

An effective password system shall be used to authenticate users.

The password management systems, used by ICL Pathway, should provide an effective, interactive facility that ensures quality passwords. It should use system mechanisms to enforce the rules for passwords (e.g. password length and change frequency) wherever possible.

User guidance for password use is provided in section 7.3.1.

ICL Pathway's password management system(s) should:

a) enforce the use of individual passwords to maintain accountability (subject to the constraints outlined in section 7.5.3),
b) allow users to select and change their own password and include a confirmation procedure to allow for typing errors,
c) enforce a minimum length for passwords (see section 7.3.1),
d) enforce a password change at regular intervals (see section 7.3.1),
e) wherever possible, maintain a record of previous user passwords and prevent users from reusing them,
f) not display passwords on the screen when they are being entered,
g) store password files separately from the main application system data,
h) store passwords in encrypted form, using a one-way encryption algorithm,
i) alter default vendor passwords following installation of software, and
j) wherever possible, check that the user has selected a quality password, based upon the guidance provided in section 7.3.1.

7.5.5 Use of System Utilities

Access to system utilities shall be restricted and controlled.

System Managers should ensure that the use of system utilities is restricted and tightly controlled. The following controls should be applied, where possible:

a) using password protection for system utilities,
b) segregating system utilities from applications software,
c) limiting of the use of system utilities to the minimum practical number of trusted, authorised users,
d) limiting the availability of system utilities (e.g. for the duration of an authorised change),
e) logging all use of system utilities,
f) defining and documenting authorisation levels for system utilities, and
g) removing all unnecessary utility and system software.

7.5.6 Duress Alarm to Safeguard Users

Provision of a duress alarm shall be considered for users who might be the target of coercion.

The decision whether to supply duress alarms should be based on an assessment of risks. There should be defined responsibilities and procedures for responding to a duress alarm.

7.5.7 Terminal Time-out

Terminals and workstations in public, or other high risk locations, shall be logged out after a specified period of inactivity. Users shall be able to blank the screen and lock the terminal when they leave it unattended for short periods.

A timeout facility should be implemented to log out of application and network sessions after a defined period of inactivity. The timeout delay must be approved by the IT Security Manager based upon an analysis of risk. This should take into account the sensitivity of the system data and the threat of unauthorised access at the terminal location.

In addition to the timeout, some form of software lock (e.g. a user invoked password protected screen saver) should be provided. User sessions on PCs or workstations can then be protected whenever users have to leave terminals unattended for short periods.

Further user guidelines for unattended user equipment are provided in section 7.3.2.

7.5.8 Limitation of Connection Time

General access to high-risk systems shall be restricted to specific times of the day and days of the week.

Connection times for general use should be restricted to normal office hours. If overtime is worked regularly, then these times may also be included. Outside these hours, high risk systems should deny access to normal users.

If possible, predetermined time slots should be used for batch jobs and file transmissions.

7.6 Application Access Control

Objective:	To prevent unauthorised access to information held in computer systems.

Logical access controls shall be used to control access to application systems and data.

Logical access to computer software and data should be restricted to authorised users. Application systems should control user access to data and application system functions, in accordance with the ICL Pathway Security Functional Specification [SFS] and Access Control Policy [AUDPOL].

7.6.1 Information Access Restriction

Access to data and information processing services shall be granted in accordance with ICL Pathway's Access Control Policy.

Users of application systems, including support staff, should be provided with access to data and application system functions in accordance with ICL Pathway's Access Control Policy [ACCPOL].

Application of the following controls should be considered in order to support access policy requirements:

a) providing menus to control access to application system functions,

b) restricting users' knowledge of data or application system functions which they are not authorised to access, with appropriate editing of user documentation,

c) controlling the access capabilities of users (e.g. read, write, delete, execute),

d) ensuring that outputs from application systems handling sensitive data contain only the data relevant to the use of the output, and
e) ensuring that outputs are only sent to authorised terminals and locations.

7.6.2 Sensitive System Isolation

Where appropriate, particularly sensitive systems used by ICL Pathway should be located in a dedicated (isolated) computing environment.

The ICL Pathway Security Manager will advise in the case of any application systems considered to be sufficiently sensitive to potential loss that they require special handling.

7.7 Monitoring System Access and Use

Objective: To detect and enable the correction of unauthorised activities.

Systems shall be monitored to ensure conformity to ICL Pathway's policies.

In particular, ICL Pathway's audit functions should be used to monitor compliance with the:

- ICL Pathway Security Policy [SECPOL],
- ICL Pathway Audit Policy [AUDPOL],
- ICL Pathway Security Functional Specification [SFS], and
- ICL Pathway Access Control Policy [ACCPOL].

The terminology used, within these procedures, is as defined in Annex A, namely:

- **Security Event Management** (SEM) is the collection, analysis and monitoring of security relevant events recorded by components within the ICL Pathway solution.
- **Audit Trail** is a record of those activities considered important to the secure and correct running of the system.
- **Audit Event** is an individual activity reported to the auditing system for inclusion in the audit trail.
- **Audit Analysis** is the process of examining the audit trail for particular events which meet selected analysis criteria.
- **Audit Log** is the output that results from analysis of the audit trail.

7.7.1 Audit Trails

Audit trails of user access and other security-critical events shall be maintained.

All events in the following categories should be capable of being audited:

- authentication actions (including logon, unsuccessful logon attempts and logoff),
- exception conditions (detected by operating systems and at the application level),
- system start-up and close down,
- change of user rights (including granting of additional privileges),
- write access to selected files, and
- system management activities (including addition of new users and reset of any user's password).

Access to the audit trail should be "read only" and granted only to "auditors" (i.e. authorised persons acting in Security Event Management roles).

Audit trails should be protected from unauthorised or accidental deletion, loss corruption or any other form of illicit tampering.

7.7.2 Monitoring System Use

Procedures for monitoring system use, including regular audit analysis, shall be established.

Security Event Management activities should entail routine analysis of audit trail information using agreed selection and filtering criteria. Such analysis should be used to produce higher level summary reports for use by ICL Pathway's Security Manager.

Particular attention should be paid to:

- access failures,
- review of logon patterns for indications of abnormal use or revived user Ids,
- allocation and use of accounts with a privileged access capability,
- tracking of selected transactions, and
- the use of sensitive resources.

All monitoring activities should be formally authorised by the ICL Pathway Security Manager.

7.7.3 Clock Synchronisation

Computer clocks shall be synchronised for accurate recording.

The correct setting of computer clocks is important to ensure the accuracy of audit trails, which may be required for investigations or as evidence in legal or disciplinary cases. Inaccurate audit logs may hinder such investigations and damage the credibility of such evidence.

Where a computer or communications device has the capability to operate a real-time clock, it should be set to an agreed standard (e.g. Greenwich mean time (GMT) or local standard time). There should also be a procedure that checks for and corrects any significant variation.

7.8 Mobile Computing and Networking

Objective:	To ensure information security when using mobile computing and teleworking facilities.

Security risks associated with mobile computing and teleworking shall be assessed and appropriate protection applied.

7.8.1 Mobile Computing

ICL Pathway shall ensure that facilities used for mobile computing are suitably protected.

All users of mobile equipment (e.g. notebooks, laptops and mobile phones) should ensure that business information is not compromised. They are responsible for looking after equipment entrusted to them, ensuring that virus protection measures are updated regularly and that back-up copies are maintained.

Mobile equipment should:

a) be protected using appropriate physical protection, access controls, cryptographic techniques, back-up and virus protection,

b) only be connected to approved networks,

c) used with particular care in public places, meeting rooms and other unprotected areas outside the organisation,

d) use approved cryptographic techniques (see section 8.3) to avoid unauthorised access to or disclosure of sensitive stored information,

e) be installed with up-to-date virus protection software,

f) subject to regular back-up procedures with back-up copies held securely (see section **Error! Reference source not found.**), and

g) not be left unattended in cars (and other forms of transport), hotel rooms, conference centres and meeting places.

Resent surveys have shown that theft is one of the main causes of security breaches, hence all personnel need to be vigilant.

7.1.2 Teleworking

ICL Pathway shall ensure that facilities used for teleworking are suitably protected.

Teleworking enable authorised personnel to work remotely from outside the normal physical ICL Pathway boundaries.

Locations used for teleworking may be fixed (e.g. remote office or home) or temporary (e.g. hotel room) provided appropriate communications are available but in all cases operation must be in accordance with ICL Pathway's Security Policy [SECPOL] and Access Control Policy [ACCPOL].

The ICL Pathway Security Manager's formal approval is required for all forms of teleworking. Such approval should only be granted after he/she has given careful consideration to the:

a) existing physical security of the teleworking site(s),

b) proposed teleworking environment,

c) hardware and software to be used,

d) communications technology to be used,

e) provision and maintenance of virus protection,

f) provision and storage of back-up copies for the off-site equipment used,

g) need for remote access to information held by ICL Pathway, as specified in the Access Control Policy [ACCPOL],

h) threat of unauthorised access to information from other people using the accommodation (e.g. family and friends), and

i) compliance with ICL Pathway's Security Policy [SECPOL].

8. SYSTEM DEVELOPMENT AND MAINTENANCE

8.1 Security Requirements of Systems

Objective:	To ensure that security is built into information processing systems.

Security requirements shall be identified and agreed prior to the development of information processing systems.

Protecting systems is a matter of risk management. The security countermeasures will be cheaper and more effective if they are incorporated into application systems at the requirements specification and design stages.

8.1.1 Security Requirements Analysis and Specification

System Managers shall ensure that an analysis of security requirements is carried out at the analysis stage of each development project.

All security requirements, including the need for fallback processing, should be identified at the requirements phase and justified, agreed and documented as part of the overall business case for an information system.

A risk assessment review of business-critical systems should be commissioned prior to its development. This risk assessment should be revised whenever the system is upgraded to assess the risks introduced by the enhancements.

The results of the risk assessment review contribute to the ICL Pathway Security Policy and Security Functional Specification, hence these should be revised accordingly.

In particular, the analysis of security requirements must consider:

- control of access to information and services (see section 7),
- auditing of access and security-critical events (see section 7.7),
- data integrity checking at all stages of processing and transmission (see section 8.2),
- date encryption (see section 8.2.3),
- compliance with legal, regulatory and commercial requirements (see section 10.1.4),
- back-up of essential data and system software (see section 1.1.1),
- business continuity planning (see section 9),
- computer and network management (see section **Error! Reference source not found.**), and
- security awareness training for users (see section 4.2.1).

The ICL Pathway Security Policy, Security Functional Specification, Access Control Policy and Technical Environment Description have been based upon the results of security analysis of the ICL Pathway solution.

8.2 Security in Application Systems

Objective:	To prevent loss, modification or misuse of user data in application systems.

Appropriate security controls, including audit trails, shall be designed into application systems.

The design and operation of systems, used and developed by ICL Pathway, shall conform to accepted industry standards of good security practice.

8.2.1 Input Data Validation

Data input to, and processed by, application systems shall be validated.

Data should be subjected to validation, reasonableness and consistency checks to reduce the risk of user error and system misuse.

Controls should include:

a) inspection of hard-copy input documents for any unauthorised changes to input data,

b) checks to detect:

- out-of-range values,
- invalid characters in data fields,
- missing or incomplete data, and
- unauthorised or inconsistent control data,

c) periodic review of key data to confirm validity and integrity,

d) checks on the integrity of data transmitted between network nodes,

e) procedures for responding to validation errors, and

f) separation of duties in the data input process.

8.2.2 Control of Internal Processing

Data processed by application systems shall be validated.

Data correctly entered into ICL Pathway's application system should be protected against corruption which could result from processing errors and/or deliberate acts. Validation checks should be incorporated into systems to detect such corruption.

The controls needed will depend on the nature of the application and the business impact of any corruption of data. They should normally include:

a) session or batch controls, to reconcile data file balances after transaction updates,

b) balancing controls, to check opening balances against previous closing balances, namely:

- run-to-run controls,
- file update totals, and
- program-to-program controls,

c) validation of system-generated data,

d) checks on the integrity of data or software downloaded, or uploaded, between central and remote computers (see section 8.3.3),

e) hash totals of records and files.

8.2.3 Message Authentication

A message authentication system shall be considered for applications which involve the transmission of sensitive data.

ICL Pathway will use message authentication mechanisms, where appropriate, to detect unauthorised changes to, or corruption of, the contents of a transmitted electronic message.

Message authentication should be considered for applications where it is vital to protect the integrity of the message content (e.g. electronic funds transfers or other electronic data exchanges). Its use should be based upon an assessment of security risks.

Message authentication provides data integrity protection without data confidentiality protection. It is not, therefore, designed to protect the contents of a message from eavesdropping.

Where there is a requirement to also provide data confidentiality protection, data encryption (see section 8.2.3) should be used.

8.2.4 Output Data Validation

System Managers shall ensure that all software is thoroughly tested before it is used operationally. Where appropriate, validation should include plausibility checks on output data.

System Managers should ensure that (at least) three levels of testing are completed successfully before software is used for operational purposes.

a) **Program or Unit Testing** by system developers to ensure that program modules, programs and functional areas operate in accordance with their specification,

b) **System or Integration Testing** by an independent system integration test group, to ensure that the system as a whole works properly, and

c) **User Acceptance Testing** by user representatives to ensure that users' requirements have been met.

Each of these tests should include verification that the security functionality operates in accordance with its specification.

The ICL Pathway Security Functional Specification [SFS] and Access Control Policy [ACCPOL] specify the base level of security requirements for testing purposes. Test specifications should be used to document the test procedures and expected results.

Formal acceptance should be based upon the successful completion of all tests in accordance with their test specifications.

The environment used for testing must be separated from the operational environment. This will ensure that testing cannot affect the operation of the live system or the integrity of live data.

8.3 Cryptographic Controls

Objective:	To protect the confidentiality, integrity and authenticity of information.

Cryptographic controls shall be used to protect information wherever other controls do not provide the required level of protection.

8.3.1 Policy on the Use of Cryptographic Controls

Use of cryptographic controls, within the ICL Pathway system, shall be based upon an assessment of the security risks.

The initial risk assessment for the ICL Pathway system confirmed that cryptographic controls were needed to provide the required level of protection.

This ICL Pathway Security Functional Specification [SFS] specifies the cryptographic functionality, within the ICL Pathway system, used to protect:

- data on individual communications links,
- individual messages from creation to use (end-to-end), and
- data stored on physically insecure Post Office filestore.

Essential considerations include:

a) the types of cryptographic protection required (i.e. integrity and/or confidentiality),
b) the encryption algorithms used,
c) the key management techniques,
d) recovery of encrypted information in the case of lost, compromised or damaged keys,
e) roles and responsibilities (e.g. key custodians), and
f) selection of appropriate cryptographic products.

All cryptographic products and techniques, deployed within the ICL Pathway system, shall be used in strict accordance with Government guidelines.

8.3.2 Encryption

Classified information shall be encrypted before it is stored and transmitted in an untrusted environment. Government guidelines on encryption shall be followed.

Encryption is the process of transforming information into an unintelligible form, to safeguard its confidentiality and integrity during transmission or in storage. The process uses an encryption algorithm and secret key information, known only to the authorised users. The level of protection provided depends on the quality of the algorithm and the secrecy of the key.

ICL Pathway shall use encryption to protect sensitive information that is vulnerable to unauthorised access, in transmission or storage. An assessment of security risks shall be undertaken to determine where encryption is necessary, and to identify the level of protection required.

The encryption methods used within the ICL Pathway solution shall be based upon specialist advice with suitable products and algorithms selected in accordance with Government guidelines. The design and implementation of the key management system shall be given particular attention to detail.

The high level specification of the encryption facilities used shall be documented in the ICL Pathway Security Functional Specification [SFS]. This will identify the communications links to be protected, the algorithms to be used and the key management methods. The SFS shall also define the cryptographic requirements for protecting information stored on hard disks located in vulnerable locations.

8.3.3 Digital Signatures

Wherever appropriate, ICL Pathway system shall use standard public key technology to provide integrity protection of messages.

Under public key technology, protected messages shall be digitally signed by a private key and validated using the private key's matching public key.

Working public keys shall be distributed either at roll-out or by a Key Management System (KMS) using public key certificates signed by a private key from a Certification Authority (CA).

8.3.4 Non-repudiation Services

Non-repudiation services, based upon the use of cryptographic techniques, shall be used, where appropriate, within the ICL Pathway system.

Proof of occurrence or non-occurrence of an action or event should, where necessary, be based upon the cryptographic mechanisms used to protect messages.

8.3.5 Key Management

A message authentication system shall be considered for applications that involve the transmission of sensitive data.

ICL Pathway will use message authentication mechanisms, where appropriate, to detect unauthorised changes to, or corruption of, the contents of a transmitted electronic message.

Message authentication should be considered for applications where it is vital to protect the integrity of the message content (e.g. electronic fund transfers or other electronic data exchanges). Its use should be based upon an assessment of security risks.

Message authentication provides data integrity protection without data confidentiality protection. It is not, therefore, designed to protect the contents of a message from eavesdropping.

Where there is a requirement to also provide data confidentiality protection, data encryption (see section 8.2.3) should be used.

8.4 Security of System Files

Objective:	To ensure that IT projects and support activities are conducted in a secure manner.

Access to System Files shall be controlled, in accordance with ICL Pathway's Access Control Policy [ACCPOL].

Maintaining system integrity is initially the responsibility of the Development Manager. It subsequently becomes the responsibility of the Operations Manager when the application has been accepted for operational use.

8.4.1 Control of Operational Software

Strict control shall be exercised over the implementation of software on operational systems.

The controls implemented, within ICL Pathway, to minimize the risk of corruption of operational systems should ensure that:

a) the updating of the operational program libraries is only performed by the nominated librarian upon authorisation from the IT support manager for the application (see section 1.1.1),
b) wherever possible, only executable code is held on operational systems,
c) executable code is not be implemented on an operational system until evidence of successful testing and user acceptance is obtained, and the corresponding program source libraries have been updated,
d) an audit log is maintained of all updates to operational program libraries, and
e) previous versions of software are retained as a contingency measure.

8.4.2 Protection of System Test Data

Test data shall be protected and controlled.

System and acceptance testing usually requires substantial amounts of test data that is as close as possible to the live data.

The use of real data for testing should be avoided wherever possible. Personal data (e.g. information provided by the Benefit Agency) must only be used if it is first de-personalised such that the individual's identity is replaced with fictitious information.

The following controls should be applied to protect test data when it is used for testing purposes.

a) an appropriate level of access should be applied to the data (see section 7.1.1),
b) separate approval should be sought from the System Manager each time real data is copied for testing purposes, and
c) the copying of live data should be logged for audit purposes.

Test data should be stored in a separate environment from that used to store operational data. The aim is to ensure that test data cannot be used accidentally in the live environment nor affect the integrity of real data.

8.4.3 Access Control to Program Source Library

Access to program source libraries shall be restricted and controlled.

ICL Pathway should maintain strict control over access to program source libraries in order to minimize the corruption of computer programs.

In particular:

a) program source libraries should not be held in operational systems,
b) a program librarian should be nominated for each application,
c) IT support staff should not have unrestricted access to program source libraries,
d) updating program source libraries and issuing program sources to programmers should only be performed by the nominated librarian,
e) all requests to the librarian(s) should be authorised,
f) program listings should be held in a secure environment (see section 6.6.4),
g) all accesses to program source libraries should be logged by the librarian(s), and
h) old versions of source programs should be archived.

Maintenance and copying of program source libraries should be subject to strict change control procedures (see section 8.5.1). These should include a clear indication of the precise dates and times when the objects were operational, together with all supporting software, job control, data definitions and procedures.

8.5 Security in Development and Support Processes

Objective:	To maintain the security of application system software and data.

Project and support environments shall be strictly controlled.

Managers who are responsible for application systems should also be responsible for the security of the project or support environment. They should ensure that all proposed system changes are reviewed to ensure that they do not compromise the security of either the system or the operating environment.

8.5.1 Change Control Procedures

All systems development shall be controlled either by rigorous project controls or by formal change control procedures.

System Managers should ensure that system changes are subject to configuration management. This should include all links between system components so that the impact of all changes can be assessed.

Formal change control procedures should ensure that security and control procedures are not compromised, that support programmers are only given access to those parts of the system that are necessary for their work, and that formal approval for any change is obtained. This process should include:

a) maintaining a record of agreed authorisation levels, including:
   - IT support team focal point for change requests,
   - user authority for submission of change requests,
   - user authority levels for acceptance of detailed proposals, and
   - user authority for the acceptance of completed changes,

b) only accepting changes submitted by authorised users,

c) reviewing security controls and integrity procedures to ensure that they will not be compromised by the changes,

d) identifying all computer software, data files, database entities and hardware that require amendment,

e) obtaining approval for detailed proposals before work commences,

f) ensuring that changes are accepted by the authorised user before implementation,

g) ensuring that the system documentation set is updated on the completion of each change and that old documentation is archived or disposed of,

h) maintaining a version control for all software updates, and

i) maintaining an audit log of all change requests.

Operational aspects are described in section1.1.1.

8.5.2 Technical Review of Operating System Changes

The impact of operating system changes on security shall be reviewed.

ICL Pathway will need to periodically change the operating system (e.g. to install a new release of Windows NT) on selected platforms. When such changes are necessary, the application systems should be reviewed to ensure that there is no adverse impact on security.

This process should include:

a) review of application control and integrity procedures to ensure that they have not been compromised by the operating system changes,

b) ensuring that the annual support plan and budget will cover reviews and system testing resulting from operating system changes, and

c) ensuring that notification of operating system changes are provided in time to allow appropriate reviews to take place before implementation.

8.5.3 Restrictions on Changes to Software Packages

Modifications to software packages shall be discouraged and essential changes strictly controlled.

As far as possible, and practicable, vendor-supplied software packages should be used without modification. In circumstances where it is deemed essential to modify software packages it is important to assess:

a) the risk of built-in controls and integrity processes being compromised,

b) the possible need to obtain the consent of the vendor,

c) the possibility of obtaining the required changes from the vendor as standard program updates, and

d) the possibility of the organisation becoming responsible for the future maintenance of the software as a result of changes.

If changes are deemed essential, then the original software should be retained and the changes applied to a clearly identified copy. These changes should be fully documented, so that they can be reapplied, if necessary, to future software upgrades.

8.5.4 Covert Channels and Trojan Code

ICL Pathway shall take appropriate precautions to prevent information being exposed through the exploitation of indirect or obscure means, known as Covert Channels.

All reasonable precautions shall also be taken to ensure that software used does not contain Trojan Horses that can be triggered to cause the programs to operate in an unauthorised manner. Precautions used will include the application of appropriate controls for bespoke development activities and purchase of standard products from reputable suppliers.

8.5.5 Outsourced Software Development

ICL Pathway shall ensure that all outsourced software development is adequately controlled.

For all outsourced software development, ICL Pathway shall ensure that:

a) licensing arrangement, code ownership and Intellectual Property Rights (IPR) are formally agreed,

b) the quality and accuracy of the work undertaken is verified,

c) formal test and acceptance procedures are completed successfully before the software is used operationally, and

d) escrow arrangements are considered, to enable recovery from failure using a third party.

9. BUSINESS CONTINUITY MANAGEMENT

9.1 Aspects of Business Continuity Management

Objective:	To ensure that business-critical processes are restored to normal operation as soon as possible following any likely disaster or failure that affects resources, services or IT facilities.

Business continuity plans shall be available to protect business-critical processes from the effects of major failures or disasters.

ICL Pathway shall develop and maintain appropriate plans for the speedy restoration of business-critical processes and services in the event of serious business interruptions. Such interruptions may be caused by, for example, natural disasters, accidents, equipment failures, deliberate action, loss of supplied services or loss of utilities.

Business continuity planning shall include measures to identify and reduce risks, limit the consequences should a threat be realized, and ensure speedy resumption of essential operations.

9.1.1 Business Continuity Management Process

There shall be a managed process for developing and maintaining business continuity plans for all business-critical ICL Pathway processes.

Business continuity planning should involve identifying and reducing the risks from deliberate or accidental threats to vital services.

Plans shall be developed to enable business-critical operations to be maintained following failure of, or damage to, vital services or facilities.

The business continuity planning process includes:

a) identifying and prioritizing business-critical processes,
b) determining the likely impact of disasters on those processes,
c) defining the timescales and minimum service levels for recovery,
d) identifying and allocating the responsibilities and emergency and recovery action,
e) documenting procedures in an easy-to-follow style,
f) educating staff in the execution of the emergency procedures,
g) testing the plans, and

reviewing and updating the plans.

The planning process should focus primarily on keeping business-critical processes and services running, including staffing and other non-computing requirements, rather than just focusing on IT contingency arrangements.

9.1.2 Business Continuity and Impact Analysis

Business continuity shall be based upon analysis of events that can cause interruption to business processes.

Once potentially disruptive events (e.g. equipment failure, flood and fire) have been identified the potential impacts and risks must be assessed, in terms of both scale and recovery period.

A strategic plan should be developed to determine the overall approach to business continuity. ICL Pathway's senior management should endorse this plan.

9.1.3 Writing and Implementing Continuity Plans

Contingency arrangements shall be co-ordinated and reviewed.

System and network managers should ensure that appropriate fallback arrangements are established for all information processing services. This should provide an alternative, temporary means of continuing processing for business-critical systems in the event of damage to, or failure of, equipment.

The business owner of each individual application should specify fallback arrangements, based on a business continuity planning process (see section 9.1.1).

Service providers should coordinate fallback requirements for shared services.

Fallback facilities and procedures must be tested regularly (see section 9.1.5). Operators and users must be prepared for the tasks that they will be expected to carry out in the event of a contingency.

9.1.4 Business Continuity Planning Framework

A consistent framework of business continuity plans shall be maintained.

The ICL Pathway Director of Quality and Risk shall ensure that a single framework of plans is maintained for all business-critical processes and services (see section 2.1).

Each business continuity plan should specify clearly the conditions for its activation, as well as the individuals responsible for executing each component of the plan. New plans should be consistent with established emergency procedures, e.g. evacuation plans, and existing fallback arrangements for computer services, telecommunications and accommodation.

Within the total framework, different levels of plan will be required, because each level will have a different focus and may involve different recovery teams.

The framework should ensure that plans are consistent but do not rely upon common resources. Hence, if two plans are invoked at any time dependency on common resources (which cannot support both plans) should be avoided.

The ICL Pathway business continuity framework should have four main components, as follows:

a) **Emergency Procedures** - which must be executed immediately following a major incident which jeopardizes business operations and/or human life,
b) **Fallback Procedures** - which move essential business activities and/or support services to alternative and temporary footing,
c) **Resumption Procedures** - which returns business operations to their normal state, and
d) **Ttest Schedule** - which specifies how and when the plan will be tested.

Emergency procedures, manual fallback plans, and resumption plans should be the responsibility of the appropriate business process owner. Fallback arrangements for alternative technical services, such as computers and communications, should be the responsibility of the service providers.

9.1.5 Testing Business Continuity Plans

Business continuity plans shall be tested regularly.

Many business continuity plans fail when tested, often because of incorrect assumptions, oversights or changes in equipment or personnel. They should therefore be regularly tested to ensure that they are effective. Such tests should also ensure that the plan is fresh in the minds of all members of the recovery team and other relevant staff.

Those with key roles should be given a list of actions to take in an emergency. They must also have easy access to any other resources that they would need in the event of an emergency.

A schedule for business continuity plan tests should be specified and followed. It should indicate how and when each element of the plan is to be tested.

Components of the plan must be tested frequently in a rolling programme. A full test of the plan must be executed, within a typical business unit, at least one a year.

9.1.6 Maintaining and Re-assessing Business Continuity Plans

Business continuity plans shall be updated regularly.

Business continuity plans must be reviewed whenever there are changes in business processes or in the organisation of business units. The owner of the plan should decide whether it needs updating and testing.

Plan updates should be considered for the following events:

a) IT system upgrade,
b) new IT system installed,
c) staff or organisational change,
d) changes of contractors or suppliers,
e) changes of addresses or telephone numbers,
f) changes to business processes,
g) changes to the applications used,
h) changes in operating practices,
i) changes in legislation.

Plan owners and those with key business continuity roles should meet regularly to review test results and to consider the need for updating plans.

A formal method of change control is needed to ensure that the implications of change are identified and disseminated prior to updating and redistribution of the plan.

10. COMPLIANCE

10.1 Compliance with legal requirements

Objective:	To avoid breaching any criminal or civil law, statutory or commercial obligations that govern the design, operation and use of information processing systems.

The design, operation and use of information processing systems shall be in accordance with statutory and contractual security requirements.

10.1.1 Identification of Applicable Legislation

ICL Pathway shall ensure compliance with all legislative requirements, including the:

- Data Protection Act (1984),
- Computer Misuse Act (1990), and
- Copyright, Designs and Patents Act (1988),

and appropriate sections of the:

- Police and Criminal Evidence Act (PACE),
- Post Office and Telegraph Acts,
- Official Secrets Act 1989,
- Companies Act, and
- relevant EU Directives.

10.1.2 Intellectual Property-rights (IPR)

ICL Pathway shall ensure compliance with legal restrictions on the use of material that is protected by Intellectual Property Rights (IPR), copyright, design rights or trademarks.

Software licenses shall be controlled to ensure that copyright material is not copied without the owner's consent.

Proprietary software products used by ICL Pathway are supplied under licence agreements that can limit the use of the products to specified machines. They may also limit copying to the creation of back-up copies.

Line Managers must ensure that all proprietary software products used within their system or business unit are licensed. They must also ensure that each product is used in accordance with the licence agreement.

Where it is necessary to use a software product on additional machines, licenses should be extended or additional copies purchased.

All licensed software must be recorded in an inventory of assets (see section 3.1.1). Asset records must include the identity of the licence holder. The licence holder must retain proof of purchase and maintain a record of the number of users currently permitted to use the product.

Where users have access to licensed software disks or executable files, they must be advised that these must not be copied except under licence conditions and with the documented authority of the licence holder.

Regular audits of software should be carried out to reconcile installed software and licenses. Any discrepancies must be reported to the IT Security Manager and reconciled as soon as possible.

Copyright infringement by individuals will be treated as a disciplinary offence within ICL Pathway.

10.1.3 Safeguarding of Organisational Records

Important records held by ICL Pathway shall be protected from loss, destruction and falsification.

Within ICL Pathway there are records which need to be securely retained to meet statutory requirements, as well as to support essential business activities.

Typically, records that may be required as evidence that ICL Pathway operates within statutory regulations, and records which relate to the safekeeping of assets entrusted to ICL Pathway, should be protected.

In addition, the Companies Act 1985 requires UK companies to keep their accounting records, and requires adequate precautions to be taken to protect against, and detect, falsification of records.

The owners of such records shall ensure that:

a) an inventory of key information sources is maintained,

b) the storage, handling and disposal of records is defined, and

c) the retention period for each record type is specified.

Where necessary, the IT Security Manager shall advise on measures to be implemented to protect essential records and information from loss, destruction and falsification, in accordance with the ICL Pathway Security Policy.

10.1.4 Data Protection and Privacy of Personal Information

Personal data shall be obtained, used, disclosed and stored in strict accordance with ICL Pathway's registration under the Data Protection Act. The data protection co-ordinator(s) shall manage the registrations and oversee compliance with the Act.

ICL Pathway's data protection co-ordinator(s) shall be responsible for maintaining registration under the Act and dealing with all correspondence with the Office of the Data Protection Registrar.

The data protection co-ordinator(s) shall:

- provide expertise on the requirements of the Act,
- check that systems within ICL Pathway comply with the Act, and
- handle requests from data subjects for access to their personal data.

System Managers are responsible for ensuring that their systems comply with the Act. In particular, they must ensure that personal data is:

- covered by ICL Pathway's registrations,
- relevant, adequate, accurate and up-to-date,
- obtained and processed fairly and lawfully,
- held only for as long as is necessary for specified purposes,
- not be used or disclosed except in line with ICL Pathway's registrations,

- kept secure from unauthorised access, alteration, disclosure, loss or destruction, and
- readily available to data subjects, in an understandable form, should they request access to it.

System Managers must consult a data protection co-ordinator before any change in the collection, use or disclosure of personal data.

Line Managers must ensure that their people are fully aware of their responsibilities under the Act. They should also ensure that compliance with the Act is monitored.

Individual system users must ensure that they are aware of their data protection obligations. Individual infringement of the Act will be treated as a disciplinary offence.

Applications processing personal data on individuals should comply with data protection legislation and principles.

10.1.5 Prevention of Misuse of Information Processing Facilities

ICL Pathway's information processing systems shall only be used for authorised business purposes. Unauthorised use by ICL Pathway personnel shall be treated as a disciplinary offence and unauthorised users may be prosecuted.

ICL Pathway's information processing systems are provided solely for authorised business purposes. They must not be used by anyone other than those authorised by the relevant System Manager (see section 7.1.1).

System Managers must ensure that procedures and controls are implemented so that individuals can be held accountable for their actions (see section 3.1).

Where improper use of ICL Pathway's systems is suspected, the case must be referred for formal investigation (see section 4.3.1).

Unauthorised use by ICL Pathway personnel shall be treated as a disciplinary offence. Serious offenders may be prosecuted under the Computer Misuse Act 1990 that introduced three criminal offences: unauthorised access, unauthorised access with intent to commit a further, serious offence, and unauthorised modification of computer material.

10.1.6 Registration of Cryptographic Controls

ICL Pathway shall ensure that cryptographic facilities are used in strict accordance with national law.

This control applies in all cases where cryptographic hardware and/or software is subject to national controls.

10.1.7 Collection of Evidence

ICL Pathway shall ensure that appropriate precautions are taken wherever evidence needs to be collected.

ICL Pathway shall ensure that information, which might need to be used as evidence to support an action against a person or organisation, is:

- admissible as evidence,
- of sufficient weight, in terms of quality and completeness, and
- adequately protected to preserve accuracy and consistency.

To help ensure admissibility of evidence, ICL Pathway shall ensure that their information systems are operated in accordance with the ICL Pathway Security Policy [SECPOL] and the security management procedures defined in this document.

10.2 Security Reviews of Security Policy and Technical Compliance

Objective:	To ensure compliance with the ICL Pathway Security Policy and standards.

The security of ICL Pathway's information processing systems shall be regularly reviewed.

Reviews should be done against the appropriate security policies, with the technical platforms and information processing facilities checked for compliance with security implementation standards.

10.2.1 Compliance with Security Policy

All areas within the organisation shall be considered for regular review to ensure compliance with security policies and standards.

The high level ICL Pathway Security Policy should be used as a basis for reviews.

The ICL Pathway Access Control Policy (and the related ICL Pathway Security Functional Specification) provide additional specifications for technical compliance checking (see section 10.2.2).

Reviews should include:

a) information systems and systems providers,

b) information and data owners,

c) users, and

d) management.

The ICL Pathway Security Manager should ensure that Owners of information systems (see section 3.1) sponsor regular reviews of the compliance of their systems with the appropriate security policies, standards and any other security requirements.

10.2.2 Technical Compliance Checking

Information processing facilities shall be regularly checked for compliance with security implementation standards.

Technical compliance checking involves the examination of operational systems to ensure that hardware and software security controls have been correctly implemented. This type of compliance checking requires specialist technical assistance. It should be performed manually by an experienced system engineer, or by an automated software package which generates a technical report for subsequent interpretation by a technical specialist.

Such checks should only be carried out by, or under the supervision of, competent persons authorised by the ICL Pathway Security Manager.

The ICL Pathway Access Control Policy (and the related ICL Pathway Security Functional Specification) provide the initial specifications for technical compliance checking. Checks should also be made against more detailed platform specific specifications.

10.3 System Audit Considerations

Objective	To minimize interference to/from the system audit process.

Controls shall be provided to to safeguard operational systems and audit tools during system audits.

Security protection is also required to safeguard the integrity, and prevent misuse of, audit tools.

10.3.1 System Audit Controls

Audits of operational systems shall be planned and agreed.

The ICL Pathway Audit Policy defines the policy for auditing activity on the ICL Pathway solution. It encompasses the business level audit activities and the lower level Security Event Management (SEM).

Audit requirements and activities involving checks on operational systems should be carefully planned and agreed, to minimize the risk of disruptions to business processes. In particular:

a) audit requirements should be agreed with the appropriate Managers,

b) the scope of the checks should be agreed and controlled,

c) the checks should be limited to read-only access to software and data,

d) other types of access (other than read-only) must only be allowed for isolated copies of system files, which should be erased when the audit is completed,

e) IT resources for performing the checks should be explicitly identified and made available,

f) requirements for special or additional processing should be identified and agreed with service providers,

g) all access must be monitored and logged to produce a reference trail, and

h) all procedures, requirements and responsibilities should be documented.

10.3.2 Protection of System Audit Tools

Access to system audit tools shall be safeguarded.

Access to system audit tools (i.e. software or data files) must be safeguarded to prevent any possible misuse or compromise. Such tools should be separated from development and operational systems and not held in disk/tape libraries or user areas, unless given an appropriate level of additional security protection.

ANNEX A DEFINITIONS

The following definitions are those used by British Standard BS 7799.

Expression	Definition
Availability	Ensuring that information and vital services are available to users when required.
Confidentiality	Protecting sensitive information from unauthorised disclosure or intelligible interception.
Data	The representation of facts, concepts, or instructions in a normalized manner suitable for communication, interpretation, or processing by human or by automatic means.
digital signature	a special form of message authentication, usually based on public-key cipher techniques, which provides authentication of the sender, as well as assurance of the integrity of the message content.
Duress alarm	Mechanism by which a *user* can indicate to the host system that a logon is being attempted under duress. Note. An alternative password, or the substitution or inclusion of special characters in a password, could be used to trigger the alarm.
Information	The meaning that is currently assigned to data by means of the conventions applied to that data.
Information security	Protection of information for: a) *confidentiality*: protecting sensitive information from unauthorised disclosure or intelligible interception, b) *integrity*: safeguarding the accuracy and completeness of information and computer software, c) *availability*: ensuring that information and vital services are available to users when required.
Information security management	Provision of a mechanism to enable the implementation of *information security*.
Information technology (or IT)	The scientific, technological and engineering discipline and the management of techniques used in data handling and processing, their applications, computers and their interactions with people and machines, and associated social, economic and cultural matters.
Integrity	Safeguarding the accuracy and completeness of information and computer software.
Organisation	Group of people collectively responsible for a defined set of activities. e.g. a company, a local authority, an academic institution.
Owner	Individual or organisation having responsibility for specified information asset(s) and for the maintenance of appropriate security measures.

risk analysis	Comprehensive concept for defining and analysing threats to, and vulnerabilities of, computer system assets and capabilities, and for supplying management with information suitable for a (risk management) decision in order to optimize investment in security countermeasures.
Security incident	Any event that has, or could have, resulted in loss or damage to organisational assets, or an action that is in breach of organisational security procedures.
Special privilege	Any feature or facility of a multi-user IT system that enables a *user* to override system or application controls.
User	Individual or organisation that makes use of *information technology*.

ANNEX B INFORMATION SECURITY OVERVIEW

The overview presented in this Annex is essentially the introductory information provided by BS7799. It has been included to help readers, who may not be familiar with the subject, understand the rationale behind both BS7799 and these ICL Pathway Security Management Procedures.

Definitions for the words in *italics* have been included in Annex A.

What is information security?

The purpose of *information security* is to ensure business continuity and minimize business damage by preventing and minimizing the impact of security incidents. Information security management enables information to be shared, while ensuring the protection of information and computing assets. It has three basic components:

a) **confidentiality** - protecting sensitive information from unauthorised disclosure or intelligible interception,

b) **integrity** - safeguarding the accuracy and completeness of information and computer software,

c) **availability** - ensuring that information and vital services are available to *users* when required.

Information takes many forms. It can be stored on computers, transmitted across networks, printed out or written down on paper, and spoken in conversations. From a security perspective, appropriate protection should be applied to all forms of information, including papers, databases, films, view foils, models, tapes, diskettes, conversations and any other methods used to convey knowledge and ideas.

Why action is needed

Information and the IT systems and networks that support it are important business assets. Their availability, integrity and confidentiality may be essential to maintain a competitive edge, cash-flow, profitability, legal compliance and respected organisation image.

Any organisation may now be facing increasing security threats from a wide range of sources. Its IT systems and networks may be the target of a range of serious threats, including computer-based fraud, espionage, sabotage, vandalism and other sources of failure or disaster. New sources of damage, such as the highly publicized threats of computer viruses and computer hackers, continue to emerge. Such threats to information security are expected to become more widespread, more ambitious and increasingly sophisticated. At the same time, because of increasing dependence on IT systems and services, organisations may be becoming more vulnerable to security threats. The growth of networking presents new opportunities for unauthorised access to computer systems and the trend to distributed computing reduces the scope for central, specialist control of IT facilities.

Security measures are considerably cheaper and more effective if incorporated into IT systems and services at the requirements specification and design stages. The sooner any organisation takes action to safeguard its information systems, the cheaper and more effective it will be for that organisation in the long run.

Are all the controls applicable?

Some controls in BS7799 are not applicable to every IT environment and should be used selectively, according to local circumstances. The descriptions of these controls make this clear[2]. However, most of the controls documented are widely accepted by large, experienced organisations as recommended good practices for all situations, subject of course to limiting factors such as environmental or technological constraints. These generally accepted controls are often referred to as baseline security controls, because they collectively define an industry baseline of good security practice.

Ten of the controls in this BS7799 code of practice (designated key controls) are considered to be especially important. These key controls provide a good starting point for information security management.

A few controls (e.g. data encryption) may require specialist security advice and an assessment of risks to establish if they are required, and to determine how they should be implemented. In some cases, further (stronger) controls, outside the scope of the BS7799 code of practice, may be required to provide enhanced protection for especially valuable assets or to counter exceptionally high levels of security threat.

How to establish your security requirements

There are three main sources of security requirements in any organisation.

The first source of security requirements is the unique set of security risks, comprising both threats and vulnerabilities, to assets and the potential impact of these security risks on business. Most of these risks are addressed and can be effectively countered by using the guidance in this BS7799 code of practice. However, there will be some risks that require special treatment, and these will need to be addressed by risk assessment of each individual organisation or component system.

The second source of requirements is the set of statutory and contractual requirements that an organisation, its trading partners, contractors and service providers have to satisfy, with an increasing need for standardisation as inter-organisational networking proliferates. This BS7799 code of practice is intended to serve as a consistent reference point for generic requirements of this type.

The third source of requirements is the unique set of principles, objectives and requirements for information processing that an organisation has developed to support its business operations. It is important (e.g. for a competitive edge) that the security policy supports these requirements, and vital that the implementation, or absence, of security controls in the IT infrastructure does not impede efficient business operations.

Incorporation of the right controls and the required degree of flexibility from the start of the IT planning process is critical to the successful outcome of the work.

Assessing your security risks

Expenditure on IT security controls needs to be balanced against, and appropriate to, the business value of the information and other IT assets at risk, and the business harm likely to result from security failures. A periodic review of business risks and IT security controls, to address changing business requirements and priorities, is therefore a regular feature of information security management.

[2] Those not applicable to ICL Pathway have been identified and alternative text has been provided in the relevant sections of this document.

Generally, *risk analysis* techniques are applied to complete information systems and facilities, but they can also be directed to individual system components or services where this is practicable, realistic and helpful. Assessment of risks involves systematic consideration of the following items:

a) the business harm likely to result from a significant breach of IT security, taking account of the potential consequences of failures of information confidentiality, integrity and availability, and

b) the realistic likelihood of such a breach occurring in the light of prevailing threats and controls.

The results of this assessment will help to guide and determine the appropriate management action and priorities for managing information security risks and for implementing the controls recommended in this BS7799 code of practice. Assessment of these two aspects of risk depends upon the following factors:

- the nature of the business information and systems,
- the business purpose for which the information is used,
- the environment in which the system is used and operated, and
- the protection provided by the controls in place.

The risk assessment might identify exceptional business security risks requiring stronger controls that are additional to the recommendations given in this standard. These controls will need to be justified on the basis of the conclusions of the risk assessment.

Critical success factors

Experience has shown that the following factors are often critical to the successful implementation of information security within an organisation:

a) security policy, objectives and activities that reflect business objectives

b) an approach to implementing security that is consistent with the organisational culture,

b) visible support and commitment from top management,

c) a good understanding of the security requirements, risk assessment and risk management,

d) effective marketing of security to all managers and employees,

d) distribution of guidance on information security policy and standards to all employees and contractors,

e) providing appropriate training and education, and

f) an effective system of measurement which is used to evaluate performance in information security management and feedback suggestions for improvement.

Developing your own guidelines

There is no single best structure for security guidance. Each category of user or IT specialist in a particular environment will have a different set of requirements, problems and priorities depending on the particular function, organisation and business or computing environment.

Many organisations have addressed this problem by developing a portfolio of individual interpretation guides for particular groups of employees, to ensure more effective dissemination of security guidance.
Organisations that decide to adopt a different structure (or perhaps develop a local interpretation guide[3]) are advised to retain cross-references

[3] ICL Pathway has adopted this approach with the production of this set of Security

[4] to the text of this BS7799 code of practice to enable future business partners or auditors to establish a direct link between it and organisational security guidelines.

Management Procedures.

[4] By retaining the same basic structure as BS7799, there is very close mapping between the section numbers and section headings used in both documents.