FUJ00232554

Document Title: HORIZON SECURITY POLICY

Document Type: Policy

Release: BI3 S75 onward

Abstract: This security policy specifies mandatory security requirements to be applied throughout Post Office Account.

Document Status: FOR APPROVAL

Originator & Dept: Brian Pinder (CS Security & Risk)

Contributors: Pete Sewell, Mik Peach, Alex Robinson

Internal Distribution: Graham Chatten ;Dave Baldwin; Peter Burden; Carl Marx; Richard Brunskill ;Liam Foley ;Alex Robinson; Jan Holmes Mark Wiltshire, Naomi Elliott, Hillary Forrest

External Distribution: Sue Lowther – Post Office Ltd.

Approval Authorities: (*See PA/PRO/010 for Approval roles)*

Name	Position	Signature	Date
Dave Baldwin	POA Business Unit Director		
Colin Lenton-Smith	Director, Commercial		
Mark Wiltshire	Programme Director POA		
Naomi Elliott	Service Director POA		
Sue Lowther	Post Office Ltd		
Brian Pinder	POA Security Manager		

FUJ00232554

0.0 Document Control

0.1 Document History

Version No.	Date	Reason for Issue	Associated CP/PinICL
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 Pathway Management team	
1.0	16/8/96	Incorporates comments from DSS/BA and POL	
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 Internally	
5.1	20/11/00	Incorporates clarification in respect of DPA and OBCS.	
6.0	20/11/00	Approved Internally	
6.1	08/08/01	Incorporation of changes in organisation. For review and circulation as a baseline to inform NWB contractual negotiations.	
6.2	30/04/02	Change from ICL branding to Fujitsu Services	
7.0	28/05/02	Approved	
7.1	12/07/02	Incorporation of the Network Banking Service. Minor typographical and contextual changes.	
7.2	15/08/02	Incorporation of comments from review.	
8.0	03/09/02	Approved	
8.1	Jan 2003	Updates in line with BS ISO/IEC 17799 and	

FUJ00232554

		inclusion of the Debit Card System	
9.0	24/01/03	Approved	
9.1	30/4/04	To reflect change to Post Office Account and incorporate planned new products and services introduced by S50, S52, S52R, S60, S70 and S75. Introduction of Vulnerability Management and Technical Compliance Testing.	
9.2	30/9/04	Additions to legal compliance to cover Financial Services Authority requirements and Money Laundering Regulations.	
10.0	11/11/04	Approved	
10.1	20/4/06	To reflect recent personnel changes	
11.0	23/6/2006	Approved	

0.2 Review Details

Review Comments by :	22nd June 2006
Review Comments to :	Pete Sewell

Mandatory Review Authority	Name
POA	
Service Director POA	Naomi Elliott
Programme Director POA	Mark Wiltshire
Director Commercial	Colin Lenton Smith
Cryptographic Development	Alex Robinson*
Audit & Risk	Jan Holmes*
POA Security	Brian Pinder
Post Office Limited	Sue Lowther
Optional Review / Issued for Information	
Customer Services	Peter Burden

FUJ00232554

Customer Services	Carl Marx
Customer Services	Richard Brunskill*

(*) = Reviewers that returned comments

0.3 Associated Documents

Reference	Version	Date	Title	Source
BS ISO/IEC 17799-1: 2000			Information Technology – Code of practice for information security management	British Standard
BS 7799-2 2002			Information security management specification for information security management systems	British Standard
PA/TEM/001			Fujitsu Services Document Template	PVCS
			Fujitsu Services Group Security Policy	Fujitsu Services
RS/POL/003			Post Office Account Access Control Policy	PVCS
KH2879			Post Office Information Systems Security Policy Document	Post Office Ltd.
BP/POL/002			Post Office Counters Information Systems Security Policy (SSR Appendix 4-1)	Post Office Ltd
BP/ION/002			A Code of Practice for Post Office Information Systems Security	Post Office Ltd
CR/FSP/004			System Architecture Design Document	PVCS
RS/FSP/001			Security Functional Specification	PVCS
RS/PRO/170			POA Incident Management	PVCS

Unless a specific version is referred to above, reference should be made to the current approved versions of the documents.

FUJ00232554

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
DCS	Debit Card System
DSS	Department of Social Security
EPOSS	Electronic Point Of Sale Service
ISO	International Standards Organisation
LFS	Logistics Feeder Service
NBS	Network Banking Service
OBCS	Order Book Control Service
PFI	Private Finance Initiative
PIN	Personal Identification Number
PPP	Public Private Partnership
SEM	Security Event Management

0.5 Changes in this Version

Version	Changes
9.0	Minor amendment to Diagram in paragraph 4 to reflect revised Post Office Organisation
9.1	Amended to reflect change from Pathway to Post Office Account Changes to document distribution and approval Incorporation of planned new products and services at S60 and aspects of S70 and S75, Introduction of Vulnerability Management and Technical Compliance Testing.
9.2	Additions to legal compliance to cover Financial Services Authority requirements and Money Laundering Regulations.

FUJ00232554

10.0	Minor amendments to correct typos and reflect correct abbreviations within the document.
10.1	Reflect changes to update recent personnel changes
11.0	Minor comments incorporated

0.6 Changes Expected

Changes
None

FUJ00232554

0.7 Table of Contents

FUJ00232554

FUJ00232554

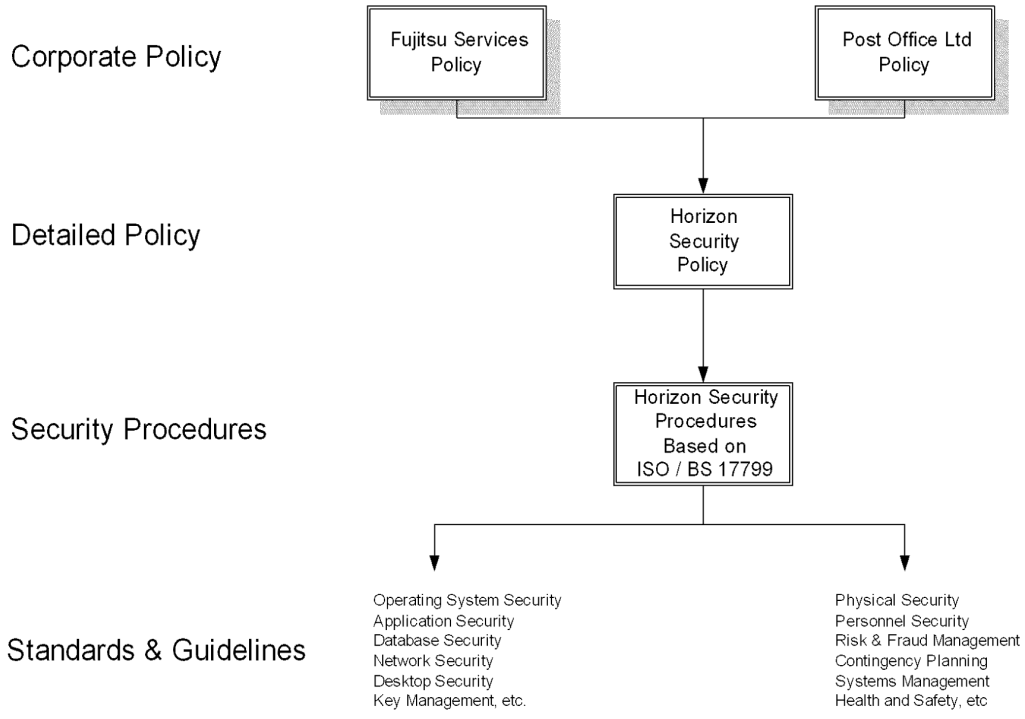
1.0 Foreword

This document defines Post Office Account'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 Post Office Account to comply with legislative and commercial requirements.

Post Office Account's policy statement (which is essentially the same as the Corporate Policy statement used by Group (Fujitsu Services)) is:

It is the policy of Fujitsu Services, Post Office Account 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 Post Office Account.

This document fits into the structure illustrated below, with the BS ISO/IEC 17799 Code of Practice being used as a basis for Post Office Account's Security Procedures. Lower level implementation standards are incorporated as appropriate.



Post Office Account's Security Policy, Procedures and Standards

FUJ00232554

2.0 Introduction

In May 1996, Fujitsu Services, Post Office Account, formerly ICL (Pathway), 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.

In July 2002, Post Office Account was awarded a contract to provide a Network Banking Service (NBS), which initially supports several On-line counter transaction types. In September 2002 this contract was extended to include a Debit Card system interfacing with National Westminster Streamline as Merchant Acquirer.

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

2.1 Service Overview

The agreement is a PPP project, whereby Post Office Account automates approximately 16,000 Post Offices and provides the infrastructure which enables users to make automated payments at outlets throughout the UK.

- Automated Payment Services (APS) and (AP ADC).
- Electronic Point Of Sale Service (EPOSS).
- Logistics Feeder Service (LFS).
- Network Banking Service (NBS).
- The Debit Card System (DCS).
- Pin Pad authentication for NBS, DCS, incorporating EMV Chip and PIN.
- Bureau de Change.
- E Top Ups.
- NS&I.
- DVLA, incorporating PAF.
- SAP Hosting

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

The SAP Hosting solution is jointly managed by Fujitsu Services and Prism who share operational responsibility for the system. Security of the solution will be based on the current security agreement between Post Office and Fujitsu Services for running the Horizon systems. Areas deemed relevant to SAP are:

- Identification and Authentication
- Access Controls

FUJ00232554

- Audits and Alarms
- Network Security
- Virus Protection

2.2 Scope

This Security Policy specifies mandatory security requirements to be applied throughout Post Office Account.

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

Post Office Account's Security Policy must be compatible with Post Office Ltd. Security Policy. The interfaces between Post Office Account and all external organisations must be clearly defined and formally agreed with the organisations concerned.

Security obligations for subcontractors involved in development activities are subject to individual agreements with Post Office Account. Commercial off the shelf (COTS) products are provided by the appropriate product suppliers.

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 Post Office Account's Security Policy and Procedures are defined in section 4.

3.0 Objectives

This document provides a definition of Post Office Account's high-level Security Policy.

Post Office Account will establish an infrastructure that will minimise and control liabilities to itself and Post Office Ltd.

The Security Policy defines the requirements for Post Office Account 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 4) in order that the policy requirements can be communicated throughout Post Office Account. This ensures that all parties are fully aware of their responsibilities and legal obligations.

Post Office Account has stated its commitment to ensuring that it encompasses the very best commercial practices for security. Post Office Account's aim is to be fully compliant with BS ISO/IEC 17799.

FUJ00232554

Compliance with legislative requirements (including the Data Protection Act 1998) and BS / ISO17799 is considered under "Compliance" (in section 10).

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 Post Office Account's reputation.

3.2 IT Security Objectives

Post Office Account's overall IT security objective can be summarised as achieving the requirement expressed in the following policy statement:

It is the policy of Fujitsu Services, Post Office Account 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 Post Office Account'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, Post Office Account's services.
4. All users of Post Office Account'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 Post Office Account 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 Post Office Account's services. These alarms will be used to trigger prompt investigation and remedial action in order to minimise the impact of any security breach.

FUJ00232554

7. Post Office Account 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

Post Office Account must remain fully compliant with all relevant legislation and regulations.

In addition to the existing legislative obligations, identified in section 10.2, it is important to track and anticipate emerging UK and European regulations that could affect Post Office Account's operation.

4.0 Responsibilities for Security

Post Office Account's Managing Director has ultimate responsibility for security.

Post Office Account's commitment to security will be communicated throughout Minor amendment to Diagram in paragraph 4 to reflect revised Post Office Organisation Post Office Account, as evidenced by board level approval of Minor amendment to Diagram in paragraph 4 to reflect revised Post Office Organisation Post Office Account's Security Policy.

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

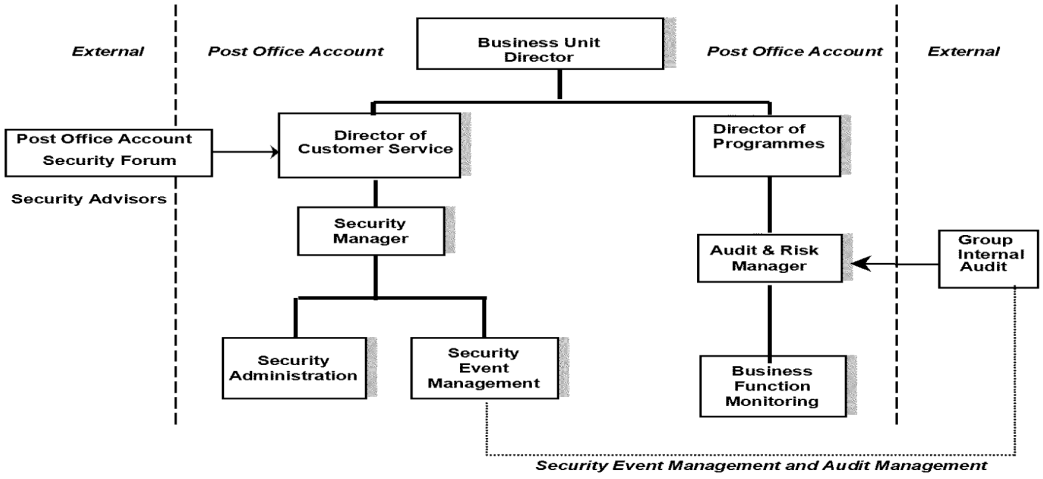


Figure 1 Post Office Account's Security Management Structure

4.1 Director, Customer Services

The security related responsibilities of the Director, Customer Services, include:

- overall control and management of security throughout Post Office Account,
- provision of adequate resources for security,
- being Chairman of the Post Office Account Security Board (see section 4.2),

FUJ00232554

- owner of Post Office Account's Security Policy,
- approval authority for Post Office Account's Security Policy,
- approval authority for Post Office Account's Security Procedures,
- establishing the security interface with Post Office Ltd, and
- establishing the security interface with all subcontractors.

Overall control of risk management functions is the responsibility of the Programme Director.

4.2 Post Office Account Security Forum

The representatives on Post Office Account's Security Forum are nominated by the Director, Customer Services, and approved by the Post Office Account Forum.

The Security Board participants, who will include Horizon Security Liaison staff, represent a broad range of interests to ensure that alternative perspectives are considered.

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

Security Board responsibilities include:

- ownership of Post Office Account's Security Strategy,
- determining the adequacy of Post Office Account'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 Post Office Account.

Post Office Account's Security Manager's responsibilities include:

- physical and environmental security,
- monitoring for compliance with Post Office Account'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 Post Office Account's Security Policy,
- owner of Post Office Account's Security Procedures,
- documentation of Post Office Account's Security Procedures,
- communication of security policy and procedures throughout Post Office Account,
- 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 Post Office Ltd Security staff,

FUJ00232554

- liaison with the Post Office Ltd Information Security Manager, external regulators and suppliers' security personnel,
- reporting to the Post Office Limited Information Security Manager any actual or potential threats or breaches that may have a material effect on any service, and
- recruitment selection of security administration personnel.

4.4 Security Administration

The description "Security Administration" is used to describe Post Office Account personnel assigned to roles with particular responsibility for security.

Post Office Account's Security Manager is the normal line manager for this group; hence many of the activities assigned to Security Administrators are in support of the functions listed in section 4.3.

Wherever possible, Security Administrators 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 Post Office Account's Security Policy,
- implement Post Office Account's Security Procedures,
- conduct independent reviews of compliance to policy and procedures,
- report actual and suspected security incidents, and recommend changes, to enhance Post Office Account'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 Post Office Account.

At some sites, notably Data Centres and support sites, Post Office Account 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 Post Office Account equipment installed.

4.6 All Personnel

All Post Office Account service users will be subject to Post Office Account'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.

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

Promoting security awareness, throughout Post Office Account, to subcontractors, and temporary staff is an important responsibility assigned to Post Office Account's Security Manager. Publicising security reporting and escalation procedures will be part of this awareness strategy.

FUJ00232554

4.7 Reporting Security Incidents

Post Office Account has established effective procedures for reporting, acting upon and escalating all incidents that could affect security. It is the responsibility of all users of the Post Office Account services and Post Office Account personnel to use these procedures.

Post Office Account'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.

5.0 Responsibilities for Audit

The Director of Programmes is accountable for the Audit function within Post Office Account, as illustrated in figure 1.

The Audit Manager's responsibilities, listed in section 5.1, are primarily concerned with managing the internal Audit function within Post Office Account but they also include liaison with Post Office Ltd. audit personnel.

As the point of contact with external audit personnel, the Audit Manager maintains regular contact with many Post Office Account 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 Post Office Account'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

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

The Audit Manager's responsibilities include:

- planning and carrying out audits of Post Office Account'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 Post Office Account's Audit Policy,
- providing the point of contact for all audit related matters,
- overall responsibility for Minor amendment to Diagram in paragraph 4 to reflect revised Post Office Organisation Post Office Account's Audit activities,
- documentation of Post Office Account's Audit Policy,
- being the owner of Post Office Account's Audit Standards,
- documentation of Post Office Account's Audit Standards,
- communication of Audit policy and standards within Post Office Account,
- co-ordinating the evaluation of all new audit products proposed,
- specifying and arranging Audit education and training,
- liaison with Post Office Ltd. audit personnel,

FUJ00232554

- liaison with Fujitsu Services 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 Post Office Account personnel assigned to roles with particular responsibility for Audit.

Post Office Account's Audit Manager is the normal line manager for this group; hence many of the activities assigned to Business Function Monitoring are in support of the functions listed in section 5.1.

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

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

5.3 Security Event Management Responsibilities

The description "Security Event Management" is used to describe Post Office Account personnel assigned to roles with particular responsibility for security relevant events recorded by Post Office Account's systems.

Post Office Account's Security Manager is the normal line manager for this group; hence many of the activities assigned to Security Event Management personnel are supporting functions.

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

- ensure that specified events are being audited on the relevant platforms,
- ensure that all access (and attempted access) to Post Office Account's systems is audited,
- monitor usage by Post Office Account operations and management staff,
- analyse the audit logs generated by the different Post Office Account 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 Post Office Account's Security Procedures (particularly with regard to audit),
- report actual and suspected security incidents, and
- recommend changes, to enhance Post Office Account's security controls, to the Security Manager.

6.0 Personnel Security

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

FUJ00232554

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 Post Office Account's own employees and to staff from subcontractor's organisations.

6.1 Recruitment Selection

All applicants are subject to an appropriate level of vetting, using criteria approved and provided by Fujitsu Services Group Security. This includes checks on their identification, qualifications and financial circumstances. Business and personal references are checked for all applicants.

6.2 Job Descriptions, Contracts and Assessment

Post Office Account will apply best commercial practice, based upon BS ISO/IEC 17799, to include security considerations within, Employees Terms and Conditions for Employment, and generic job descriptions.

6.3 Security Education and Training

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

The programme will include:

- all Post Office Account employees, and
- appropriate training for contractors and third parties.

7.0 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.

Post Office Account's Security Procedures will provide more detailed guidance based upon the corresponding BS ISO/IEC 17799 sections. This will include the provision and maintenance of an asset register and up to date inventories of all significant component assets – information, software, hardware and services.

7.1 Classification of Information

All information used by Post Office Account 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.

Post Office Account will assume that aggregation cannot increase the classification of any information unless risk assessment indicates otherwise.

FUJ00232554

Post Office Account's Security Procedures will include guidance on protective marking, handling and disposal of information.

7.2 Safeguarding Post Office Ltd. Records

Post Office Account will protect all manual and electronic records supplied by Post Office Ltd in accordance with agreed contractual obligations. The records will be safeguarded from unauthorised disclosure, modification, loss, destruction and falsification.

7.3 Protection of Horizon Documentation

All information which is held on paper, in databases or data files, system documentation, user manuals, training material, operational or support procedures, continuity plans and fallback arrangements, backup files can all be categorised by subject. The inventory will hold the following information:-

- The information subject asset name and high level description
- The information asset classification,
- Special files classification in any subject information
- The information subject owner.
- The information subject custodian.

7.3.1 Protection of Magnetic Media

Magnetic media must be protected against theft, damage or deterioration. Data centres must have a secure media library with procedures to control the movement of media in and out. In other locations, magnetic media must be stored in lockable containers, cabinets, fire safes etc.

7.3.2 Protection of Paper Documents

Input forms, printout, microfilm, documents and other hard-copy information must be handled, distributed, stored and destroyed securely. Documents with potential value must be handled "as if" they have that value.

7.3.3 Protection of Back-up Media

Secure off-site storage must be provided for back-up copies of magnetic media and essential hard-copy documents.

7.4 Physical and Environmental Security

Use of existing secure computing facilities for Post Office Account's central services simplifies the task of establishing secure areas for the protection of IT facilities. The physical security measures 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.

FUJ00232554

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:

- Post Office Account supports approximately 16,000 sites throughout the UK,
- Post Office Account cannot control the physical security at Post Offices,
- Post Office Account owns the IT assets installed in each Post Office,
- high specification commercial PCs are installed at each site,
- Post Office Account cannot vet or select Post Office personnel, and
- changes to the Post Office operating environment can occur.

Physical and logical segregation of Post office Account assets from other Fujitsu contracts is to be maintained, however, shared use of data centres, server rooms and environmental facilities is permitted. Security measures associated with installed equipment will take these factors into consideration to reduce Post Office Account's risks to an acceptable level.

Similar considerations apply to Post Office Account assets at other non-Post Office Account sites (e.g. AP Client sites)

7.5 System Access Control

Control of access to Post Office Account's systems and data is in accordance with Post Office Account's Access Control Policy, which is based upon analysis of security and business requirements.

The Access Control Policy and associated Security Procedures 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 Post Office Account systems components,
- control of access to all data within the Post Office Account 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 is enforced where appropriate.

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

7.6 Configuration Management

The Horizon Solution will be subject to strict configuration management as defined within the Security Functional Specification (RS/FSP/001) and other pertinent system documentation.

FUJ00232554

7.7 Cryptography

Post Office Account complies with Government Policy with regard to the protection of Government Data. It also complies with relevant regulatory requirements and with ISO standards for the handing of cryptographic key material in accordance with agreed contractual obligations.

Where appropriate, Post Office Account will seek the guidance of Communications-Electronics Security Group (CESG) or follow recognised financial industry guidelines 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).

8.0 Administration of Security

The following subsections provide an overview of the controls required within Post Office Account's organisation. Post Office Account's Security Procedures provide further guidance, based upon the BS ISO/IEC 17799 controls, for:

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

8.1 System and Network Management

Operational management of the system, applications and network is under the control of Operations and Support within Post Office Account.

The system privileges and access permissions required to perform management functions are considerably higher than those assigned to normal users. Post Office Account therefore ensures 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

Post Office Account ensures 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

FUJ00232554

- audit trails are archived and stored for an agreed duration.

8.3 Systems Development and Maintenance

Post Office Account ensures 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,
- segregation of development, test and operational systems
- secure operation in degraded mode,
- incorporation and analysis of audit trails,
- data and system integrity protection,
- use of encryption to prevent unauthorised disclosure and/or modification of data, and
- system resilience, including operation in fallback mode and recovery.

All software developed by or for Post Office Account 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.

Post Office Account ensures that software development activities are fully supported by procedures and standards that cover all aspects of the development process. Audits and reviews are conducted to ensure that the procedures are being applied effectively and that any supporting documentation meets approved standards. Security testing provides confirmation that the security functionality of the systems has been implemented to meet the agreed security specifications.

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

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

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

8.4 Change Control Procedures

8.4.1 Change Control

Strict control over the implementation of changes to the Horizon network, hardware system and application software will be enforced. Such change control procedures must ensure that any changes do not compromise any security or control procedure. Change control procedures must ensure:

- The identification of all components affected by the change.
- The authorisation of all changes and their approval on completion.
- The control of software versions at each stage.

FUJ00232554

- Quality and content control.
- The maintenance of a full record of all changes (audit trail)
- The deletion of any temporary UserIDs/passwords, data and linkages when the system becomes live.
- Changes only carry out their required function and nothing more.
- Only those changes that have been tested are implemented on the live system.
- Changes meet operational requirements.

8.4.2 Operational Changes

Change controls procedures must exist which permit the controlled correction of live systems in order to meet operational requirements and emergencies, e.g. patching of system vulnerabilities. All such changes must be reviewed and approved by the appropriate line management as soon as possible. All Operational and emergency changes should be reviewed following implementation and either removed from the live environment or consolidated via the normal change control and build procedures.

8.4.3 Operating System Changes

Prior to any operating system upgrade or change, a review of all application control and integrity procedures must be carried out to ensure that they will not be compromised by the proposed changes.

8.5 Vulnerability Management Policy

All computer systems and networks contain vulnerabilities which can be exploited by hackers, crackers and insider's intent on doing harm. The vulnerabilities may be as a result of:

- Software defects requiring vendor issued patches or fixes
- Insecure accounts with weak or nonexistent passwords
- Unnecessary services such as, Telnet or remote access
- Built In weaknesses, such as backdoors accounts.
- System misconfiguration

These vulnerabilities can be exploited even when anti virus, firewalls and intrusion detection systems are in place and the only way to properly secure a system is to first assess the existing vulnerabilities on each machine or network segment, determine the degree of risk for each vulnerability, and then mitigate - or fix - the vulnerabilities by updating hardware and software versions or applying vendor issued service packs, hot fixes and patches. This process of finding, evaluating and mitigation is known as vulnerability management.

Post Office Account will adopt industry standard best practise and BS ISO/IEC 17799 recommendations by implementing vulnerability management.

FUJ00232554

8.6 Malicious Software Control Policy

Software and information processing facilities are vulnerable to the introduction of malicious software, such as computer viruses, network worms, Trojan horses and logic bombs. All Post Office Account users should be made aware of the dangers of unauthorized or malicious software, and, where appropriate, controls to detect or prevent the introduction of malicious software, such as computer viruses, network worms, Trojan horses and logic bombs is to be in place on all critical servers and desktop computers.

Protection against malicious software should, where possible, be based on security policy, effective security awareness, appropriate system access and change management controls as well as the installation and regular update of anti-virus detection and repair software. However, it is essential that appropriate management procedures and business continuity plans for recovering from virus attacks, including all necessary data and software back-up and recovery arrangements are available in accordance with section 9 below...

8.7 Information Exchange Control

Post Office Account defines agrees and enforces (with relevant parties) procedures for the exchange of information handled electronically and by other means. The procedures used comply with legal and contractual requirements and depend upon the sensitivity of the information.

In particular, the exchange of information, with Post Office Ltd, is subject to formally agreed controls.

8.8 Control of Proprietary Software

Post Office Account uses proprietary software within the terms of the licence conditions.

Unauthorised copying of software and documentation is prohibited.

Post Office Account 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 Post Office Account's Security Manager.

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

8.9 External Contractors and Suppliers

Post Office Account ensures that appropriate safeguards cover the use of external contractors and suppliers. This includes agreements with contractual terms and conditions and checks on the integrity of external contractors before any work is assigned to them.

External personnel are not 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 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 is sought where externally supplied goods or services are used to process critical and/or sensitive information.

FUJ00232554

9.0 Business Continuity

Post Office Account ensures 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 are established 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 Post Office Account, contingency plans 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 are tested on a regular basis under representative operational conditions.

9.3 Subcontractor's Contingency Plans

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

10.0 Compliance

Post Office Account is required to comply with legislative requirements and commercial standards.

10.1 Compliance with Post Office Account's Security Policy

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

Periodic reviews are carried out at least annually, under the direction of Post Office Account's line managers, to verify that Post Office Account is operating in accordance with its security policy and procedures.

Post Office Account's Audit function (see section 5) provides the essential monitoring activities needed to provide senior management with visibility that Post Office Account is operating in accordance with this policy.

10.2 Compliance with Legislative Requirements

Post Office Account will ensure compliance with all legislative requirements, including the:

- Computer Misuse Act (1990)
- Data Protection Act (1998),

FUJ00232554

- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act (2000)
- Financial Services and Markets Act 2000
- Money Laundering Regulations (2003), and
- Copyright, Designs and Patents Act (1988).

All applications handling personal data on individuals will comply with data protection legislation and principles. Post Office Account shall process personal data only in accordance with the instructions of each Data Controller as set out in the Codified Agreement and applicable provisions of the Service Definition Schedules dealing with such processing.

The security features, capabilities and related procedures provided in respect of the Network Banking will be compliant with the requirements of Part 3 of the Regulation of Investigatory Powers Act 2000.

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. Warning notices to this effect will be displayed to potential users prior to system log-on.

Post Office Account will protect against unauthorised copying of documentation and software.

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

10.3 Technical Compliance Checking

Information systems should be regularly checked for compliance with security implementation standards. Technical compliance checking involves the examination of operational systems to ensure that hardware and software controls have been correctly implemented. This type of compliance checking requires specialist technical assistance. It should be performed manually (supported by appropriate software tools, if necessary) by an experienced system engineer, or by an automated software package which generates a technical report for subsequent interpretation by a technical specialist.

Compliance checking also covers, for example, penetration testing, which might be carried out by independent experts specifically contracted for this purpose. This can be useful in detecting vulnerabilities in the system and for checking how effective the controls are in preventing unauthorized access due to these vulnerabilities. Caution should be exercised in case success of a penetration test could lead to a compromise of the security of the system and inadvertently exploit other vulnerabilities.

Any technical compliance check should only be carried out by, or under the supervision of, competent, persons authorised by the Post Office Account Security Manager.

10.4 Compliance with BS ISO/IEC 17799

The controls defined in BS ISO/IEC 17799 are designed to provide a sound baseline for commercial organisations of many types.

FUJ00232554

Post Office Account will apply BS ISO/IEC 17799 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 Post Office Account context.

Section	Category of Controls	Security Policy Section
1	Security Policy	All
2	Organisational Security	4 (and 5)
3	Asset classification and control	7.1 and 7.2
4	Personnel security	6
5	Physical and environmental security	7.3
6	Communications and operational management	8.1
7	Access control	7.4
8	Systems development and maintenance	8.3
9	Business continuity planning	9
10	Compliance	10

Table 1 BS ISO/IEC 17799 Control Categories

Post Office Account's Security Procedures, based upon BS ISO/IEC 17799 will provide further guidance.