FUJ00002000

Document Title: Service Description for the Security Management Service

Document Type: Customer Services Specification

Release: N/A

Abstract: A document forms the description of the implementation and maintenance of the security policy, processes and procedures, including all applicable security controls and legal aspects associated with the management of information technology.

Document Status: APPROVED

Originator & Dept: Pete Sewell, Brian Pinder CS Security

Internal Distribution: As required

External Distribution: Sue Lowther, Post Office Ltd
Graham Ward, Post Office Ltd
Jamie Butler, Post Office Ltd

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

Name	Role	Signature	Date
Dave Baldwin	Director, Customer Service, Post Office Account		
Sue Lowther	Post Office Information Security Manager		

FUJ00002000

0.0 Document Control

0.1 Document History

Version No.	Date	Reason for Issue	Associated CP/PEAK/PPRR Reference
0.1	19/12/01	Initial Draft	
0.2	23/12/02	Masons' comments on v0.1	
0.3	31/12./02	Sue Lowther (POL) comments on version 0.2	
0.4	31/12/02	Graham Hooper / Masons' comments on Version 0.3	
1.0	6/01/2003	Issued for Approval	
1.1	27/10/04	Draft for agreement following changes to Audit Data Retrieval limitations.	
1.2	30/11/04	Amendment following receipt of comments from document review.	
2.0	02/12/04	For Approval	
2.1	29/09/05	Inclusion of Section 10.2 Compliance with Post Office Security Compliance Requirements and Freedom of Information Act	na
2.2		Not Used	
2.3	19/01/06	Inclusion of the APOP Voucher Retrieval Service	
3.0	06/03/06	Issued for approval.	

0.2 Review Details

Review Comments by :	N/A
Review Comments to :	N/A

Mandatory Review	
Role	*Name*
Director of Customer Service	Dave Baldwin
CS Security Manager	Brian Pinder
CS Security and Risk	Pete Sewell
Commercial Contract Manager	Hilary Forrest
Operations & Support Services Manager	Carl Marx
Post Office Information Security Manager	Sue Lowther
Post Office Casework Manager	Graham Ward
Optional Review	

FUJ00002000

Role	*Name*
POA Project Manager	John Burton
*Issued for Information – **Please restrict this distribution list to a minimum***	
Position	*Name*
CS Security	Bill Membery
CS Security	Andy Dunks
CS Security	Neneh Lowther
CS Security	Penny Thomas

(*) = Reviewers that returned comments

0.3 Associated Documents

Reference	Version	Date	Title	Source
PA/TEM/001	---	---	Fujitsu Services Document Template	PVCS
RS/POL/002	---	---	Horizon Security Policy (CCD)	PVCS
RS/POL/003	---	---	Access Control Policy(CCD)	PVCS
RS/FSP/001	---	---	Security Functional Specification (CCD)	PVCS
RS/FSP/003	---	---	Statements on Security Objectives and Methods for the Protection of Siemens Metering Code and Data	Hardcopy Only
PSO/000/GEN/SCO/105	---	---	Community Information Security Policy for Horizon	Post Office Ltd

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

N.B. Printed versions of this document are not under change control.

0.4 Abbreviations/Definitions

Abbreviation	Definition
CCD	Contract Controlled Document
DPA	Data Protection Act 1998
FOIA	Freedom of Information Act
TESQA	Transaction Enquiry Service Query Application
TOR	Terms of Reference
NBS	Network Banking Service

FUJ00002000

ID	Identification
SLA	Service Level Agreements
APOP	Automatic Payments Out Pay

0.5 Changes in this Version

Version	Changes
1.1	Minor amendments to correct formatting and grammatical text to aid understanding.
1.2	Amendment to Section 3.10 following receipt of comments from document review.
2.0	Minor changes and typo's identified by review
2.1	Inclusion of Section 10.2 Compliance with Post Office Security Compliance Requirements and Freedom of Information Act
2.3	Inclusion of the APOP ARQ service.

0.6 Changes Expected

Changes
Comments from reviewers

FUJ00002000

0.7 Table of Contents

FUJ00002000

1.0 Service Summary

This Security Management Service provides a wide range of security-related activities that assist the establishment and maintenance of an ISO17799 compliant infrastructure, supports legal and contractual obligations and minimises and controls liabilities to Fujitsu Service's, and Post Office Ltd. The service monitors operations and introduces specific protective security controls on a risk assessment basis to maintain the integrity, availability and confidentiality of information used and produced by the various Services and the support environment.

Fujitsu Service's overarching obligations for delivering and continued provision of a secure system is set out in Clause 8 of the Agreement. The elements of the Security Management Services are described as follows:

- Implementation and maintenance of security policy and procedures
- Compliance monitoring and audit
- Cryptographic key management
- Security event management and firewall event analysis
- System and physical access control
- Anti-Virus and malicious software management
- Security incident reporting and problem management
- System security change management
- Security awareness and training
- Audit data retrievals and prosecution support
- Subject Information Requests management

Each of these services is described in Section 3.

2.0 Service Principles

2.1.1 The following service principles will apply in the provision of the Security Management Service. Security Management staff will:

a) Be appropriately trained to carry out the service;

b) Provide the appropriate balance between contractual and legal obligations and the need to maintain delivery of the various Services;

c) Be responsive to prevailing threats and vulnerabilities. Resource is therefore allocated on a flexible, risk management basis.

2.1.2 The Fujitsu Services' Information Security Manager shall have overall responsibility for the management of the service, but may delegate a suitable representative to act on his behalf, for:

FUJ00002000

a) Co-operating with the Post Office Information Security Manager in the development and operation of Post Office's network banking automation security policy as specified in paragraph 7.3.1 of Schedule 2 (Policies and Standards);

b) Establishing Fujitsu Service's security policy as specified in paragraph 7.3.2 of Schedule 2 (Policies and Standards);

c) Communicating to the Post Office Information Security Manager the identity of the persons authorised to receive sensitive security-related material (including cryptographic key components) on behalf of Fujitsu Services;

d) Receiving from the Post Office Information Security Manager the identity of the persons authorised to receive such security-related material on behalf of Post Office;

e) Liasing with the Post Office Information Security Manager and security representatives of other parties involved in the End to End Banking on such security-related matters as may be agreed.

3.0 Service Definition

3.1 Security Organisation and Management

This element of the service provides a number of organisational and management activities required for compliance with ISO17799:

- Co-ordination of security activities and prioritises activities according to risk;
- Input to contractual and liability issues and assessments of the security impact of new service requirements and the associated processes necessary to implement them;
- Creation and maintenance of security-related procedural and process documentation to assist compliance and help maintain correct operation by staff;
- Regular reviews of other Post Office Account documentation to provide appropriate security input and compliance to the requirements of ISO9001;
- Management of ISO17799 gap analysis, preparation of plan for implementation in accordance with agreed TOR and monitoring of corrective actions.

3.1.1 Fujitsu Service's obligations for the establishment of an organised security infrastructure, compliant to ISO17799 are set out in Schedule 2 – paragraphs 4.1.1 to 4.1.3.

3.1.2 Fujitsu Service's obligations for compliance with Post Office security standards are set out in Schedule 2 – paragraph 4.1.4.

3.1.3 Fujitsu Service's rights and obligations with regard to the security and processing of Personal Data are set out in Schedule 2 – paragraphs 2.4 to 2.8.

3.1.4 Fujitsu Service's rights and obligations with regard to the processing of Personal Data are set out in Schedule 2 – paragraph 2.4.6.

3.2 Compliance Monitoring and Audit

This element of the service provides a number of compliance monitoring and audit activities required for compliance with ISO17799:

3.2.1 Undertaking of periodic physical security and system security audits of operational sites on a risk management basis to provide ongoing assurance of compliance to security policies and procedures. Activities include reviews of operational processes, provision of reports covering IT, environmental, physical, personnel security etc. and the monitoring of identified corrective actions;

3.2.2 Provision of advice and guidance on issues affecting personnel security within Fujitsu Service's including the investigation of personnel security issues and staff vetting queries.

3.3 Cryptographic Key Management

This element of the service provides a number of cryptographic key management activities:

- Management of the automated Key Management System (KMS) for the creation, distribution and installation of required cryptographic material to the live estate. Maintenance of periodic key replacement for all Branches;
- Operation of functionality & configuration changes to the automated service to optimise service;
- Management of KMS event logging and incident handling to assist 1st, 2nd, 3rd and 4th line support in error resolution and problem management;
- Management of the manual cryptographic estate by maintaining the creation, distribution, auditing and periodic replacement of cryptographic keys within agreed timescales;
- Supplier management of cryptographic key suppliers;
- Provision of contingency arrangements for Key Management Service to maintain continuation of service in the event of absence etc.
- If requested by the Post Office Ltd, Fujitsu Services will on receipt of the appropriate forms, submit a completed Compliance Supplier Questionnaire in respect of A&L and CAPO.
- Fujitsu Services shall support Post Office Ltd in the completion of the annual LiNK Security Statement, by submitting a completed Compliance Supplier Questionnaire in respect of LINK when requested by Post Office Ltd.

FUJ00002000

In the event that the LINK Security Standard is updated, Post Office Ltd and Fujitsu Services Ltd will review the revised Link LIS specification and associated Security documents to identify any changes required to the service. The identification of changes and any subsequent implementation required will be handled through Change Control."

3.3.1 PIN Pads

The use of PIN Pads and the associated cryptographic management shall be supported by the NBS. PIN Pads shall comply with the requirements of ISO 9564. Fujitsu Service's key management for any key directly or indirectly protecting the secrecy of PIN values (together, "PIN Encryption Keys") shall comply with ISO 11568 Parts 1 to 3.

The key management scheme used between each PIN Pad and the rest of the Post Office Service Infrastructure shall be the DUKPT scheme as described in section 4.7 and Appendix A of the ANSIX9.24-2004 standard.

In the event of an actual or suspected key compromise in respect of a PIN Encryption Key used within the Post Office Service Infrastructure, Fujitsu Services shall implement key change mechanisms in accordance with the principles stated in ISO 11568 Parts 1 to 3.

The actual or suspected compromise affects a key shared with the NBX the parties' obligations in respect of key change mechanisms shall be as documented elsewhere.

3.4 Security Event Management and Firewall Event Analysis

This element of the service provides a number of security event management and firewall event analysis activities:

- Management of audit mechanisms to monitor detect and record events that might threaten the security of the Horizon system and associated services;
- Operation of the Security Event Management system utilising the Systems Management system to track and report events of security significance and daily monitoring of the system to identify relevant events and logging of details;
- Regular analysis of audit trails to identify new features and vulnerabilities introduced by new systems to facilitate trend analysis and to assist the investigation of security breaches;
- Reviewing security configurations of event filters to optimise efficiency and minimise security weaknesses;
- Undertaking risk assessments to establish adequate firewall policies / rule bases and the subsequent monitoring of events generated by the system;
- Analysis of firewall event logs using trend analysis software to identify the presence of any potential attacks or of areas of vulnerability and the provision of advice for any remedial action;

FUJ00002000

- Prompt investigation and remedial action in order to minimise the impact of any security breach.

3.5 System and Physical Access Control

This element of the service provides a number of system and physical access controls:

- Management of the process for validating that Users of the Horizon system are authorised before being permitted access to the live network;
- Management of the allocation and auditing of SecurID tokens where used to validate that Users who access the live system from locations remote from the Data Centres do so via secondary token authentication. Undertaking of supplier management of tokens and licensing costs.

3.6 Anti-Virus and Malicious Software Management

This element of the service provides a number of anti-virus and malicious software management activities:

- Management of the distribution of updated anti-virus software across the live estate to maintain protection of the service from malicious software;
- Initial configuration of alerting mechanisms and event filters to provide automatic notification and prompt virus incident response;
- Provision of regular DAT updates to identify and cleanse new and emerging virus strains;
- Daily checks of emerging viruses and other malicious software to inform threats and determine the required defensive measures;
- Provision of event monitoring and incident response via normal incident handling procedures. Analysis of details to understand the threat and inform corrective actions.

3.6.1 Protection Against Malicious Software for NBS

Fujitsu Services shall provide protection against malicious software as set out in paragraph 8.1 of the CCD entitled "*NBS Definition*".

3.7 Security Incident Reporting and Problem Management

This element of the service provides a number of security incident reporting and problem management activities:

- Provision of a central point of contact for all security-related issues;
- Investigation and reporting to Post Office of any actual or potential threats or breaches that may have a material effect on the Services in accordance with agreed procedures;

FUJ00002000

- Provision of ongoing liaison with Post Office and support to the Fujitsu Services' Security Board as defined in the CCD entitled "*Horizon Security Policy*" (RS/POL/002).

3.8 System Security Change Management

This element of the service provides a number of system security change management activities:

- Management of security compliance with agreed change processes and the assessment of the business and security impact of PinICLs and other problem management systems including the provision of options for resolution and containment of security and business risk;
- Assessment of the business and security impact of change proposals and the assessment and approval/rejection of security related operational change proposals.

3.9 Security Awareness and Training

This element of the service provides a security awareness programme for Fujitsu Services and relevant Post Office personnel. The service covers the provision of periodic awareness activities and training including induction training, presentations and briefing notes and input to magazines, journals and other periodicals.

3.10 Information Retrieval and Audit

3.10.1 For the purpose of this paragraph:

"Banking Transaction Record Query" means a Record Query in respect of a Banking Transaction which the Data Reconciliation Service has reconciled or has reported as an exception, the result or records of which are subsequently queried or disputed by Post Office or a third party;

"Audit Record Query" means a Record Query which is not a Banking Transaction but which relates to Transactions;

"APOP Voucher Query" means a Record Query for APOP Voucher archived records

"Old Data" means the extraction of records created before the 3rd January 2003, but not earlier than the 18th May 2002 before which data was automatically deleted, relating to Transactions, other than Banking Transactions meeting the Search Criteria, such extraction being limited to the following specific types of information/data fields: the ID for the User logged-on, Counter Position ID, stock unit reference, Transaction ID, Transaction start time and date, Customer Session ID, mode (e.g. serve customer), product number and quantity, and sales value, Entry Method, State, IOP Ident, Result, Foreign Indicator

"Period One" means, in respect of each Transaction the period of 90 days commencing on the date of that Transaction;

FUJ00002000

"Period Two" means, in respect of each Transaction the period commencing the day after expiry of Period One for that Transaction, expiring the earlier of the date:

a) Seven (7) years in the case of Transaction records up to and including the 18th May 2002 if created before commencement of the NB Pilot Soft (Soft Launch),

b) Of completion of transfer of Post Office Data (including the record of that Transaction) in accordance with Schedule 22.

"Query Day" means each date against which an Audit Record Query or an Old Format Query is raised;

"New Data" means the extraction of records created on and following the 3rd January 2003 in accordance with the terms of this paragraph 3.10 relating to Banking Transactions (and, in the case of Audit Record Queries relating to all Transactions) meeting the Search Criteria, such extraction being limited to specific types of information/data fields as follows:

- In the case of an Audit Record Query - the ID for the User logged-on, Counter Position ID, stock unit reference, Transaction ID, Transaction start time and date, Customer Session ID, mode (e.g. serve customer), product number and quantity, and sales value, Entry Method, State, IOP Ident, Result, Foreign Indicator; and
- In the case of a Banking Transaction Record Query - Banking Transaction ID, Banking Transaction type, receipt date, receipt time, the reason code (in the case of a discrepancy) and DRSH sub-value(s) (e.g. C0 Confirmation, C1 Confirmation, NB Decline); and
- In all cases an 'Event Log' will also be produced and provided with the Audit Record Query, detailing; GroupID, ID, Date, User, SU, EPOSSTransaction.T and EPOSSTransaction.Ti.

"Search Criteria" means:

- In the case of an Audit Record Query of either:
  a) Date or dates (not exceeding 31 consecutive days), Branch FAD and PAN (or equivalent identifier); or
  b) Date or dates (not exceeding 31 consecutive days), and Branch FAD Code; or in the absence of a FAD Code the full Branch Postal Address; and
- In the case of a Banking Transaction Record Query of either:
  c) Date, Branch FAD Code and PAN; or
  d) Date and Branch FAD Code,

To be specified for each individual Record Query or Old Format Query (as applicable).

3.10.2 Fujitsu Services shall have access (such access being restricted to properly authorised Fujitsu Service staff) to records of each Banking Transaction during Period One and Period Two.

FUJ00002000

3.10.3 Limits and Target Times for Record Queries

a) The table below sets out the limits on New and Old Format Queries which Fujitsu Services shall be obliged to carry out and the target times for carrying out each Audit Record Query:

	(1) Limits on Banking Transaction Record Queries carried out by MSU		(2) Limits on Audit Record Queries carried out by Security and Risk for Post Office
	Period One	**Period Two**	**Period One and Period Two**
Limits & Target Times	This process is actioned directly by Post Office Ltd means of the TESQA	Enquiries normally actioned via the TESQA, but no longer available due to expiry of the 180 day time limits set on the retention of data on the TESQA 100 per year (on a rolling year basis) with no more than 14 in any calendar month.	Subject to paragraph 3.10.6 below, the limit per year (on a rolling year basis) shall be the first of the following to be reached; (i) 720 Audit Record Queries consisting of Old or New Data or APOP Voucher Queries or (ii) (ii) 15,000 Query Days. The limit per calendar month, allowing a 'burst rate' of 14% shall be the first of the following to be reached: (i) 100 Audit Record Queries, of which not more than 10 shall be APOP Voucher Queries or (ii) (ii) 2100 Query Days subject to the constraints of the agreed annual limits above.

	(1) Limits on Banking Transaction Record Queries carried out by MSU		(2) Limits on Audit Record Queries carried out by Security and Risk for Post Office
	Period One	**Period Two**	**Period One and Period Two**

FUJ00002000

		7 Days, this task will be carried out within CS Security and will be met by provision of a simple query response as per the NBX Query provided on the Audit Retrieval System	Subject to paragraph 3.10.4 below and applicable only in respect of Audit Record Queries, consisting of data archived with effect from the 4th Jan 2003, 7 working days (for queries of 14 or less days' duration) and 14 working days (for queries of greater than 14 days' duration). Subject to paragraph 3.10.4 below and applicable only in respect of Audit Record Queries consisting of data archived between the 18th May 2002 up to the 3rd Jan 2003, 14 working days (for queries of 14 or less days' duration) and 28 working days (for queries of greater than 14 days' duration)

b) The limits set out in column number 1 in the table above and the provisions of this paragraph 3.10 relevant in connection with the application of those limits shall apply.

c) The limits set out set out in the column 2 in the table above and the provisions of this paragraph 3.10 relevant in connection with the application of those limits shall apply with effect from the date of approval by both parties of this document.

d) For the purpose of applying the limits in column 2 in the table above from the date of approval by both parties of this document, the equivalent Audit Record Queries (and associated Query Days) carried out in the 12 months prior to that date shall count towards the annual limit (on a rolling year basis).

e) For the purpose of applying the limits in column 2 in the table above from the date of approval by both parties of this document, the equivalent of Audit Record Queries carried out in the calendar month in which this document is approved (prior to the date of such approval) shall count towards the limits for that month.

3.10.4 Where:

a) A new Audit Record Query is received by Fujitsu Services or Post Office requires analysis of an existing Audit Record Query: and

b) A member of Fujitsu Service's personnel is needed to deal with that new or existing Audit Record Query; but

c) That person is unavailable due to his or her attendance at court or other proceedings in connection with an Audit Record Query,

FUJ00002000

d) The target times specified in paragraph 3.10.3 shall not apply to that new or existing Audit Record Query referred to in paragraph 3.10.4 (a) which Fujitsu Services shall instead deal with as soon as reasonably practicable.

3.10.5 For the avoidance of doubt, the limits set out in paragraph 3.10.3 in respect of Banking Transaction Record Queries shall not apply in respect of reconciliation incident management and settlement reporting carried out as a function of the Data Reconciliation Service.

3.10.6 Post Office may at any time on three months' notice vary the aggregate limits of Audit Record Queries which Fujitsu Services is required to carry out as specified in column numbered 2 in the table in paragraph 3.10.3, between

a) The limits specified in paragraph 3.10.3; and

b) The following substitutes for those limits (applicable on the same basis): 1020 Audit Record Queries or 21250 Query Days per year on a rolling year basis, and a maximum, allowing a 'burst rate' of 14%, of 142 Audit Record Queries or 2975 Query Days per calendar month

And between

c) The substitute limits set out in paragraph 3.10.6 (b) above, and;

d) The following substitutes for those limits (applicable on the same basis): 1500 Audit Record Queries or 31250 Query Days per year on a rolling year basis, and a maximum, allowing a 'burst rate' of 14%, of 210 Audit Record Queries or 4375 Query Days per calendar month

In each case Fujitsu Service's charges in respect of dealing with any Audit Record Queries up to the limits as varied in accordance with this paragraph shall be as specified in Schedule 10.

3.10.7 Post Office shall submit:

a) Banking Transaction Record Queries to the Horizon System Help Desk which will pass the Record Query to Fujitsu Service's customer service management support unit; and

b) Audit Record Queries and Old Format Queries to Fujitsu Service's customer service security prosecution support section.

Fujitsu Services shall accept Record Queries and Old Format Queries only from properly authorised Post Office staff.

3.10.8 Litigation Support

Where Post Office submits an Audit Record Query or Old Format Query, at Post Office's request Fujitsu Services shall, in addition to conducting that query:

a) Present records of Transactions extracted by that query in either Excel 95, Excel 97 or native flat file format, as agreed between the parties; and

FUJ00002000

b) Subject to the limits set out below:

(i) Analyse:

- The appropriate Fujitsu Service's Help Desk records for the date range in question;
- Branch non-polling reports for the Branch in question; and
- Fault logs for the devices from which the records of Transactions were obtained

c) In order to check the integrity of records of Transactions extracted by that query;

(ii) Request and allow the relevant employees of Fujitsu Services to prepare witness statements of fact in relation to that query, to the extent that such statements are reasonably required for the purpose of verifying the integrity of records provided by Audit Record Query or Old Format Query, and are based upon the analysis and documentation referred to in this paragraph 3.10.8; and

(iii) Request and allow the relevant employees to attend court to give evidence in respect of the witness statements referred to in (ii) above,

d) Provided that:

(iv) Fujitsu Service's obligations set out in (i) and (ii) above shall be limited, in aggregate, to dealing with a maximum of 150 (in aggregate) Record Queries and Old Format Queries per year (on a rolling year basis); and

(v) Fujitsu Service's obligations in the case of provision of witnesses referred to in paragraph (iii) above shall be to provide witnesses to attend court up to a maximum (for all such attendance) of 60 days per year (on a rolling year basis).

For the avoidance of doubt the target times set out in paragraph 3.10.3 for dealing with Audit Record Queries and Old Format Queries shall not apply in respect of Fujitsu Service's obligations under paragraph 3.10.8.(b).

3.10.9 Any information requested beyond that available by Record Query and/or any witness statements or witness attendance beyond that available in accordance with this paragraph 3.10 shall be agreed on a case by case basis and shall be dealt with in accordance with the Change Control Procedure.

3.10.10 Sensitive Card Data included in records of Banking Transactions extracted by Record Query and provided to Post Office (but, for the avoidance of doubt, not that included in records for Transactions extracted for Audit Record Queries in respect of any other Post Office Service) shall be in the encrypted form in which they are held by the NB System.

FUJ00002000

3.10.11 Audit Access. Reasonable access to the audit trail of Banking Transactions for Post Office auditors for audit purposes shall be by request and reasonable notice to the following:

- The Post Office Account Security Manager
- The Post Office Account Audit Manager.

FUJ00002000

3.11 Data Protection Act 1998 - Subject Information Requests

The management and provision of responses in respect of Subject Information Requests will be as defined in Schedule 2 of the Schedules of Agreement which are set out below.

3.11.1 Subject Information Requests

"Subject Information Request" means a valid request (as provided for in the Data Protection Act 1998) by or on behalf of a Customer or User for a copy of Personal Data of that Customer or User held or which may be held by Fujitsu Services;

"Response Capability" means in relation to any Subject Information Request for Personal Data in Transaction records held by Fujitsu Services notified to Fujitsu Services in accordance with paragraph 2.4.9, Fujitsu Services' ability to respond to that request within the applicable time limit taking into account the following factors:

3.11.1.1 The number, type and frequency of Subject Information Requests notified to Fujitsu Services and/or to which Fujitsu Services is already responding at the time of such notice;

3.11.1.2 The number of Audit Record Queries to which Fujitsu Services is also responding;

3.11.1.3 The processing time estimated by Fujitsu Services for retrieval of data required to satisfy each Subject Information Request;

3.11.1.4 Where Subject Information Requests and/or Audit Record Queries cover the same dates, whether contention for archive access could occur; and

3.11.1.5 The availability of workstations on which to do the work.

"Extraction Rate" means the rate at which information required to satisfy a Subject Information Request for Personal Data in Transaction records can be loaded from the archive, sorted as required and the necessary information transferred to CD ROM, including all associated intervening manual and automated processes.

3.11.2 Fujitsu Responsibilities

3.11.2.1 Fujitsu Services shall record and then refer all written Subject Information Requests (other than those notified to Fujitsu Services in accordance with paragraph 2.4.9 of Schedule 2) it receives to Post Office or (if Post Office shall have previously notified Fujitsu Services of the appropriate Data Controller contact name and address) to the appropriate Data Controller within five (5) days of receipt of the request, whether or not the request was received in error.

FUJ00002000

3.11.2.2 Post Office shall notify Fujitsu Services of each Subject Information Request it requires Fujitsu Services to deal with, providing the time limit applicable in respect of each such request and sufficient information in each case to enable Fujitsu Services to locate and retrieve the information requested or to confirm that the information is not held by Fujitsu Services, as the case may be. In respect of each Subject Information Request for Personal Data which are or may be held by Fujitsu Services in Transaction records, such information shall include the date or date range, the relevant personal identifier and, where available, the Branches to be covered by the search, giving the FAD code for each such Branch.

3.11.3 Subject Matter Requests - Provisions

3.11.3.1 The following provisions shall apply in respect of Subject Information Requests for Personal Data which are or may be held by Fujitsu Services in Transaction records: basis.

3.11.3.2 A Subject Information Request which satisfies the conditions set out below can be responded to by Fujitsu Services at an Extraction Rate of forty five (45) days worth of Transaction information per Branch requested per day. Each such Subject Information Request which, if processed at that rate (and allowing for other Subject Information Requests then being or which are required to be processed by Fujitsu Services) would be responded to within the time limit notified to Fujitsu Services for that request, shall be within the Response Capability of Fujitsu Services.

3.11.3.3 The conditions referred to above are that:

3.11.3.4 The FAD codes for the Branches covered by the Subject Information Request are provided to Fujitsu Services;

3.11.3.5 The period to which the Subject Information Request relates is between 45 and 90 consecutive days; and

3.11.3.6 The rate at which Audit Record Queries are being processed by Fujitsu Services at the time of receipt of the Subject Information Request is less than five hundred and eighty (580) per year on a rolling year basis.

3.11.3.7 Fujitsu Services shall assess and notify Post Office which of the Subject Information Requests notified to it by Post Office (other than those within the Response Capability in accordance with the above paragraphs can be responded to within the Response Capability and those in relation to which Fujitsu Services' ability to respond is outside the Response Capability.

3.11.3.8 If Fujitsu Services' ability to respond to a Subject Information Request is within the Response Capability, Fujitsu Services shall, subject to Fujitsu Services' current

FUJ00002000

and expected future workload for dealing with both Audit Record Queries and Subject Information Requests remaining the same or decreasing, respond to that request within the applicable time limit.

3.11.3.9 Subject to the paragraphs below, if Fujitsu Services' ability to respond to a Subject Information Request is outside the Response Capability, Fujitsu Services shall notify Post Office how long it would take to respond to that Subject Information Request, and shall (subject to Fujitsu Services' current and expected future workload for dealing with both Audit Record Queries and Subject Information Requests remaining the same or decreasing) respond to that request within Fujitsu Services' estimated response time plus 10% of that time.

3.11.3.10 If Fujitsu Services' ability to respond to a Subject Information Request is outside the Response Capability and Fujitsu Services reasonably believes that at its current workload it may never be able to respond to that request, it shall notify Post Office of that fact and Post Office may nevertheless request Fujitsu Services to respond to that request as soon as reasonably practicable. Post Office acknowledges and agrees that for so long as Fujitsu Services' ability to respond to such requests remains outside the Response Capability, Fujitsu Services will not be able to respond to them.

3.11.3.11 Unless agreed otherwise, Fujitsu Services' response to each Subject Information Request shall be in the form of an Excel (or other equivalent product) spreadsheet and shall be provided to Post Office (or the relevant Data Controller) on CD ROM.

3.11.3.12 Fujitsu Services shall seek to accommodate the priorities (of which it is notified) of Post Office for Subject Information Requests to be responded to in a particular order. Post Office agrees that if by accommodating such priorities, Fujitsu Services would be unable to achieve a time limit for a Subject Information Request to which Fujitsu Services is responding or is required to respond, that time limit shall not be applicable and (unless otherwise agreed) Fujitsu Services shall respond to such request as soon as reasonably practicable.

3.11.3.13 If the number, type and frequency of Subject Information Requests Fujitsu Services receives from Post Office and/or Data Controllers are such that some or all of those requests are not being responded to within applicable time limits or Fujitsu Services' ability to respond is or is forecast to be outside the Response Capability the following shall apply:

FUJ00002000

3.11.3.14 The parties shall assess the need for changes to the relevant system architecture and/or investment in additional hardware, software or other equipment to enable forecast numbers of Subject Information Requests to be responded to within applicable time limits, with any necessary consequential changes having been made to the Response Capability; and

3.11.3.15 Any such investment shall be the subject of a CCN and shall not be undertaken by Fujitsu Services without Post Office's prior agreement.

3.11.4 Subject Information Requests - Limitations

3.11.4.1 In respect of any Subject Information Requests to which paragraph 3.11.5 does not apply, Fujitsu Services shall respond to those requests as soon as reasonably practicable taking into account the time limits notified to Fujitsu Services for those requests and the technical limitations of any systems used to source the information requested.

3.11.5 Post Office Responsibilities

Post Office shall:

3.11.5.1 Be responsible for referring Subject Information Requests received by it from Fujitsu Services to the appropriate Data Controller;

3.11.5.2 Promptly notify Fujitsu Services when Post Office becomes aware that Fujitsu Services' assistance is required with a Subject Information Request; and

3.11.5.3 Pay Fujitsu Services' Charges for assisting with Subject Information Requests, but not for referring Subject Information Requests to Post Office or to third party Data Controllers, for which Post Office shall not be charged. Such charges to be calculated on a time and materials basis using Fujitsu Services rates set out in paragraph 6.2 of Schedule 10 (Charges).

3.12 Freedom of Information Act 2000 – Requests for Information

3.1.1 Freedom of Information Act

The Post Office Account Security Manager will act as the point of contact for all requests for information under the Freedom of Information Act 2000.

All requests by Post Office will be made in writing directly to the Post Office Account Security Manager within 3 working days of receiving such a request.

Post Office Account will within 5 working days of receiving a request put forward a response in order to provide Post Office with a timeframe and costing for responding to the request.

FUJ00002000

4.0 Compliance Monitoring and Audit

Horizon is subject to Monitoring and Audit Activities to ensure compliance with the BS ISO/IEC 17799 Code of Practise and the LINK Information Security Standard. This process will include:

- The periodic undertaking of physical security and system security audits of operational sites to ensure ongoing compliance to agreed security policies and procedures.
- Reviews of operational processes, key management processes, environmental, physical, personnel security, etc
- Production of Audit Reports and monitoring of corrective actions
- Advice and guidance on issues affecting personnel security within Fujitsu Services including the investigation of personnel security issues and staff vetting issues
- Assisting Post Office in completion of the Annual Security Compliance Statement to LINK.
- In the event of changes to the LINK Security Standards Post Office Account will review the LiNK Standards to identify any change in requirements

5.0 Service Availability

The Service will be available between the hours of 09:00 to 17:30 Monday to Friday excluding all Bank and public holidays.

6.0 Service Levels and Service Targets

Relevant SLA targets relate primarily to Audit Record Queries, which are defined in Section 3 of this document and Subject Information Requests which are defined in Schedule 2.

7.0 Service Dependencies & Post Office Responsibilities

7.1 Service Dependencies

7.1.1 The dependencies on the provision of Information Retrieval and Audit are set out in Section 10 of this document CS/SER/016.

7.1.2 The dependencies on the provision of Subject Information Requests are set out in Schedule 2 - paragraph 2.4.10.

7.2 Post Office Responsibilities

7.2.1 Post Office responsibilities with regard to the provision of an Information Security Manager are set out in Schedule 4.

FUJ00002000

7.2.2 Post Office's authority and obligations with regard to compliance with the Data Protection Act are set out in Schedule 2 – paragraphs 2.4 to 2.5.

7.2.3 Post Office responsibilities with regard to Subject Information Requests are set out in Schedule 2 - paragraphs 2.4.9 and 2.4.12.6.2.4