

ICL Pathway

ICL SECURITY POLICY
COMMERCIAL IN-CONFIDENCE

Ref: RS/POL/002
Version: 6.0
Date: 20/11/00

Document Title: ICL PATHWAY SECURITY POLICY

Document Type: Policy Document

Release: Not Applicable

Abstract: This Security Policy specifies mandatory security requirements to be applied throughout ICL Pathway

Document Status: APPROVED

Originator & Dept: Peter Harrison (Graham Hooper) – Quality Risk Management

Contributors: Graham Hooper, Geoffrey Vane, Alan D'Alvarez, Rob Arthan
John Coakes

Reviewed By: Graham Hooper, Martyn Bennett, Geoffrey Vane, Alan
D'Alvarez, Peter Jeram, John Coakes, Jim Flynn, Graham
Chatten, Ian Morrison, Steve Doyle, Lorraine Holt, Chris
Humphries, Chris Wannell, Martin Riddell, Peter Burden, Paul
Westfield, Gill Jackson, Mike Stares, Tony Oppenheim, Terry
Austin, John Dicks, Stephen Muchow

Comments By:

Comments To: Document Controller & Graham Hooper

Distribution: Graham Hooper, Martyn Bennett, Lorraine Vaughan, Geoffrey
Vane, Alan D'Alvarez, Peter Jeram, John Coakes, Jim Flynn,
Graham Chatten, Ian Morrison, Steve Doyle, Lorraine Holt,
Chris Humphries, Chris Wannell, Martin Riddell, Peter Burden,
Paul Westfield, Gill Jackson, Mike Stares, Tony Oppenheim,
Terry Austin, John Dicks, Stephen Muchow

0.0 Document Control

0.1 Document History

Version No.	Date	Reason for Issue	Associated CP/Pin/ICL No.
0.1	27/5/96	Initial draft issued for comments	
0.2	31/5/96	Revised draft issued for comments	
0.3	26/6/96	Incorporates comments from the ICL Pathway Management team	
1.0	16/8/96	Incorporates comments from DSS/BA and POCL	
2.0	23/9/96	Incorporates further comments from Authority	
3.0	8/10/96	Approved	
3.1	24/11/97	Revised for internal review purposes	
3.2	10/01/98	Incorporates comments from internal review	
3.3	23/2/98	Incorporates further comments	
3.4	28/9/98	Minor updates	
4.0	30/4/99	Approved	
4.1	24/6/99	Removal of references to DSS/Benefits Agency relating to Contract changes.	
4.2	03/10/00	Incorporates changes following internal review and re-organisation of responsibilities.	
5.0	13/11/00	Approved	
5.1	20/11/00	Incorporates clarification in respect of DPA and OBCS.	
6.0	20/11/00	Approved	

0.2 Approval Authorities

Name	Position	Signature	Date
Mike Stares	Managing Director		
Tony Oppenheim	Director Commercial and		

ICL Pathway

ICL SECURITY POLICY
COMMERCIAL IN-CONFIDENCERef: RS/POL/002
Version: 6.0
Date: 20/11/00

	Finance		
Terry Austin	Director Development		
Martyn Bennett	Quality and Risk Director		
John Dicks	Customer Requirements Director		
Steve Muchow	Customer Requirements Director		

0.3 Associated Documents

Reference	Version	Date	Title	Source
	2.0	1/5/92	ICL Group Security Policy	ICL
	1.2	17/9/99	ICL Pathway Security Management Procedures	ICL Pathway
	3.3	11/2/00	ICL Pathway Access Control Policy	ICL Pathway
			Post Office Information Systems Security Policy Document (KH2879)	POCL
			Post Office Counters Information Systems Security Policy (SSR Appendix 4-1)	POCL
	1.5	28/10/94	A Code of Practice for PO Information Systems Security	POCL
	2.0	15/5/99	BS7799 - A Code of Practice for Information Security Management	BSI
	5.2	29/10/99	System Architecture Design Document	ICL Pathway

0.4 Abbreviations/Definitions

Abbreviation	Definition
APS	Automated Payment Services
CESG	Communications-Electronics Security Group
CLEF	Commercial Licensed Evaluation Facility
COTS	Commercial Off The Shelf

ICL Pathway

ICL SECURITY POLICY
COMMERCIAL IN-CONFIDENCERef: RS/POL/002
Version: 6.0
Date: 20/11/00

DSS	Department of Social Security
EPOSS	Electronic Point Of Sale Service
OBCS	Order Book Control Service
PFI	Private Finance Initiative
PPP	Public Private Partnership
POCL	Post Office Counter Limited

0.5 Changes in this Version

Version	Changes
5.1	Clarification that compliance with DPA relates to the 1984 Act and amendment in respect of EPOSS.
6.0	Approved

0.6 Changes Expected

Changes

0.7 Table of Contents

1	Foreword.....	7
2	Introduction.....	8
	2.1 Service Overview.....	8
	2.2 Scope.....	8
	2.3 Policy Review.....	9
3	Objectives.....	9
	3.1 Business Objectives.....	9
	3.2 IT Security Objectives.....	10
	3.3 Legal Obligations.....	11
4	Responsibilities For Security.....	11
	4.1 Director, Quality Management.....	11
	4.2 ICL Pathway Security Board.....	12
	4.3 Security Manager.....	12
	4.4 Security Administration.....	13
	4.5 Responsibilities for Physical Security.....	13
	4.6 All Personnel.....	13
	4.7 Reporting Security Incidents.....	14
5	Responsibilities For Audit.....	14
	5.1 Audit Manager's Responsibilities.....	14
	5.2 Business Function Monitoring Responsibilities.....	15
	5.3 Security Event Management Responsibilities.....	15
6	Personnel Security.....	16
	6.1 Recruitment Selection.....	16
	6.2 Job Descriptions, Contracts and Assessment.....	16
	6.3 Security Education and Training.....	16
7	Implementation Policies.....	17
	7.1 Information Classification.....	17
	7.2 Safeguarding POCL Records.....	17
	7.3 Physical and Environmental Security.....	17
	7.4 System Access Control.....	18
	7.5 Cryptography.....	18

8	Administration of Security.....	19
	8.1 System and Network Management.....	19
	8.2 Audit Management.....	19
	8.3 Systems Development and Maintenance.....	19
	8.4 Malicious Software Control Policy.....	20
	8.5 Information Exchange Control.....	20
	8.6 Control of Proprietary Software.....	21
	8.7 External Contractors and Suppliers.....	21
9	Business Continuity.....	21
	9.1 Contingency Planning.....	21
	9.2 Testing Contingency Plans.....	22
	9.3 Subcontractor's Contingency Plans.....	22
10	Compliance.....	22
	10.1 Compliance with ICL Pathway's Security Policy.....	22
	10.2 Compliance with Legislative Requirements.....	22
	10.3 Compliance with BS7799.....	23

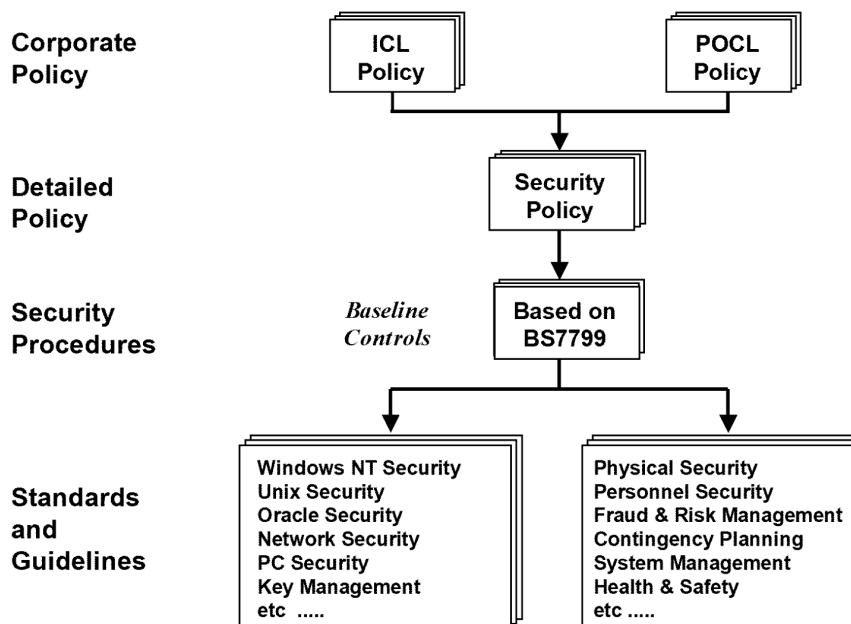
1 Foreword

This document defines ICL Pathway's policy for the protection of its assets (including hardware, applications, databases, network, people and documentation) against loss of confidentiality, integrity and availability. It also enables ICL Pathway to comply with legislative and commercial requirements.

ICL Pathway's policy statement (which is essentially the same as the Corporate Policy statement used by the ICL Group) is:

It is the policy of ICL Pathway Limited to provide a secure working environment for the protection of employees, and also to ensure the security of all assets owned by or entrusted to ICL Pathway.

This document fits into the structure illustrated below, with the BS7799 Code of Practice being used as a basis for ICL Pathway's Security Procedures. Lower level implementation standards will be incorporated as appropriate.



ICL Pathway's Security Policy, Procedures and Standards

2 Introduction

In May 1996, ICL Pathway Limited was selected to set up and operate the services to automate counter transactions at Post Offices throughout the UK.

The requirement to implement a Benefit Payment Service for the Benefit Agency was removed when the UK Government's major Private Finance Initiative (PFI) project was changed to a Public Private Partnership (PPP) project during 1999.

The purpose of this policy document is to lay the foundation that will enable ICL Pathway to protect the integrity, availability and confidentiality of all assets associated with the services. It also enables ICL Pathway to comply with legislative and commercial requirements.

2.1 Service Overview

The agreement is a PPP project, whereby ICL Pathway will automate 20,000 Post Offices and provide the infrastructure which enables users to make automated payments at outlets throughout the UK.

Computerised facilities at Post Office counters enable a range of Automated Payment Services (APS) to be provided, allowing customers to make payments to utilities and other clients supported by Post Office Counters Limited (POCL).

The Electronic Point Of Sale Service (EPOSS) supports all services, or products, provided by the counter clerk to the customer.

The Order Book Control Service (OBCS) is a discrete counter application, transactions in respect of which are recorded via EPOSS.

The services are designed to provide secure payment facilities, hence particular attention is focused upon the security aspects of the services throughout their life cycle.

2.2 Scope

This Security Policy specifies mandatory security requirements to be applied throughout ICL Pathway.

ICL Pathway has overall responsibility for the design, development, implementation, roll-out, operation and support of the service throughout the contract period. Specific activities will be subcontracted to appropriate organisations, which will be required to work within the security framework defined by ICL Pathway.

ICL Pathway's Security Policy must be compatible with POCL Security Policy. The interfaces between ICL Pathway and all external organisations must be clearly defined and formally agreed with the organisations concerned.

Security obligations for subcontractors involved in development activities (including Escher, Oracle and ICL) will be subject to individual agreements

with ICL Pathway. Commercial off the shelf (COTS) products will be provided by the appropriate product suppliers (including Microsoft).

2.3 Policy Review

Once approved, this policy document will be formally reviewed at least annually and after any significant security incident or occurrence of fraud, and updated whenever necessary.

Responsibilities for approval, review and issue of ICL Pathway's Security Policy and Procedures are defined in section 3.

3 Objectives

This document provides a definition of ICL Pathway's high-level Security Policy.

ICL Pathway will establish an infrastructure that will minimise and control liabilities to itself and POCL.

The Security Policy defines the requirements for Pathway enabling it to protect the integrity, availability and confidentiality of information used and produced by the services. This includes making adequate provision for:

- Business Continuity, and
- compliance with relevant legislation.

The responsibilities for policy implementation are defined (in section 3) in order that the policy requirements can be communicated throughout ICL Pathway. This will ensure that all parties are fully aware of their responsibilities and legal obligations.

ICL Pathway has stated its commitment to ensuring that it encompasses the very best commercial practices for security. ICL Pathway's aim is to be fully compliant with BS7799.

Compliance with legislative requirements (including the Data Protection Act 1984) and BS7799 is considered under "Compliance" (in section 9).

3.1 Business Objectives

The business Objectives are:

1. Identifying and managing risks
2. Protection of information assets
3. Protection of IT assets
4. Provide continuity of services
5. Maintenance of ICL Pathway's reputation.

3.2 IT Security Objectives

ICL Pathway's overall IT security objective can be summarised as achieving the requirement expressed in the following policy statement:

It is the policy of ICL Pathway Limited to protect its investment in IT assets, and to ensure the confidentiality, integrity and availability of all information conveyed, processed or stored, by the services.

1. Security measures in ICL Pathway's IT systems will ensure appropriate confidentiality, integrity and availability of services, software components and data, whether in storage or in transit.
2. Physical and logical access to the IT systems will be controlled, with access granted selectively, and permitted only where there is a specific need. Access will be limited to persons with appropriate authorisation and a "need to know" requirement.
3. Authentication, whereby a user's claimed identity is verified, is essential before any access is granted to any IT system. Authentication mechanisms are also required to ensure that trust relationships can be established between communicating components within, and external to, ICL Pathway's services.
4. All users of ICL Pathway's services will be individually accountable for their actions. Accountability for information assets will be maintained by assigning owners, who will be responsible for defining who is authorised to access the information. If responsibilities are delegated then accountability will remain with the nominated owner of the asset.
5. Audit mechanisms are required to monitor, detect and record events that might threaten the security of the ICL Pathway services or any service(s) to which it is connected. Regular analysis of audit trails is essential to facilitate the identification and investigation of security breaches.
6. Alarm mechanisms are required to alert security personnel to the occurrence of security violations that could seriously threaten the secure operation of ICL Pathway's services. These alarms will be used to trigger prompt investigation and remedial action in order to minimise the impact of any security breach.
7. ICL Pathway will monitor all developments and operations to maintain assurance that its services are performing in accordance with approved security procedures and controls. This will give a high level of confidence that all information is being protected during processing, transmission and storage.

3.3 Legal Obligations

ICL Pathway must remain fully compliant with all relevant legislation and regulations.

In addition to the existing legislative obligations, identified in section 9.2, it is important to track and anticipate emerging UK and European regulations that could affect ICL Pathway's operation.

4 Responsibilities For Security

ICL Pathway's Managing Director has ultimate responsibility for security.

ICL Pathway's commitment to security will be communicated throughout ICL Pathway, as evidenced by board level approval of ICL Pathway's Security Policy.

Figure 1 illustrates the security organisation used within ICL Pathway. Senior management is supported by experienced specialists and technical staff with specific expertise in the areas of IT, security, fraud prevention and risk management.

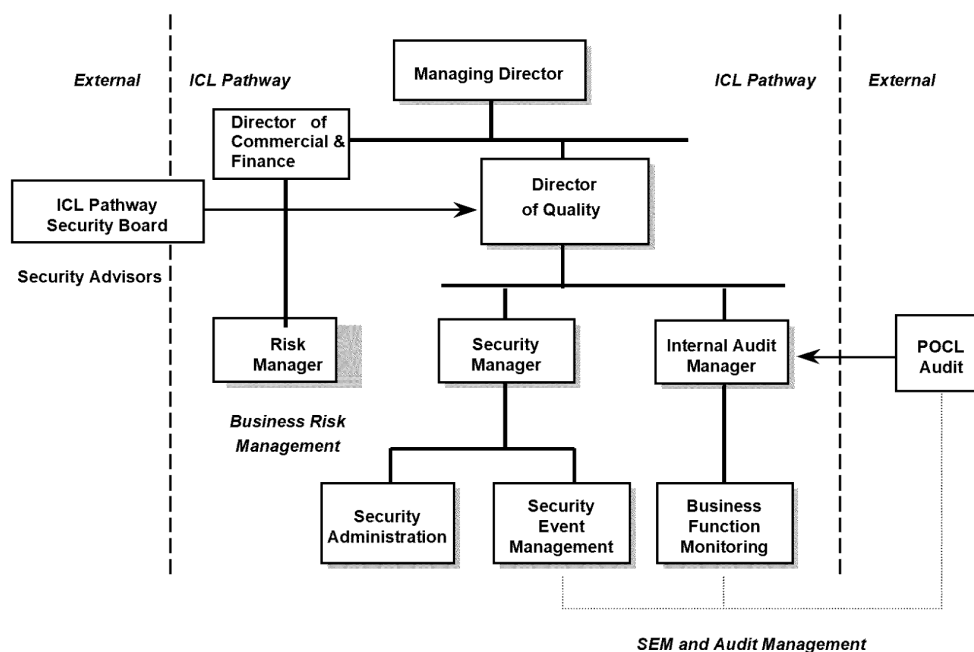


Figure 1 ICL Pathway's Security Management Structure

4.1 Director, Quality Management

The responsibilities of the Director, Quality Management, include:

- overall control and management of security throughout ICL Pathway,
- provision of adequate resources for security,
- being Chairman of the ICL Pathway Security Board (see section 3.2),
- owner of ICL Pathway's Security Policy,

-
- approval authority for ICL Pathway's Security Policy,
 - approval authority for ICL Pathway's Security Procedures,
 - overall control of risk management functions,
 - establishing the security interface with POCL, and
 - establishing the security interface with all subcontractors.

4.2 ICL Pathway Security Board

The representatives on ICL Pathway's Security Board are nominated by the Director, Quality Management, and approved by the ICL Pathway Board.

The Security Board participants, which will include 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.

4.3 Security Manager

The Security Manager is responsible for ensuring implementation of policy and procedures, and maintaining "best practice", within the remit of ICL Pathway.

ICL Pathway's Security Manager's responsibilities include:

- physical and environmental security,
- monitoring for compliance with ICL Pathway's Security Policy,
- providing the point of contact for reporting all types of security incidents,
- ensuring that security incidents are recorded and investigated,
- ensuring that security relevant events are recorded,
- ensuring that system audit trails are analysed on a regular basis,
- documentation of ICL Pathway's Security Policy,
- owner of ICL Pathway's Security Procedures,
- documentation of ICL Pathway's Security Procedures,
- communication of security policy and procedures throughout ICL Pathway,
- authorisation and approval for system changes,
- co-ordinating the evaluation of all new security products proposed,
- specifying and arranging security education and training,
- devising and conducting security awareness programmes,

-
- maintaining a partnership approach to security with Horizon Security Liaison staff,
 - liaison with POCL and suppliers' security personnel, and
 - recruitment selection of security administration personnel.

4.4 Security Administration

The description "Security Administration" has been 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 in section 3.3.

Wherever possible, Security Administrators will act in a supporting or monitoring role rather than as a Service Provider for the operational services. In this capacity they can:

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

4.5 Responsibilities for Physical Security

The local Site Managers have responsibility for physical security at all sites used by ICL Pathway.

At some sites, notably Data Centres and support sites, ICL Pathway can benefit from existing security infrastructure in order to protect against threats from physical and environmental sources.

At Post Office outlets, the Post Office Manager has particular responsibility for safeguarding the ICL Pathway equipment installed.

4.6 All Personnel

All service users, most of whom will be at Post Office counters, will be included in ICL Pathway's awareness and/or training programmes. Security aspects, an integral part of these programmes, will be set in a context appropriate to the user's role (for example, Post Office Manager or clerk).

All ICL Pathway employees, subcontractors and system users have security responsibilities and they will be required to work together in support of this security policy. Personnel who may not regard themselves as any kind of "system user" will still have security responsibilities. In particular, they are expected to be vigilant in reporting anything they believe may be suspicious.

Promoting security awareness, throughout ICL Pathway, to subcontractors, and within Post Offices, is an important responsibility assigned to ICL Pathway's Security Manager.

Publicising security reporting and escalation procedures will be part of this awareness strategy.

4.7 Reporting Security Incidents

ICL Pathway will establish effective procedures for reporting, acting upon and escalating all incidents that could affect security. It is the responsibility of all users of the ICL Pathway services and ICL Pathway personnel to use these procedures.

ICL Pathway's Security Manager is responsible for ensuring that all incidents are recorded, investigated and resolved with appropriate urgency. This will include liaison with Horizon Security Liaison staff to review incidents and actions.

5 Responsibilities For Audit

The Director, Quality Management, is accountable for the Audit function within ICL Pathway, as illustrated in figure 1.

The Audit Manager's responsibilities, listed in section 4.1, are primarily concerned with managing the internal Audit function within ICL Pathway but they also include liaison with POCL audit personnel.

As the point of contact with external audit personnel, the Audit Manager will need to maintain regular contact with many ICL Pathway groups (e.g. Customer Service, Programmes, Commercial and Finance) to co-ordinate audit related activities.

The Security Event Management function, illustrated in figure 1, encompasses the routine IT Security activities concerned with security relevant events recorded by ICL Pathway's systems. It is really part of the day-to-day security administration activity, but has been highlighted to identify the need for regular analysis of event logs.

5.1 Audit Manager's Responsibilities

ICL Pathway's Audit Manager is responsible for ensuring implementation of ICL Pathway's Audit Policy and maintaining "best practice", within the remit of ICL Pathway.

The Audit Manager's responsibilities include:

- planning and carrying out audits of ICL Pathway's business functions,
- examining and evaluating the results of (business function) audits,
- developing and agreeing improvement programmes,

-
- monitoring and reporting improvement activities,
 - monitoring for compliance with ICL Pathway's Audit Policy,
 - providing the point of contact for all audit related matters,
 - overall responsibility for ICL Pathway's Audit activities,
 - documentation of ICL Pathway's Audit Policy,
 - being the owner of ICL Pathway's Audit Standards,
 - documentation of ICL Pathway's Audit Standards,
 - communication of Audit policy and standards within ICL Pathway,
 - co-ordinating the evaluation of all new audit products proposed,
 - specifying and arranging Audit education and training,
 - liaison with POCL audit personnel,
 - liaison with ICL Group Audit personnel, and
 - recruitment selection of Audit personnel.

5.2 Business Function Monitoring Responsibilities

The description "Business Function Monitoring" has been used to describe ICL Pathway personnel assigned to roles with particular responsibility for Audit.

ICL Pathway's Audit Manager is the normal line manager for this group, hence many of the activities assigned to Business Function Monitoring will be to support the functions listed in section 4.1.

Wherever possible, Business Function Monitoring will act in a supporting role rather than as a Service Provider for the operational services. In this capacity they can:

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

5.3 Security Event Management Responsibilities

The description "Security Event Management" has been used to describe ICL Pathway personnel assigned to roles with particular responsibility for security relevant events recorded by ICL Pathway's systems.

ICL Pathway's Security Manager is the normal line manager for this group, hence many of the activities assigned to Security Event Management personnel will be supporting functions.

Wherever possible, Security Event Management will act in a monitoring role supporting the audit related security administration activities. In this capacity they can:

- ensure that specified events are being audited on the relevant platforms,

-
- ensure that all access (and attempted access) to ICL Pathway's systems is audited,
 - monitor usage by ICL Pathway operations and management staff,
 - analyse the audit logs generated by the different ICL Pathway platforms,
 - assist with investigations (as assigned by the Security Manager),
 - extract copies of audit information for investigation purposes,
 - ensure that archived audit information is being stored securely,
 - implement ICL Pathway's Security Procedures (particularly with regard to audit),
 - report actual and suspected security incidents, and
 - recommend changes, to enhance ICL Pathway's security controls, to the Security Manager.

6 Personnel Security

Staff concerned with the operations and management of central services are to be managed under the guidance of ICL's Personnel Policy Manual and associated documents.

Staff working on high-risk areas in the organisation (those classified as "sensitive") are to be subject to more frequent vetting reviews and internal audits. This applies to ICL Pathway's own employees and to staff from subcontractor's organisations.

6.1 Recruitment Selection

All applicants will be subject to an appropriate level of vetting, using criteria approved and provided by ICL Group Security. This will include checks on their identification and financial circumstances.

Business and personal references will be checked for all applicants.

6.2 Job Descriptions, Contracts and Assessment

ICL Pathway will apply best commercial practice, based upon BS7799, to include security considerations within:

Employees Terms and Conditions for Employment, and generic job descriptions.

6.3 Security Education and Training

ICL Pathway's education and training programme will promote security awareness and explain the importance and use of security controls.

The programme will include:

- all ICL Pathway employees,
- training for all system users, tailored to their particular role, and
- appropriate training for contractors and third parties.

7 Implementation Policies

The following subsections provide an overview of the controls required for:

- asset classification and control,
- physical and environmental security, and
- system access control.

ICL Pathway's Security Procedures will provide more detailed guidance based upon the corresponding BS7799 sections. This will include the provision and maintenance of an asset register.

7.1 Information Classification

All information used by ICL Pathway will be handled in accordance with its classification, as specified by its owner. Information owners are required to classify all information that they own, in accordance with a process that will be jointly agreed.

The sensitivity of information will be measured by the consequences of a potential security breach associated with that information.

ICL Pathway will assume that aggregation cannot increase the classification of any information.

ICL Pathway's Security Procedures will include guidance on protective marking and handling of information.

7.2 Safeguarding POCL Records

ICL Pathway will protect all manual and electronic records supplied by POCL in accordance with agreed contractual obligations. The records will be safeguarded from unauthorised disclosure, modification, loss, destruction and falsification.

7.3 Physical and Environmental Security

Use of existing secure computing facilities for ICL Pathway's central services will simplify the task of establishing secure areas for the protection of IT facilities. The physical security measures will include:

- specialist site security staff in attendance 24 hours per day,
- surveillance and intruder detection systems,
- multi-zone areas controlled by a card access system, and
- regular security reviews and audit checks.

All equipment and cabling will be well maintained and protected against environmental hazards, including fire and water damage.

Post Offices pose some significant challenges for several reasons:

- ICL Pathway will use approximately 20,000 sites throughout the UK,
- ICL Pathway cannot control the physical security at Post Offices,

-
- ICL Pathway owns the IT assets installed in each Post Office,
 - high specification commercial PCs will be installed at each site,
 - ICL Pathway cannot vet or select Post Office personnel, and
 - changes to the Post Office operating environment can occur.

The security measures associated with installed equipment will take these factors into consideration to reduce ICL Pathway's risks to an acceptable level.

7.4 System Access Control

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

The Access Control Policy and associated Security Procedures will specify:

- a clear definition of responsibilities for all authorised users,
- specification of roles and responsibilities for all types of system usage,
- control of access to all ICL Pathway systems components,
- control of access to all data within the ICL Pathway systems,
- control of access to all stored information and documentation,
- control of access to database facilities and tools,
- control of access to applications running on servers and workstations,
- control of access to the network and network management systems,
- procedures for allocation of access rights to IT systems,
- management, assignment and revocation of privileges,
- identification and authentication of human and system "users", and
- password management, including password generation and expiry.

Accountability of individuals is essential and segregation of duties will be enforced where appropriate.

Wherever authorisation is given orally, normally over a telephone link, additional verification methods must be used.

7.5 Cryptography

ICL Pathway will comply with Government Policy with regard to the protection of Government Data.

ICL Pathway will seek the guidance of Communications-Electronics Security Group (CESG) on all matters concerning cryptography. This includes:

- choice of encryption algorithms,
- strength of mechanisms,
- encryption of information stored on disks within Post Offices, and
- encryption key management (including key generation, distribution and change).

8 Administration of Security

The following subsections provide an overview of the controls required within ICL Pathway's organisation. ICL Pathway's Security Procedures will provide further guidance, based upon the BS7799 controls, for:

- computer and network management, and
- system development and maintenance.

8.1 System and Network Management

Operational control of ICL Pathway's services will be managed by a central System Support unit responsible for system and network management.

The system privileges and access permissions required to perform management functions are considerably higher than those assigned to normal users. ICL Pathway will therefore ensure that:

- staff assigned to management functions are carefully selected,
- physical and logical access controls are clearly defined and rigorously implemented,
- individuals are not granted unnecessary privileges,
- separation of duties is achieved whenever appropriate,
- individuals are held accountable for all system changes,
- the ability to grant and modify access permission is controlled, and
- all significant system changes are recorded.

8.2 Audit Management

ICL Pathway will ensure that:

- all security critical events are time stamped and recorded,
- auditable events are carefully selected to minimise overheads,
- audit trail information is protected from modification,
- audit trails include a record of all significant system changes,
- effective audit analysis reduction and analysis tools are used,
- all observed system irregularities are investigated, and
- audit trails are archived and stored for an agreed duration.

8.3 Systems Development and Maintenance

ICL Pathway will ensure that system security, considered at the requirements analysis stage, fully reflects the business value of the information assets involved. The analysis will consider:

- identification and authentication of human and system "users",
- control of access to information and services,
- segregation of duties,
- secure operation in degraded mode,
- incorporation and analysis of audit trails,
- data and system integrity protection,

-
- use of encryption to prevent unauthorised disclosure of data, and
 - system resilience, including operation in fall-back mode and recovery.

All software developed by or for ICL Pathway will be specified and implemented using proven methodologies, taking care to ensure that:

- input data validation is comprehensive and reliable,
- processing protects against errors and attacks, and
- integrity checking is performed where appropriate.

ICL Pathway will ensure that software development activities are fully supported by procedures and standards that cover all aspects of the development process. Audits and reviews will be conducted to ensure that the procedures are being applied effectively and that the supporting documentation meets approved standards. Security testing will provide confirmation that the security functionality of the systems has been implemented to meet the agreed security specifications.

Assurance during development will be supported by the definition of security requirements, security architecture, detailed security design, design reviews and security testing.

Design and specification changes will be reviewed to ensure they do not compromise the security of the systems.

All software will be subject to appropriate acceptance procedures prior to integration with other components.

8.4 Malicious Software Control Policy

ICL Pathway will analyse threats associated with malicious software and, where appropriate, will implement effective controls. These controls will include virus prevention, virus detection and appropriate user awareness procedures.

8.5 Information Exchange Control

ICL Pathway will define, agree and enforce (with relevant parties) procedures for the exchange of information handled electronically and by other means. The procedures used will comply with legal and contractual requirements and will depend upon the sensitivity of the information.

In particular, the exchange of information, with POCL, will be subject to formally agreed controls.

8.6 Control of Proprietary Software

Proprietary software will only be used within the terms of the licence conditions.

Unauthorised copying of software and documentation will be prohibited.

ICL Pathway will not permit any modified or non-standard software components to be incorporated unless the modifications have been applied and validated by the normal supplier, and approved by ICL Pathway's Security Manager.

ICL Pathway's configuration management system will maintain an inventory of all proprietary software used by their services.

8.7 External Contractors and Suppliers

ICL Pathway will ensure that appropriate safeguards cover the use of external contractors and suppliers. This will include agreements with contractual terms and conditions and checks on the integrity of external contractors before any work is assigned to them.

External personnel will not be allowed access to any classified information without prior written authority from the information owner and completion of a non-disclosure agreement.

Suppliers of goods and services (including Escher and Oracle) will be subject to formal agreements in support of this security policy. Individual agreements with suppliers of standard COTS components are not required.

Evidence of the adequacy of suppliers' security procedures will be sought where externally supplied goods or services are used to process critical and/or sensitive information.

9 Business Continuity

ICL Pathway will ensure that an effective business continuity plan is agreed with Horizon Security Liaison staff and implemented to reduce the risks from deliberate or accidental threats to deny access to vital services or information.

Plans will be developed to enable internal operations and business services to be maintained following failure or damage to vital services, facilities or information. All relevant security provisions will be maintained, even if degraded conditions are in effect.

9.1 Contingency Planning

In order to minimise any disruption to the services managed by ICL Pathway, contingency plans will be developed to encompass:

- handling emergency situations,
- operating in fall-back mode, and
- recovery (or Business Resumption) to full operational status.

9.2 Testing Contingency Plans

All contingency plans will be tested on a regular basis under representative operational conditions.

9.3 Subcontractor's Contingency Plans

Contingency arrangements will be examined and managed to ensure that risks are minimised, wherever ICL Pathway is dependent upon subcontractors (or third parties), for essential services or supplies.

10 Compliance

ICL Pathway is required to comply with legislative requirements and commercial standards.

10.1 Compliance with ICL Pathway's Security Policy

Compliance with the requirements defined in this Security Policy is mandatory. The policy is to be applied throughout ICL Pathway for the secure management and operation of the services.

Periodic reviews will be carried out, under the direction of ICL Pathway's line managers, to verify that ICL Pathway is operating in accordance with its security policy and procedures.

ICL Pathway's Audit function (see section 4) will provide the essential monitoring activities needed to provide senior management with visibility that ICL Pathway is operating in accordance with this policy.

10.2 Compliance with Legislative Requirements

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

- Data Protection Act (1984¹),
- Computer Misuse Act (1990), and
- Copyright, Designs and Patents Act (1988).

All applications handling personal data on individuals will comply with data protection legislation and principles.

Under the Computer Misuse Act, it is an offence to access or modify material without proper authority, or to access material with intent to commit further offences.

ICL Pathway will protect against unauthorised copying of documentation and software.

In addition to the Acts identified above, ICL Pathway will comply with appropriate sections of PACE, Post Office and Telegraph Acts, Official Secrets Act 1989, Companies Act and relevant EU Directives.

¹ Change to Data Protection Act (1998) will be subject to CCN approval.

10.3 Compliance with BS7799

The controls defined in BS7799 are designed to provide a sound baseline for commercial organisations of many types.

ICL Pathway will apply BS7799 to provide a baseline definition for information security encompassing the ten categories of controls. This security policy document considers each of the categories, as indicated in Table 1, and outlines the requirements in the ICL Pathway context.

BS7799 Section	Category of Controls	Security Policy Section
3	Security Policy	All
4	Security organisation	3 (and 4)
5	Asset classification and control	6.1 and 6.2
6	Personnel security	5
7	Physical and environmental security	6.3
8	Communications and operations management	7.1
9	Access control	6.4
10	Systems development and maintenance	7.3
11	Business continuity management	8
12	Compliance	9

Table 1 BS7799 Control Categories

ICL Pathway's Security Procedures will provide further guidance, based upon the BS7799 Code of Practice.