Document Title:	PATHWAY SECURITY POLICY
Document Type:	Policy Document
Abstract:	This Security Policy specifies mandatory security requirements that must be applied throughout the life-cycle of the ICL Pathway services.
Distribution:	DSS POCL Pathway Pathway Library
Document Status:	Issued
Document Predecessor:	Version 2.0
Associated Documents:	See section 0.2
Author:	Peter J Harrison
Approval Authority:	Martyn Bennett, Director Quality and Risk Management
Signature/Date	
Comments To:	Author, copy to Martyn Bennett
Comments By:	-

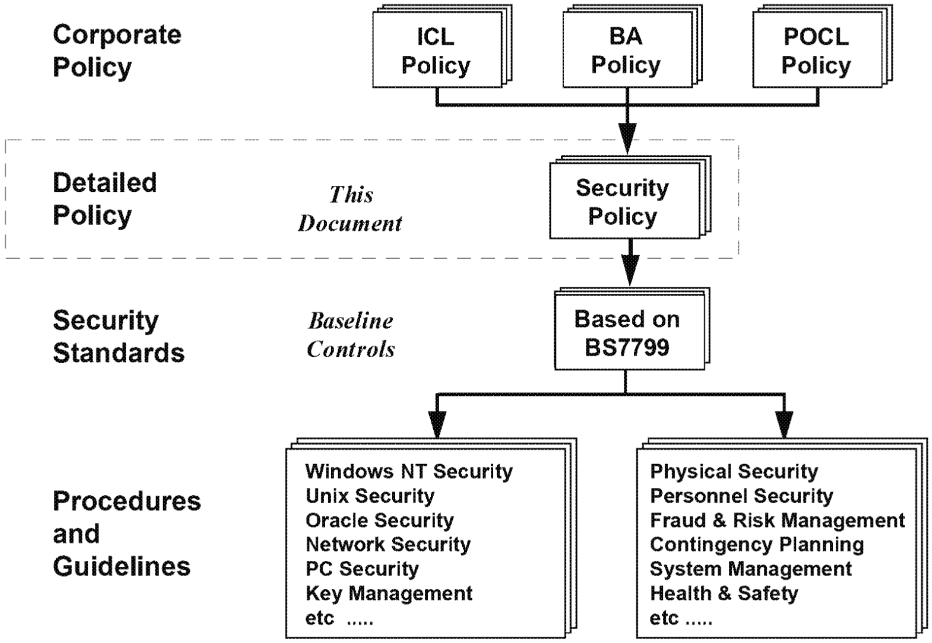
FOREWORD

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

Pathway's high level 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 Pathway.

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



Pathway's Security Policy and Standards

0. CONTENT

0.1 Document History

Version	Date	Reason
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	Submitted for formal approval

0.2 Associated Documents

Version	Date	Title	Source
2	1/5/92	ICL Group Security Policy	ICL
5	25/6/95	DSS/POCL Functional Specification	Pathway
TBA		ICL Pathway Security Standards	Pathway
TBA		ICL Pathway Access Control Policy	Pathway
6.2	-	DSS IT Security Policy (Departmental IT Security Standards) DITSG/ITSS/0001.04	DSS
-	-	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
TBA	-	Schedule B01 - Requirements Catalogue	
1	15/2/95	BS7799 - A Code of Practice for Information Security Management	BSI

0.3 Abbreviations

APS	Automated Payment Services
BA	Benefits Agency
BES	Benefit Encashment Service
CASA	Contracting Authorities Security Authority
CESG	Communications-Electronics Security Group
CMS	Card Management Service
CLEF	Commercial Licensed Evaluation Facility
DSS	Department of Social Security
EPOSS	Electronic Point Of Sale Service
OBCS	Order Book Control Service
PAS	Payment Authorisation Service
PFI	Private Finance Initiative
POCL	Post Office Counters Limited
PUN	Pick Up Notice

0.4 Contents

1. INTRODUCTION

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

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

1.1 Service Overview

The agreement is one of the UK Government's major Private Finance Initiative (PFI) projects, whereby Pathway will automate 20,000 Post Offices and provide the infrastructure used to make benefit payments to an estimated 20 million recipients.

The Benefit Payment Service (BPS) translates input from the Benefit Agency (BA), in the form of authorised payments, into benefit payments that are collected, from nominated Post Offices, by card holding claimants. It also provides returns to BA on the payments that are made, together with other information.

BPS is defined as the end-to-end service provided by the combination of Benefit Encashment Service (BES), Payment Authorisation Service (PAS) and Card Management Service (CMS).

Computerised facilities at Post Office counters also 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. Order Book Control Service (OBCS) is an optional counter application operating through EPOSS.

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

1.2 Scope

This Security Policy specifies mandatory security requirements that must be applied throughout the life -cycle of the ICL Pathway services.

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

Figure 1 illustrates how particular service functions are mapped to typical subcontractors for key components of the operational service.

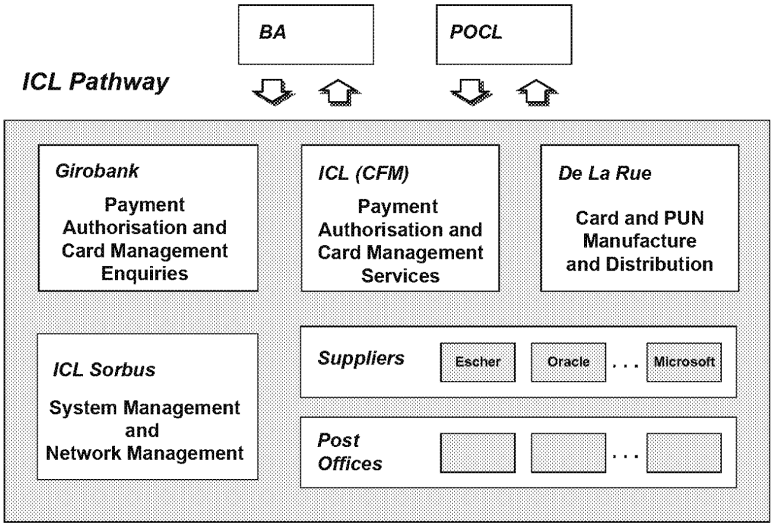

BA
POCL
ICL Pathway
Girobank
Payment Authorisation and Card Management Enquiries
ICL (CFM)
Payment Authorisation and Card Management Services
De La Rue
Card and PUN Manufacture and Distribution
ICL Sorbus
System Management and Network Management
Suppliers
Escher
Oracle
...
Microsoft
Post Offices
...

Figure 1 Subcontracted Functions for Pathway's Services

Pathway's Security Policy must be compatible with the DSS and POCL Security Policies. The interfaces between 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) and suppliers of key service components (including De La Rue and Microsoft) will be subject to individual agreements with Pathway. De La Rue has responsibility for manufacture and initial distribution of all Cards and Pick Up Notices (PUNs).

1.3 Policy Review

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

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

1.4 Implementation Priorities

The short implementation timescales, agreed between Pathway, DSS/BA and POCL, dictate that detailed Security Standards may not be in place at the outset of all development activities.

The planned implementation order is:

- Pathway Security Policy (this document),
- security standards for system development activities,
- security standards for system integration and validation,
- security standards for pre-release,
- security standards for system roll-out, and
- security standards for all operational environments.

Guidelines provided by BS7799, a Code of Practice for Information Security Management, and relevant sections of the documents listed in section 0.2, will be used. Where appropriate, these will be supplemented by Pathway specific standards.

2. OBJECTIVES

This document aims to provide a clear definition of Pathway's high-level Security Policy.

Pathway will establish an infrastructure that will minimise and control liabilities to itself, its suppliers, the DSS and POCL (thereby meeting the requirements outlined in Appendix A).

This policy document is intended to lay the foundation that will enable Pathway to protect the integrity, availability and confidentiality of information used by the services. This includes making adequate provision for:

- Business Continuity,
- Fraud Risk Management, and
- compliance with Data Protection legislation.

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

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

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

2.1 Business Objectives

The profitability and viability of Pathway's business operation are dependent upon identifying and managing all risks for which Pathway has accepted responsibility. Protecting the information assets owned by DSS/BA, POCL and POCL clients is also of fundamental importance.

Pathway will develop Contingency Plans that will be used to ensure continuity of service. The plans, to be agreed between Pathway, DSS/BA and POCL, will be based upon the results of comprehensive Risk Assessment.

Maintaining Pathway's reputation as a supplier of secure, efficient, reliable, cost-effective services, and the reputation of DSS/BA and POCL, is extremely important. Any service malfunction might be widely publicised and exploited to the detriment of Pathway, DSS/BA or POCL.

The opportunities for additional POCL services will be influenced by the confidence established by the base services.

2.2 IT Security Objectives

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 security of all information conveyed, processed or stored, by the services.

1. Security measures in Pathway's IT systems will ensure appropriate confidentiality, integrity and availability of data, whether in storage or in transit. Maintaining the integrity of the services and software components is also essential.
2. Physical and logical access to the system 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 the system. Authentication mechanisms are also required to ensure that trust relationships can be established between communicating components within, and external to, the system.
4. All users of 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 and detect events that might threaten the security of the 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 of the occurrence of security violations that could seriously threaten the secure operation of the services. These alarms will be used to trigger prompt investigation and remedial action in order to minimise the impact of any security breach.
7. Pathway will monitor all developments and operations to maintain assurance that its services are performing in accordance with approved security standards and controls. This will give a high level of confidence that all information is being protected during processing, transmission and storage.

2.3 Legal Obligations

Pathway must remain fully compliant with all legislation and regulatory controls.

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 Pathway's operation.

3. RESPONSIBILITIES FOR SECURITY

Pathway's Managing Director has ultimate responsibility for security.

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

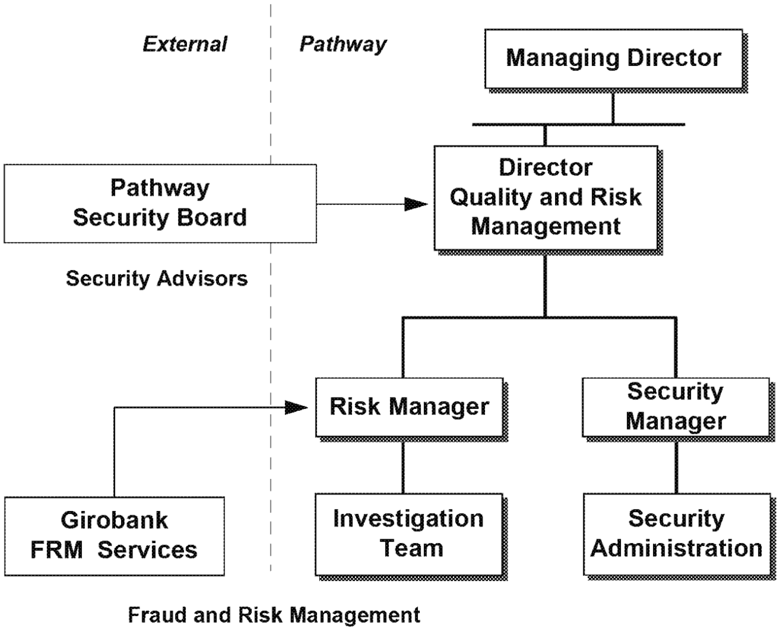


Figure 2 Pathway's Security Management Structure

Figure 2 illustrates the security organisation used within Pathway and the activities subcontracted to Girobank. Senior management is supported by experienced specialists and technical staff with specific expertise in the areas of IT, security, fraud prevention and risk management.

3.1 Director, Quality and Risk Management

The responsibilities of the Director, Quality and Risk Management, include:

- overall control of security throughout Pathway,
- provision of adequate resources for security,
- being Chairman of the Pathway Security Board (see section 3.2),
- owner of Pathway's Security Policy,
- approval authority for Pathway's Security Policy,
- approval authority for Pathway's Security Standards,
- overall control of fraud and risk management functions,
- establishing the security interface with the DSS/BA and POCL, and
- establishing the security interface with all subcontractors.

3.2 Pathway Security Board

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

The Security Board participants, which will include the Contracting Authorities Security Authority (CASA), 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 Pathway's Security Strategy,
- determining the adequacy of 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.

3.3 Security Manager

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

Pathway's Security Manager's responsibilities include:

- physical and environmental security,
- monitoring for compliance with 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 Pathway's Security Policy,
- owner of Pathway's Security Standards,
- documentation of Pathway's Security Standards,
- communication of security policy and standards throughout 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 CASA,
- liaison with DSS/BA, POCL and suppliers' security personnel, and
- recruitment selection of security administration personnel.

3.4 Security Administration

The description "Security Administration" has been used to describe Pathway personnel assigned to roles with particular responsibility for security.

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 service. In this capacity they can:

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

3.5 Responsibilities for Physical Security

By using existing operational sites, Pathway benefits from the current security infrastructure in order to protect against threats from physical and environmental sources.

Pathway has responsibility for reviewing the adequacy of all existing controls, working with a nominated manager agreed with each subcontractor. The physical security of facilities used by Pathway and its subcontractors, including development, test and integration areas, will be maintained by ICL Pathway.

3.6 Hardware Security

Post Offices pose some significant challenges for several reasons:

- Pathway will use approximately 20,000 sites throughout the UK,
- Pathway cannot control the physical security at Post Offices,
- Pathway owns the IT assets installed in each Post Office,
- high specification commercial PCs will be installed at each site,
- Pathway cannot vet or select Post Office personnel, and
- changes to the Post Office operating environment can occur.

The physical security measures associated with equipment installation will take these factors into account to reduce Pathway's risks to an acceptable level.

3.7 All Personnel

All service users, most of whom will be at Post Office counters, will be included in 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, Postmaster or clerk).

All 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 perceive may be suspicious.

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

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

3.8 Reporting Security Incidents

Pathway will establish effective procedures for reporting, acting upon and escalating all incidents that could affect security.

Pathway's Security Manager will ensure that all incidents are recorded, investigated and, where appropriate, acted upon, with appropriate urgency. This will include liaison with CASA to review incidents and actions.

4. FRAUD AND RISK MANAGEMENT

Pathway's policy is to identify and minimise the risk of fraud within the Pathway services. However, Pathway recognises that the threat of fraud incidents exists inside and outside Pathway's responsibility.

Pathway's Director, Quality and Risk Management, has responsibility for fraud and risk management, in addition to security, as outlined in section 3.1. In this former capacity, he/she is supported by a Risk Manager, an investigation team, and external specialist services, as illustrated in figure 2.

The Fraud Risk Management (FRM) service will concentrate on the identification, monitoring and management of encashment fraud within the Benefit Payment Service and the POCL Strategic Infrastructure.

4.1 Risk Manager

Pathway's Risk Manager's responsibilities include:

- identifying and categorising risks associated with fraud,
- analysis of trend incidents and fraud losses,
- fraud monitoring, to profile abnormal or irregular encashment patterns and identify potential fraud incidents,
- establishing internal controls to reduce the potential for fraud,
- reducing the potential for fraud perpetrated through collusion,
- reviewing security policy and standards from a fraud perspective,
- providing the point of contact for reporting all fraud incidents,
- recording and investigating fraud incidents,
- managing the supporting FRM services, and
- liaison with external authorities in the event of fraud.

4.2 Investigation Team

The investigation team, shown in figure 2, carry out investigations instigated by the Risk Manager. The team's activities include:

- collecting and examining system evidence in support of investigations,
- reporting on the findings of all investigations,
- quantifying the amounts involved in fraud incidents,
- identifying persons implicated in fraud perpetration,
- recommending measures which could reduce fraud risks, and
- working with specialist external bodies developing new techniques.

4.3 Management of Fraud and Risk

As illustrated, in figure 2, specialist fraud and risk management services will be invoked to supplement Pathway's internal resources. Girobank's use of the data will be restricted to that required for FRM investigations.

Use of external services enables:

- specialist skills to be invoked whenever needed,
- adequate resources to be available for special investigations,
- independent review of Pathway's own procedures, and
- Pathway to keep abreast of new methods for reducing risk.

5. 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 Pathway's own employees and to staff from subcontractor's organisations.

5.1 Recruitment Selection

All applicants will be subject to vetting, which will include checks on their identification and financial circumstances.

Business and personal references will be checked for all external applicants.

5.2 Job Descriptions, Contracts and Assessment

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

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

5.3 Security Education and Training

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

The programme will include:

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

6. 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.

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

6.1 Information Classification

All information used by 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.

Pathway will assume that aggregation cannot increase the classification of any information (unless otherwise agreed with the Authority).

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

6.2 Safeguarding DSS/BA and POCL Records

Pathway will establish appropriate controls to safeguard all manual and electronic records supplied by DSS/BA and POCL. The records will be safeguarded from unauthorised disclosure, modification, loss, destruction and falsification. The security characteristics of the records and requirements for processing and storage will be agreed, formally, with the DSS/BA or POCL provider.

6.3 Physical and Environmental Security

Use of existing secure computing facilities for 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. Alternative power supplies will be provided in accordance with Pathway's contingency plans.

6.4 System Access Control

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

The Access Control Policy and its associated Security Standards 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 Pathway system components,

- control of access to all data within the Pathway system,
- 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 services,
- management, assignment and revocation of privileges,
- mechanisms to be used for user identification and authentication,
- password management, including password generation and expiry, and
- monitoring system access and use of facilities.

Accountability of individuals is essential and segregation of duties will be enforced where appropriate. For particularly critical operations "two person controls" will be used.

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

- DSS/BA's instruction to Pathway to enter a fall-back mode,
- DSS/BA's calls to the PAS Help Desk to stop payments or place other actions,
- calls from Post Offices to the PAS Help Desk for payment authorisation when operating in fallback mode (notably for encashment at "foreign" Post Offices),
- customer calls to the CMS Help Desk for card enquiries, and
- all calls to the CMS Help Desk requesting changes.

6.5 Cryptography

Pathway will seek the guidance of Communications-Electronics Security Group (CESG) on all matters concerning cryptography. Typically, this would include:

- 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).

Pathway will comply with Government Policy with regard to the application of cryptographic techniques to the protection of Government Data.

7. ADMINISTRATION OF SECURITY

Pathway will implement effective controls to protect against the possibility of attack from "users" who are granted privileges and access rights. Similarly, individuals with access to source code and development facilities will be monitored.

The following subsections provide an overview of the controls required within Pathway's organisation. Pathway's Security Standards will provide more detailed guidance based upon the BS7799 controls for:

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

7.1 System and Network Management

Operational control of 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. Pathway will therefore ensure that:

- staff assigned to management functions are carefully selected,
- particular attention is paid to logical and physical access controls,
- 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 with before and after states.

7.2 Audit Management

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.

7.3 Systems Development and Maintenance

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:

- control of access to information and services,

- segregation of duties,
- secure operation in degraded mode,
- incorporation and analysis of audit trails,
- ensuring integrity of data using sealing and verification mechanisms,
- 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 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, using hash totals and balance controls.

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

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 system.

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

7.4 Virus Control Policy

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

7.5 Information Exchange Control

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 DSS/BA and POCL, will be subject to formally agreed controls.

7.6 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.

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 Pathway's Security Manager.

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

7.7 External Contractors and Suppliers

Pathway will ensure that the use of external contractors and suppliers is covered by appropriate safeguards. 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, Microsoft and Oracle) will be subject to formal agreements in support of this security policy.

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

8. BUSINESS CONTINUITY

Pathway will ensure that an effective business continuity plan is agreed with CASA 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.

8.1 Contingency Planning

In order to minimise any disruption to the services managed by 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.

8.2 Testing Contingency Plans

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

8.3 Subcontractor's Contingency Plans

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

9. COMPLIANCE

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

The importance of compliance is illustrated by the fact that 4 out of 10 of the key controls, defined in BS7799, are about compliance.

9.1 Compliance with Pathway's Security Policy

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

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

9.2 Compliance with Legislative Requirements

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

- Data Protection Act (1984),
- 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.

Pathway will protect against unauthorised copying of documentation and software.

In addition to the Acts identified above, Pathway will comply with appropriate sections of PACE, the Social Security Administration Act, Post Office and Telegraph Acts, Official Secrets Act 1989, Companies Act, EU Directives and other obligations to be defined in Pathway's standards.

9.3 Compliance with BS7799

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

Pathway will apply BS7799 to provide a baseline definition for information security encompassing the ten categories of controls:

BS7799 Section	Category of Controls	Security Policy Section
1	Security Policy	All
2	Security organisation	3 (and 4)
3	Asset classification and control	6.1 and 6.2
4	Personnel security	5
5	Physical and environmental security	6.3
6	Computer and network management	7.1
7	System access control	6.4
8	Systems development and maintenance	7.3
9	Business continuity planning	8
10	Compliance	9

Table 1 BS7799 Control Categories

This security policy document considers each of these categories, as indicated in Table 1, and outlines the requirements in the Pathway context.

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

APPENDIX A SECURITY POLICY REQUIREMENTS

This Security Policy document encompasses all of the requirements specified in Pathway's agreement with the Authority (as defined in Schedule B01).

By implementing the agreed Security Policy, Pathway will minimise and control liabilities to itself and the Authorities.

The security infrastructure established by Pathway will cover all areas specified by the Authority. Table A1 (which is based upon Schedule B01, Requirement 698) indicates the section of BS7799 that describes the category of control and the nature of the ten "key" controls.

Security Features	Section	BS7799	
The agreement of a Security Policy	1.2	1	key
Allocation of Security Responsibilities	3	2	key
Security Education and Training	5.3	4	key
Reporting Security Incidents	3.8	4	key
Physical Security Control	6.3	5	
Virus Control	7.4	6	key
Business Continuity	8	9	key
Control of Proprietary Software	7.6	10	key
Safeguarding DSS/BA and POCL Records	6.2	10	key
Information Classification	6.1	3	
Compliance with Data Protection and other legislation	9.2	10	key
Information Exchange Control	7.5	6	
External Contractors and Suppliers	7.7	2	
Compliance with Security Policy	9.1	10	key
Management of fraud and risk during service operation	4	6	

Table A1 Requirement 698 Cross Reference