POL00397070

Document Title: HORIZON SECURITY POLICY

Document Type: Policy

Release: BI3 S75 onward

Abstract: This security policy specifies mandatory security requirements to be applied throughout Royal Mail Group Account.

Document Status: APPROVED

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

Contributors: Bill Membery ; Paul Halliden (PO)

Internal Distribution: Graham Chatten; Dave Baldwin; Richard Brunskill; Alex Robinson; Jan Holmes, Mark Wiltshire, Naomi Elliott, Hillary Forrest, Liam Foley, Colin Lenton Smith, Nial Finnegan, Ian Cooley, Dave Tanner, Jerry Acton, Sheila Bamber, Graham Welsh, Pete Thompson, Mik Peach. Dave Wilcox, John Burton, Chris Bridgeland.

External Distribution: Sue Lowther – Post Office Limited.

Dave Jackson, Andrew Gibson, Warren Welsh.

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

Name	Position	Signature	Date
Dave Baldwin	Business Director Retail & Royal Mail Group Account		
Colin Lenton-Smith	Commercial Director Royal Mail Group Account		
Mark Wiltshire	Programme Director Royal Mail Group Account		
Naomi Elliott	Service Director Royal Mail Group Account		
Brian Pinder	Security Manager Royal Mail Group Account		
Sue Lowther	Head of Information Security Post Office Limited		

POL00397070

Jan Holmes	Audit & Risk Manager		
Tony Wicks	Business Continuity Manager		

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 Post Office Limited	
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.	

POL00397070

8.0	03/09/02	Approved	
8.1	Jan 2003	Updates in line with BS ISO/IEC 17799 and inclusion of the Debit Card System	
9.0	24/01/03	Approved	
9.1	30/4/04	To reflect change to Royal Mail Group 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	
11.1	29/10/06	1st phase of two part review to reflect the contractual changes from ISO 17799 to ISO 27001 and to pick up on CISP requirement.	
11./2	08/Mar/07	To reflect changes after 1st review	
12	5/04/07	To reflect RMG contract changes	

0.2 Review Details

Review Comments by :	20 Feb 2007
Review Comments to :	Brian Pinder

Mandatory Review Authority	Name
Service Director RMGA	Naomi Elliott
Programme Director RMGA	Mark Wiltshire
Director Commercial RMGA	Colin Lenton Smith
Cryptographic Development RMGA	Alex Robinson*
Audit & Risk Manager RMGA	Jan Holmes*
IT Security Manager RMGA	Brian Pinder

POL00397070

Head of Information Security POST OFFICE LTD	Sue Lowther
Optional Review / Issued for Information	
Customer Services RMGA	Richard Brunskill*
Service Support Manager	Peter Thompson
Head of Service Transition & Change	Graham Welsh

(*) = Reviewers that returned comments

0.3 Associated Documents

Reference	Version	Date	Title	Source
PA/TEM/001			Fujitsu Services Document Template	PVCS
BS ISO/IEC 17799: 2005		16 June 05	Information technology Security techniques Code of practice for information security management	British Standard
ISO27001		Nov 2006	Information Security Management System Requirements.	British Standard
RS/PRO/002		28/04/06	RMGA Security Vetting Process	PVCS
RS/PRO/013		4/01/06	Horizon Security Pass Procedure	PVCS
RS/POL/003		14/04/05	Royal Mail Group Account Access Control Policy	PVCS
RS/POL/04			Computer Virus Policy	PVCS
RS/POL/010		29/03/07	Vulnerability & Risk Management Policy	PVCS
RS/FSP/001		01/02/06	Security Functional Specification	PVCS
CS/SER/016		06/03/06	Service Description for the Security Management Service	PVCS
CS/PRO/018			Incident Management Document	PVCS
CS / 3		29 Jan 03	Stop and Search	Intranet Site
ITS / 8		1 Aug 04	Classification and Privacy	Intranet Site

POL00397070

			markings	
ITS / 19		4 April 06	Facility Security	Intranet Site
PCI		Jan 2005	Payment Card Industry Data Security Standard	PCI
CISP			Community Information Security Policy	Post Office Document

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

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
FS	Fujitsu Services
ISO	International Standards Organisation
LFS	Logistics Feeder Service
NBS	Network Banking Service
NDA	Non Disclosure Agreement
OBCS	Order Book Control Service
PFI	Private Finance Initiative
PIN	Personal Identification Number
POL	Post Office Limited
PPP	Public Private Partnership
RMGA	Royal Mail Group Account
SEM	Security Event Management

POL00397070

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 Royal Mail Group 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.
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
11.1	Major amendments throughout document. 1st phase of two part review to reflect the contractual changes from ISO 17799 to ISO 27001 and to pick up on CISP requirement.
12.0	Minor changes after comments from POL at para 8.0

0.6 Changes Expected

Changes
ISO 17799 /Sections 10.5.1 – 15.3.2 Outstanding
Obligation and Applicability statements requirements and PCI requirements

POL00397070

0.7 Table of Contents

POL00397070

POL00397070

POL00397070

1.0 Introduction

In May 1996, Fujitsu Services (FS), Royal Mail Group Account (RMGA), 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, Royal Mail Group 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 Royal Mail Group Account to protect the integrity, availability and confidentiality of all assets associated with the services. It also enables Royal Mail Group Account to comply with legislative and commercial requirements.

1.1 Service Overview

The agreement is a PPP project, whereby Royal Mail Group Account automates approximately 14,000 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
- MoneyGram

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 FS and Prism, who share operational responsibility for the system. Security of the solution should be based on the current security agreement between POST OFFICE LTD and FS for running the Horizon systems. Areas deemed relevant to SAP are:

POL00397070

- Identification and Authentication
- Access Controls
- Audits and Alarms
- Network Security
- Virus Protection

2.0 Security Policy

This Security Policy specifies mandatory security requirements, which all Royal Mail Group Account staff must be compliant with. Any breaches of these requirements must be brought to the attention of the Security Manager for investigation.

Royal Mail Group 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 both FS and external parties who are required to work within the security framework defined by Royal Mail Group Account.

Royal Mail Group Account's Security Policy must be compatible with POST OFFICE LTD security policy. The interfaces between Royal Mail Group Account and all external organisations must be clearly defined and formally agreed with the companies concerned.

To ensure FS complies with their security obligations for subcontractors involved in development activities they are subject to individual NDA agreements with Royal Mail Group Account. Commercial off the shelf (COTS) products are provided by the appropriate product suppliers and subject to their own legal terms and conditions which FS must comply with.

This document fits into the structure illustrated below, with the BS ISO/IEC 17799:2005 Code of Practice being used as a basis for Royal Mail Group Account's Security Controls and Policy, and it is available within FS Intranet Site. Lower level implementation standards are incorporated into procedures and work instructions.

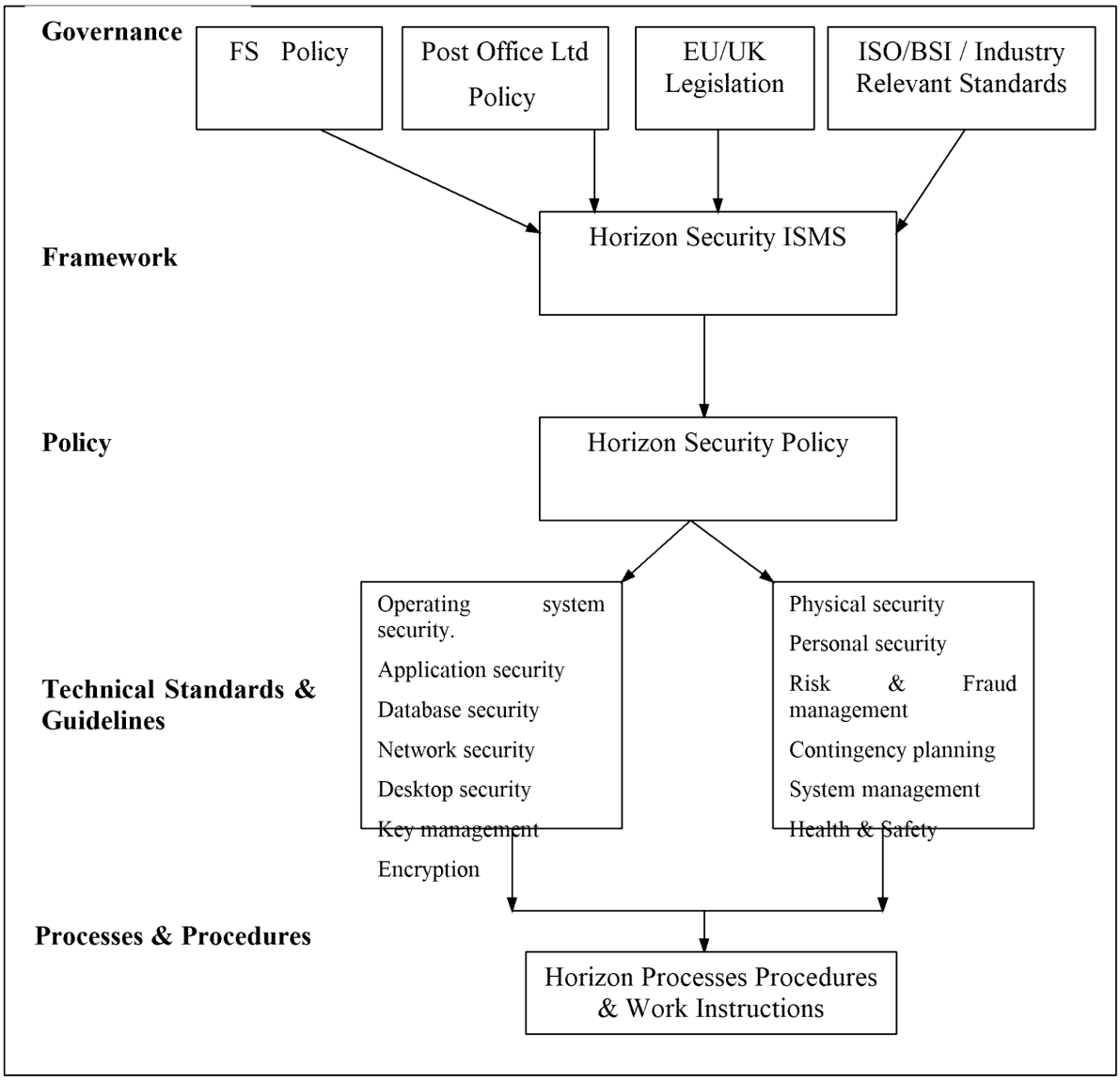
2.1 Management responsibility

Management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS by

- Establishing an ISMS policy
- Ensuring that ISMS objectives and plans are established;
- Establishing roles and responsibilities for security;
- Communicating to the organization the importance of meeting information security objectives
- Conforming to the information security policy, its responsibilities under the law and the need for continual improvement;
- Providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISMS
- Deciding the criteria for accepting risks and the acceptable levels of risk;
- Ensuring that internal ISMS audits are conducted
- Conducting management reviews of the ISMS.

POL00397070

2.2 Information Security Policy Structure



POL00397070

2.3 Policy Review

Once approved, this policy document must be formally reviewed annually based on a risk assessment. Formal reviews must take place after any major system change / new release, significant security incident or occurrence of fraud.

Responsibilities for approval, review and issue of Royal Mail Group Account's Security Policy and Procedures are defined in section 5

3.0 Objectives

This document is approved by Post Office Limited (POL) & Royal Mail Group Account (RMGA) senior management. It defines Royal Mail Group 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 Royal Mail Group Account to comply with legislative and commercial requirements.

Royal Mail Group Account's policy statement (which is essentially the same as the corporate policy statement used by Group (FS) is:

It is the policy of Fujitsu Services Royal Mail Group 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 Royal Mail Group Account. This includes assets owned by Post Office its clients its customers and its other suppliers which are entrusted to Royal Mail Group Account, and to ensure the confidentiality, integrity and availability of all information conveyed, processed, stored and transmitted.

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

The responsibilities for policy implementation are defined (in section 5) in order that the policy requirements can be communicated throughout Royal Mail Group Account. This ensures that all parties are fully aware of their responsibilities and legal obligations.

Royal Mail Group Account has stated its commitment to ensuring that it encompasses the very best commercial practices for security. Royal Mail Group Account's aim is to be fully compliant with BS ISO/IEC 17799: 2005.

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

3.1 Business Objectives

The business objectives are:

- Identifying and managing risks in a cost effective manner
- Protection of information assets
- Protection of IT assets
- Provide continuity of services
- Maintenance of Royal Mail Group Account's reputation.

POL00397070

3.2 IT Security Objectives

Royal Mail Group Account's overall IT security objective can be summarised as achieving the requirement expressed in the following:

1. Security measures in Royal Mail Group Account's IT systems must 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 must be controlled, with access granted selectively, and permitted only where there is a specific need. Access must be limited to persons, systems 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, Royal Mail Group Account's services.
4. All users of Royal Mail Group Account's services must be individually accountable for their actions. Accountability for information assets must be maintained by assigning owners, who should be responsible for defining who is authorised to access the information. If responsibilities are delegated then accountability must 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 Royal Mail Group 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 Royal Mail Group Account's services. These alarms should be used to trigger prompt investigation and remedial action in order to minimise the impact of any security breach.
7. Royal Mail Group Account will monitor all developments and operations that its services are performing to ensure a high level of confidence that all information is being protected during processing, transmission and storage to the approved security controls and policies.
8. All identified security requirements must be addressed before giving any worker access to Royal Mail Group Account information, documentation or assets.

4.0 Legal Obligations

Royal Mail Group 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 Royal Mail Group Account's operation.

5.0 Security Management Structure

Royal Mail Group Account's Business Unit Director has ultimate responsibility for security within Royal Mail Group Account.

POL00397070

The project's commitment to security must be communicated throughout RMGA as indicated by Security Cascades and Security Board Forum level approval of the RMGA Security Policies.

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

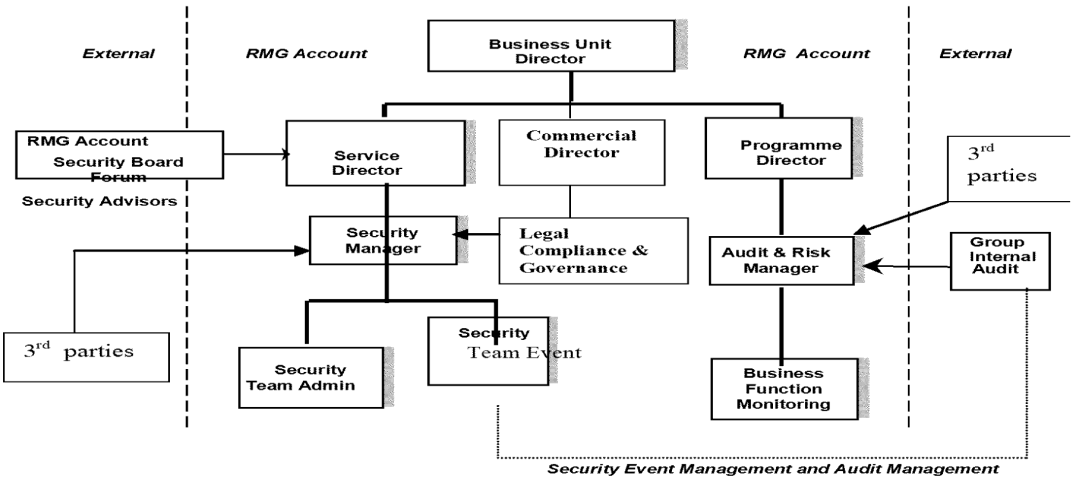


Figure 1 Royal Mail Group Account's Security Management Structure

5.1 Royal Mail Group Account Security Forum

The representatives on Royal Mail Group Account's Security Forum are nominated by the, Services Director, and approved by the Royal Mail Group Account Forum.

The Security Board Forum participants, must include Royal Mail Group Account Security staff, and 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 Forum responsibilities include:

- Ownership of Royal Mail Group Account's Security Strategy,
- Determining the adequacy of Royal Mail Group 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

5.2 Service Director

The security related responsibilities of the Service Director's include:

- Overall control and management of security throughout Royal Mail Group Account,
- Provision of adequate resources for security,

POL00397070

- Being Chairman of the Royal Mail Group Account Security Board Forum
- Owner of Royal Mail Group Account's Security Policy,
- Approval authority for Royal Mail Group Account's Security Policy,
- Approval authority for Royal Mail Group 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 – RMGA, but security risks have been delegated to the Service Director.

5.3 Security Manager

The Security Manager is responsible for ensuring implementation of policy and procedures, and maintaining "best practice", in line with all associated documents.

Royal Mail Group Account's Security Manager's responsibilities include:

- Physical and environmental security,
- Agree methodologies and processes with the Audit & Risk Manager for Information Security e.g. Risk assessment, information classification.
- Monitoring for compliance with Royal Mail Group 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 all workers on the RMGA including non- RMGA FS staff and sub-contractors must be screened in line with contractual requirements, FS Group Policy and this policy.
- Ensuring that security relevant events are recorded,
- Ensuring that system audit trails are analysed on a regular basis,
- Documentation of Royal Mail Group Account's Security Policy,
- Owner of Royal Mail Group Account's Security Procedures,
- Documentation of Royal Mail Group Account's Security Procedures,
- Identify significant security threat changes and exposure of information and information processing facilities to security threats.
- Communication of security policy and procedures throughout Royal Mail Group Account,
- Authorisation and approval for system changes,
- Co-ordinating the evaluation of all new security products proposed,
- Specifying and arranging security education and training, throughout the organisation.
- Devising and conducting security awareness programmes, throughout the organisation.
- Maintaining a partnership approach to security with Post Office Ltd Security staff,
- Liaison with the Post Office Ltd Information Security Manager, external regulators and suppliers' security personnel.
- In conjunction with PO Security, based on risk assessment, all 3rd party connectivity must be agreed.

POL00397070

- Reporting to the POST OFFICE LTD Information Security Manager any actual or potential threats or breaches that may have a material effect on any service, and
- Recruitment and selection of security administration personnel.

5.4 Security Administration

The description "Security Administration" is used to describe Royal Mail Group Account personnel assigned to roles with particular responsibility for security.

Royal Mail Group 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 5.3.

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 Royal Mail Group Account's Security Policy,
- Implement Royal Mail Group 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.

5.5 Security Event Management

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

Royal Mail Group 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 Royal Mail Group Account's systems is audited,
- Monitor usage by Royal Mail Group Account operations and management staff,
- Analyse the audit logs generated by the different Royal Mail Group 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 Royal Mail Group Account's Security Procedures (particularly with regard to audit),
- Report actual and suspected security incidents, and
- Recommend changes, to enhance Royal Mail Group Account's security controls, to the Security Manager.

POL00397070

5.6 Responsibilities for Physical Security

The local Site Managers have responsibility for physical security at all sites used by Royal Mail Group Account.

At some sites, notably Data Centres and support sites, Royal Mail Group 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 Royal Mail Group Account equipment installed

5.7 Responsibilities for Audit

The Director of Programmes is accountable for the Audit function within Royal Mail Group Account, as illustrated in figure 1.

The Audit Manager's responsibilities, listed in section 5.8, are primarily concerned with managing the internal Audit function within Royal Mail Group 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 Royal Mail Group Account groups (e.g. Customer Service, Programmes, Commercial and Finance) to co-ordinate audit related activities.

The Audit manager utilises the Event Management function, illustrated in figure 1, to enable him to obtain accurate and effective information for his audit processes.

5.8 Audit Manager's Responsibilities

Royal Mail Group Account's Audit Manager is responsible for ensuring implementation of Royal Mail Group Account's Audit Policy and checking best practice, based on contractual ISO standards.

The Audit Manager's responsibilities include:

- Planning and carrying out audits of Royal Mail Group Account's business functions,
- Examining and evaluating the results of (business function) audits,
- Developing and agreeing business improvement programmes,
- Monitoring and reporting improvement activities,
- Monitoring for compliance with Royal Mail Group Account's Audit Policy,
- Providing the point of contact for all audit related matters,
- Overall responsibility for Royal Mail Group Account's Audit activities,
- Documentation of Royal Mail Group Account's Audit Policy,
- Being the owner of Royal Mail Group Account's Audit Standards,
- Documentation of Royal Mail Group Account's Audit Standards,
- Communication of Audit Policy and standards within Royal Mail Group 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,
- Liaison with FS Group Audit personnel, and
- Recruitment and selection of Audit personnel.

POL00397070

5.9 Risk management Responsibilities

Senior Management will establish criteria against which security risk will be evaluated for all characteristics of RMGA including its organisational structure its locations, assets and technology, and including details of, and justifications for any exclusions from the scope, including the following;

5.9.1 Defining the risk assessment approach of RMGA:

- Identifying a risk assessment methodology that is suited to the ISMS, and the identified business information security, legal and regulatory requirements.
- Develop criteria for accepting risks and identify the acceptable levels of risk. The risk assessment methodology selected shall ensure that risk assessments produce comparable and reproducible results.

5.9.2 Risks are identified:

- Identifying the assets within the scope of the ISMS, and the owners of these assets. The term ‘owner’ identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. The term ’owner’ does not mean that the person actually has any property rights to the asset.
- Within PO Account this function is split into two areas, business risk and security risk. The policy for managing vulnerabilities is defined in RS/POL/010
- Identifying the threats to those assets.
- Identifying the vulnerabilities that might be exploited by the threats.
- Identifying the impacts that losses of confidentiality, integrity and availability may have on the assets.

5.9.3 Analysis and evaluation of the risks:

- Assessing the business impacts upon the organization that might result from security failures, taking into account the consequences of a loss of confidentiality, integrity or availability of the assets.
- Assessing the realistic likelihood of security failures occurring in the light of prevailing threats and vulnerabilities, and impacts associated with these assets, and the controls currently implemented.
- Estimating the levels of risks.
- Determining whether the risks are acceptable or require treatment using the criteria for accepting risks defined above.

5.9.4 Identification and evaluation options for the treatment of risks:

- Applying appropriate controls;
- Knowingly and objectively accepting risks, providing they clearly satisfy the organisation’s policies and the criteria for accepting risks see above.
- Avoiding risks,
- Transferring the associated business and security risks to other parties, e.g. insurers, suppliers.

POL00397070

5.9.5 Control objectives and controls for the treatment of risks.

- Control objectives and controls will be selected and implemented to meet the requirements identified by the risk assessment and risk treatment process. This selection will take account of the criteria for accepting risks as well as legal, regulatory and contractual requirements.
- The control objectives and controls from BS ISO/IEC 27001:2005 Annex A will be selected as part of this process to cover the identified requirements.
- The control objectives and controls listed in BS ISO/IEC 27001:2005 annex A are not exhaustive and additional control objectives and controls may also be selected.

5.9.6 Approve all proposed residual risks.

5.9.7 Authorise the implementation and operation of the ISMS.

5.9.8 Ensure the preparation of a Statement of Applicability that includes the following:

- The control objectives and controls selected and the reasons for their selection
- The control objectives and controls currently implemented.
- The exclusion of any control objectives and controls in BS ISO/IEC 27001:2005 annex A and the justification for their exclusion.

NOTE: The Statement of Applicability provides a summary of decisions concerning risk treatment. Justifying exclusions provides a cross-check that no controls have been inadvertently omitted.

5.10 Business Function Monitoring Responsibilities

The description "Business Function Monitoring" has been used to describe Royal Mail Group Account personnel assigned to roles with particular responsibility for Audit.

Royal Mail Group 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 5.8.

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 Royal Mail Group Account's Audit Policy,
- Implement Royal Mail Group Account's Audit Standards,
- Conduct independent reviews of compliance to policy and standards,
- Report actual and suspected security incidents, and
- Recommend changes, to enhance Royal Mail Group Account's audit controls, to the Audit Manager.

6.0 All Personnel Security Awareness

All Royal Mail Group Account service users must be subject to Royal Mail Group Account's awareness and/or training programmes. Security aspects are an integral part of these programmes and should be set in a context appropriate to the user's role.

POL00397070

All Royal Mail Group Account workers, 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 Royal Mail Group Account, to subcontractors, and temporary staff is an important responsibility assigned to Royal Mail Group Account's Security Manager. Publicising security reporting and escalation procedures must be part of this awareness strategy.

6.1 Security Education and Training

eRoyal Mail Group Account's education and training programme must promote security awareness through the provision of regular updates, security briefings, explaining the importance and use of security controls. It should also monitor individual's security training and ensure appropriate training is provided for contractors and third parties.

7.0 Co-operation between Organisations

Appropriate contacts with law enforcement authorities, regulatory bodies, information service providers and telecommunications operators must be maintained to ensure that appropriate action can be quickly taken, and advice obtained, in the event of a security incident. Similarly, membership of security groups and industry forums should be considered. Exchanges of security information should be restricted to ensure that confidential information is not passed to unauthorised persons.

8.0 Classification of Information

8.1 Information Control

Information must be classified to indicate the need, priorities, and expected degree of protection when handling the information. Information has varying degrees of sensitivity and criticality e.g. financial information or highly confidential information and information often ceases to be sensitive or critical after a certain period of time, for example, when the information has been made public. Some items may require an additional level of protection or special handling. An information classification scheme is used to define an appropriate set of protection levels and communicate the need for special handling measures. These aspects should be taken into account, as over-classification can lead to the implementation of unnecessary controls resulting in additional expense.

Royal Mail Group Account (FS) defines agrees and enforces (with relevant parties) procedures for the exchange of information handled "***electronically and by other means***". The procedures used must comply with FUJITSU legal and contractual requirements and must depend upon the classification and sensitivity of the information. In particular, the exchange of information, with Post Office Ltd, must be subject to formally agreed controls based on the classification and sensitivity of the information transmitted.

8.2 Overview of Policy

Information owners, both Post Office Ltd and FUJITSU staff are required to classify all information that they own. All information used must be handled in accordance with its classification, as

POL00397070

specified by its owner in line with existing Policy. FS staff can find reference to this on the site Intranet and Post Office Ltd have their own classification system which is available in the CISP (S1).

8.3 General Principle

The sensitivity of information must be measured by the consequences of a potential security breach associated with that information. Royal Mail Group Account should assume that aggregation cannot increase the classification of any information unless risk assessment indicates otherwise.

8.4 FJS Security Classifications

Personal:

This privacy marking applies to matters relating to named individuals where disclosure could render the company liable to prosecution under privacy legislation such as the UK Data Protection Act.

Staff:

This privacy marking applies to matters relating to staff and their services, where the subject matter under discussion could apply to a group of staff, and where disclosure or unauthorised access could lead to commercial embarrassment or staff discontent.

Unclassified:

Unclassified information is that which by its nature can be made publicly available. This is either because it has no commercial value or its publication would enhance the reputation of the Company. Declassification is not applicable in this case.

There is no need to mark unclassified material, unless it is believed that there is a need to indicate that the material is unclassified because others of a similar type are classified.

Where a document contains pages of differing classifications the highest classification must be marked on the covers.

Eyes Only:

These classifications apply to information and material, the unauthorised disclosure or loss of which could cause embarrassment or might be detrimental to the interests of all or part of the Company, but where such impact would not be severe or cause long term damage.

At company level, the following should be used and recognised:

FUJITSU EYES ONLY - Should be available only to employees of Fujitsu and trusted contractors.

FUJITSU SERVICES EYES ONLY - Should be available only to employees of Fujitsu Services and trusted contractors.

Qualifications can also be business specific. In such cases these qualifications must be defined by local policies. The term 'EYES ONLY', or a consistent translation in the local language, must be used.

POL00397070

Where a document contains pages of differing classifications the highest classification must be marked on the covers.

Commercial in Confidence:

This classification applies to information and material, the unauthorised disclosure of which could cause embarrassment or might be detrimental to the interests of the Company, but which nevertheless can be shared with third parties if necessary for business purposes.

Where a document contains pages of differing classifications the highest classification must be marked on the covers.

Company Restricted:

Information whose unauthorised disclosure (even within the organisation) would cause significant harm to the interests of the organisation. This would normally inflict harm by virtue of financial loss; loss of profitability or opportunity; embarrassment or loss of reputation.

Documents and material classified COMPANY RESTRICTED should, unless otherwise stated, be downgraded to FUJITSU EYES ONLY after two years.

Company Secret:

This classification is for information and material of an extremely confidential and sensitive nature, or of strategic importance, the disclosure of which could cause grave damage to the interests of the Company.

Documents and material classified COMPANY SECRET must, unless otherwise stated, be downgraded to FUJITSU EYES ONLY after two years.

All pages must be consecutively numbered to reflect the total number of pages e.g. 1 of 6, 2 of 6 etc. Copies must be numbered in the same manner i.e. 1 of 6 copies etc.

A distribution list must be attached showing the copy number of copies sent to each recipient.

8.5 POST OFFICE LTD Classifications

Information security classification

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

Horizon information that is generated, processed, communicated or stored within the Horizon community, either physically or electronically, must be assessed to identify its level of security classification and determine the protective controls to be applied.

Royal Mail Group's Information Classification Policy (S4) and associated guidelines must be used for this purpose. This defines two levels of confidentiality, for which the classification given below must be used:

- **CONFIDENTIAL**: Information that has been assessed to be of a sensitive nature and likely to cause damage following unauthorised disclosure. Personal data (as defined by the Data Protection Act) is classified as confidential. Personal data includes customer account numbers and any transaction data associated with them. FAD codes are sometimes used

POL00397070

for authentication purposes and must therefore be treated as confidential. Transaction records that do not identify a person are confidential on bulk data/reports only. Transaction receipts for individual transactions do not need to be labelled as CONFIDENTIAL, since they are intended as a receipt for a transaction by an individual.

- **STRICTLY CONFIDENTIAL**: Information meeting the classification standards of government departments, the security services, clients, or assessed to be so sensitive that unauthorised disclosure would cause acute organisational damage. PIN data and all encryption keys are interpreted as strictly confidential.

All other information must be classified as INTERNAL unless specifically authorised for release. See §**Error! Reference source not found.** in RM/POL/002 for INTERNAL information which may need to be released under the Freedom of Information Act.

All documentation and displayed output from systems containing information classified as confidential or strictly confidential must carry an appropriate classification label.

There are also legal requirements concerning the release of information – see §**Error! Reference source not found.** (RM/POL/002) for more information.

9.0 Asset Management

All major information assets identified must where possible, have an assigned named owner who must be responsible for ensuring the integrity, availability and confidentiality of the asset. This should include the provision and maintenance of an asset register and up to date inventories of all significant component assets – information, software, hardware and services.

9.1Asset Inventory

Information can be held in various forms, and an asset inventory should be maintained for each. All assets shall be clearly identified and an inventory of all important assets drawn up and maintained. The inventory should 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.

9.2 Accountability for Assets

Owners must have sufficient authority and knowledge to allow them to appreciate the value of their system and or information. They must be responsible for classifying the asset they own, and therefore ensuring that sufficient protection is being applied and maintained. The protection required must be commensurate with the value and the risk.

Custodians are appointed by the asset owners to undertake day-to-day tasks and make operational decisions on behalf of the owner.

POL00397070

9.3 Responsibility & Ownership

A management authorisation process for new information processing facilities must be defined and implemented.

The following guidelines must be considered for the authorisation process:

a) New facilities must have suitable user management authorisation, authorising their purpose and use. Authorisation must also be obtained from the manager responsible for maintaining the local information system security environment to ensure that all relevant security policies and requirements are met;

b) Where necessary, hardware and software must be checked to ensure that they are compatible with other system components;

c) The use of personal or privately owned information processing facilities, e.g. laptops, home-computers or hand-held devices, for processing business information, may introduce new vulnerabilities and necessary controls must be identified and implemented.

10.0 Personnel Security

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

Staff working on high-risk areas (those IT systems classified as "critical" or information classified as "sensitive") are to be subject to more frequent vetting reviews and internal audits. This also applies to Royal Mail Group Account's own employees, particularly those staff visiting PO sites and to staff from subcontractor's companies. For those staff visiting PO sites there is an enhanced clearance process detailed in RS/PRO/002 which is managed by Royal Mail Group Account Security staff.

Security awareness must be addressed at the recruitment stage, and referred to in job descriptions, contracts and monitored during an individual's employment with the Royal Mail Group Account. Users must be trained in security procedures and the correct use of information and systems.

Incidents affecting security must be reported through management channels and in accordance with escalation procedures. All employees and contractors must be made aware of how to report such incidents. There must be an established formal disciplinary process for dealing with employees who commit security breaches.

10.1 Job Descriptions, Contracts and Assessment

Royal Mail Group Account must apply best commercial practice, based upon BS ISO/IEC 17799, to include security considerations within, employee's terms and conditions for employment, and generic job descriptions.

10.2 Recruitment Selection

All applicants are subject to an appropriate level of vetting as described in RS/PRO/002 "RMGA Security Vetting Process". Criteria for those staff requiring access to Post Office outlets is defined within RS/PRO/013 "Horizon Security Pass Procedure" and for access to the Horizon network RS/PRO/003, "Access Control Policy".

POL00397070

10.3 Confidentiality Agreements

All employment contracts (permanent and temporary) as well as consultant, contractor and supplier contracts must include clauses governing the treatment of Royal Mail Group Account information gained as a result of their employment. This may be achieved through signing a non-disclosure agreement or personal integrity form. Staff must be informed that the use of or removal of, Post Office information by ex-Royal Mail Group Account staff, gained during their employment with RMGA, may result in prosecution by the Royal Mail Group Account or the Information Commissioner.

Contracts must make it clear to employees that they are required to comply with the Information Security Policy and Standards. Each employment contract must be signed by the employee.

10.4 Management Responsibility

All Managers must ensure that employees, contractors and third party users apply security in accordance with agreed PO & FS policies and procedures. They must ensure that staff are properly briefed and comply with the terms and conditions of their employment and both their company's information security policy and if working on Horizon this Security Policy.

10.5 Termination Procedures

Procedures must be established to re-define security responsibilities when staff, including contractors and consultants, are moved within the Royal Mail Group Account or whenever their employment ceases for any reason or when moving to other parts of Fujitsu.

The access rights of all employees contractors and 3rd party users to information and information processing facilities must be removed upon termination of their employment contract or agreement or adjusted upon change, including revoking their rights to the system and escorting them from all Horizon premises.

Where staff move within the Royal Mail Group Account, computer access must be modified or terminated as appropriate to their change of role.

Any specific security responsibilities of the departing individual must be reviewed and reallocated.

10.5.1 Return of Property

When RMGA staff leave Line managers must have formal procedures in place to ensure the return of all Royal Mail Group Account property where applicable.

10.5.2 Network Access Removal

Line managers should ensure that individual access, roles, permissions and capabilities to both physical and information systems are revoked on termination of employment.

Group, system utility or generic administrator accesses using shared, default, or known-sequence passwords, safe combination numbers, etc, must be changed on the departure of a member of the team.

POL00397070

10.6 Reporting Security Incidents and breaches

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

All security incidents must be reported to the Royal Mail Group Account Security Manager or his deputy who are responsible for ensuring that all incidents are recorded, investigated and resolved with appropriate urgency. This should include liaison with Post Office Security staff to review relevant incidents and actions.

11.0 External Contractors and Suppliers

To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties, the security of Horizon's information and information processing facilities should not be reduced by the introduction of external party products or services. Any access to the Horizon information processing facilities and processing and communication of information by external parties must be controlled.

Prior to commencement Royal Mail Group Account must ensure that appropriate safeguards cover the use of external contractors and suppliers, (including agreements on contractual terms and conditions, checks on the integrity of external contractors) before any work is assigned to them.

Prior to commencement the risks to the Horizon information and information processing facilities from any business processes involving external parties must be identified and appropriate controls implemented before granting access. Controls must be agreed, documented and defined in agreements with any external parties.

External personnel must receive appropriate training and regular updates in organisational policies and procedures including security requirements, legal responsibilities, business controls and training in the correct use of information processing facilities.

External personnel must 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 must 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 must be sought where externally supplied goods or services are used to process sensitive information.

12.0 Physical & Environmental Security

12.1 Policy

To prevent unauthorised access damage and interference to critical or sensitive business information processing facilities, all business premises housing Horizon assets must be housed in secure areas, protected by a defined security perimeter with appropriate security barriers and entry controls.

They must be physically protected from unauthorised access damage and interference their protection must be commensurate with any identified risk. Clear desk and clear screen policies are

POL00397070

required to reduce the risk of unauthorised access or damage to papers media and information processing facilities.

The selection and design of a secure area must take account of the possibility of damage from fire, flood, explosion, civil unrest and other forms of natural or man made disasters. Account should also be taken of relevant health and safety standards. Consideration must be given also to any security threats presented by neighbouring premises.

12.2 Perimeter Security Measures

The actual measures to be applied must be appropriate to the nature and amount of information, IT systems and telecommunications facilities at the site. Intrusion detection alarm systems must be used for installations which are left unattended. These may be connected to a security company or the Police. Alarm systems must be tested regularly and maintained to manufacturers' requirements.

Access points must be kept to a minimum and be subject to auditable access control measures. Emergency exits and other external doors must be fitted with alarms. Security perimeters must be clearly defined. The perimeter of a building or site containing information processing facilities must be physically sound (i.e. there must be no gaps in the perimeter or areas where a break in could easily occur). The external walls of the site must be of solid construction and all external doors must be suitably protected against unauthorised access e.g. control mechanisms bars, alarms lock etc. A manned reception area or other means to control physical access to the site or building must be in place. Access to sites and buildings must be restricted to authorised personnel only. Physical barriers must if necessary be extended from real floor to real ceiling to prevent unauthorised entry and environmental contamination such as that caused by fire and flooding. All fire doors on a security perimeter must be alarmed and must slam shut. Unoccupied secure areas must be physically locked and subject to periodic checks, and there must be physical protection and guidelines for those staff working in secure areas.

12.3 Securing Offices Rooms and Facilities

All key facilities must be sited to avoid access by the public. Buildings must be unobtrusive and give minimum indication of their purpose, with no obvious signs outside or inside the building identifying the presence of information processing activities.

Support functions and equipment e.g. photocopiers fax machines must be sited appropriately within the secure area to avoid demands for access which could compromise information.

Doors and windows must be locked when unattended and external protection must be considered for windows particularly at ground level. Suitable intruder detection systems must be installed to professional standards and regularly tested to cover all external doors and accessible windows unoccupied areas should be alarmed at all times cover must be provided for other areas e.g. computer rooms or communication rooms.

Information processing facilities managed by RMGA must be physically separated from those managed by third parties. Directories and internal telephone books identifying locations of sensitive processing facilities must not be readily accessible by the public.

Hazardous or combustible materials must be stored securely at a safe distance from a secure area. Bulk supply such as stationary must not be stored within a secure area until required. Fallback

POL00397070

equipment and backup media must be sited at a safe distance to avoid damage from a disaster at the main site.

12.4 Loading and Delivery Areas

Loading and delivery areas must be designed to ensure that supplies can be delivered or loaded without compromising secure areas, and consideration should be given to using an interlocking door mechanism.

12.5 Secure Areas

All secure areas must be compliant with FS Policy no ITS / 19 “Facility Security” and CS/3 “Stop and Search”.

All areas must be considered on the basis of a risk analysis and appropriate controls must be put in place based on the security risk.

12.6 Equipment, Cabling & Utilities

All equipment and cabling must be well maintained and protected against environmental hazards, including fire and water damage. All supporting utilities such as water, electricity air conditioning must be adequate for the systems they support and should be regularly tested and inspected to reduce the risk of malfunction and ensure their availability and integrity. Off site equipment must be stored securely and adequately protected.

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

Similar considerations apply to Royal Mail Group Account assets at other non-Royal Mail Group Account sites (e.g. AP Client sites).

12.7Access Points

Access controls must be enforced at all entry points to Royal Mail Group Account premises, except those open to the public. Additional controls must be applied to areas containing sensitive information or time critical services.

12.8 Control of Visitors

Visitors must have a Royal Mail Group Account sponsor, who must be responsible for that visitor whilst they are within a Royal Mail Group Account facility.

Visitors must only be granted access for specific and authorised purposes and must be issued with instructions on the security requirements of the area and of emergency procedures.

Access to sensitive information and information processing facilities must be controlled and restricted to authorised persons only.

Authentication controls (e.g. swipe card plus PIN) must be used to authorise and validate all access.

An audit trail of all access must be securely maintained.

POL00397070

All personnel must be required to wear some form of visible identification and must be encouraged to challenge unescorted strangers and anyone not wearing visible identification. Access rights to secure areas must be regularly reviewed and updated.

13.0 Protection of Horizon Documentation and Media

All documentation whether held in hard copy or held electronically must be classified have clearly defined ownership and review times, controlled and auditable.

13.1 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.

13.2 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.

13.3 Protection of Back-up Media

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

14.0 Maintenance and disposal of IT Equipment

14.1 Maintenance of IT equipment

IT equipment including computers, telecommunications and other electronic equipment must be maintained in accordance with manufacturers and suppliers recommended service intervals and specifications.

14.2 Disposal of IT equipment

14.2.1 Removal of Data

Data and licensed software must be erased from IT equipment prior to its disposal. Care should be exercised as 'deleted' data can in certain instances be retrieved using specialist equipment.

Where data or licensed software cannot be erased for technical reasons, the hard disk, floppy disks, etc, should be destroyed by appropriate means, e.g. shredding, degaussing or in extreme cases incineration, to prevent data retrieval.

As a minimum, hard or floppy disks should be reformatted, overwritten with '0' and 'X' and then reformatted again. Where confidential or secret data has been stored on the disk, or where for technical reasons it cannot be overwritten or reformatted the disk must be destroyed as follows:-

- Floppy Disks - Shredded, Degaussed or Incinerated

POL00397070

- Hard Drives - Degaussed or Incinerated
- Tape Reels - Degaussed or Incinerated
- Cartridges - Degaussed or Incinerated
- CD / DVD - Abrasion, Compacting or Incineration

14.2.2 Removal of Hardware

All Equipment, information or software must not be removed from site without authority.

15.0 Computer & Network Management

15.1 Policy

Information systems and networks must be managed effectively to ensure their integrity, availability and confidentiality, and to prevent their accidental or deliberate misuse.

15.1.2 General Principle

Responsibilities and procedures for the management and operation of all computers and networks must be established and supported by appropriate instructions and guidelines to ensure their correct and secure operation.

15.1.3 Operating Procedures

Clear, documented operating procedures must be developed for all operational computer systems, to incorporate instructions on:

- Handling of data files.
- Scheduling requirements.
- Error handling.
- Support contacts in the event of unexpected operational or technical difficulties.
- Handling of special output.
- System restart and recovery procedures.

Documented procedures must also be prepared for system housekeeping activities associated with computer and network management, including details for:

- Computer start-up and close-down.
- Data backup.
- Equipment maintenance.
- Computer room management and safety.

Operating procedures must be treated as formal documents. Changes must only be made after approval by authorised management, using the change management system.

POL00397070

16.0 Segregation of Duties

Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
Segregation of duties must be used to minimise the risks of accidental or deliberate system misuse.

The management must reduce the opportunities for unauthorised modification or misuse of information or services by ensuring the execution of certain duties and areas of responsibility are segregated. Care must be taken to ensure that no single person can perpetrate a security incident by having an area of single responsibility without this being detected.

17.0 Access Control Policy

The objective is to prevent unauthorised computer and network access. Security facilities at the operating level must be used to restrict access to computer and network resources. Specific detailed access controls must be published with the Horizon Access Control Policy (ACP) RS/POL/003.

Access to information, information processing facilities, and business processes must be controlled on the basis of business and security requirements. Access control rules should take account of policies for information dissemination and authorisation.

Access control rules and rights for each user or group of users must be clearly stated in an access control policy. Access controls are both logical and physical and these must be considered together. Users and service providers must be given a clear statement of the business requirements to be met by access controls.

The Access Control Policy and associated Security Procedures must take account of:

- Clear definition of responsibilities for all authorised users,
- Specification of roles and responsibilities for all types of system usage,
- Control of access by external users.
- Security requirements of individual business applications.
- Relevant legislation and any contractual obligations regarding protection of access to data services.
- The identification of all information related to business applications & the risks the information is facing.
- Recording failed and successful system accesses.
- Consistency between the access control and information classification policies of different systems and networks.
- Policies for information dissemination and authorization, e.g. the need to know principle.
- Security levels and classification of information
- Control of access to all Royal Mail Group Account systems components,
- Where appropriate restricting the connection time of users.
- Requirements for formal authorisation of access requests.
- Requirement for periodic review of access controls.
- Removal of access rights.
- Control of access to all data within the Royal Mail Group Account systems,
- Control of access to all stored information and documentation,

POL00397070

- 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,
- Standard user access profiles for common job roles in the organisation.
- Management, assignment and revocation of privileges,
- Management of access rights in a distributed and network environment recognising all types of connections available.
- Identification and authentication of human and system “users”, and
- Password management, including password generation and expiry and quality passwords
- segregation of access control roles, e.g. access request, access authorization, access
- administration.

Accountability of individuals is essential and segregation of duties must be enforced. Wherever authorisation is given orally, normally over a telephone link, additional verification methods must be used.

17.2 User Access Management

Formal procedures should be in place to control the allocation of access rights to information systems and services. The procedures should cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention should be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls.

18.0 Development, Test and Operational Facilities.

To reduce the risk of accidental changes or unauthorised access to operational systems or data:

- Development, Test and Operational facilities must be segregated;
- Different logon identities should be used for operational and test systems.
- System utilities should be stored separately from operational systems.
- User menus for test systems must display appropriate identification messages.

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

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

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

POL00397070

All software is must be to appropriate acceptance procedures and testing prior to integration with other components.

19.0 Capacity Planning

Capacity requirements must be monitored to avoid failures due to inadequate capacity. Future capacity projections must be made to ensure that processing power, network capacity and storage remain available, and to identify and avoid potential bottlenecks.

20.0 Third Party Service Delivery Management

Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, must be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.

21.0 Configuration Management

The Horizon Solution must be subject to strict configuration management procedures and principles as defined within the Security Functional Specification (RS/FSP/001).

22.0 Cryptography

Royal Mail Group Account must comply with Post Office requirements with regard to the encryption of their Data. It also complies with relevant regulatory requirements and with BS ISO/IEC 17799: 2005 standards for the handing of cryptographic key material in accordance with agreed contractual obligations.

Royal Mail Group Account should 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).

23.0 Administration of Security

The following subsections provide an overview of the controls required within Royal Mail Group Account. Royal Mail Group Account's Security Procedures provide further guidance, based upon the BS ISO/IEC 17799: 2005 controls, for:

- Computer and network management, and
- System development and maintenance.

23.1 System and Network Management

Operational management of the system, applications and network is under the control of Operations and Support within Royal Mail Group Account.

POL00397070

The system privileges and access permissions required to perform management functions are considerably higher than those assigned to normal users. Royal Mail Group 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.

23.2 Audit Management

Royal Mail Group 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
- Audit trails are archived and stored for an agreed duration.

23.3 System Acceptance Methods

Royal Mail Group Account must ensure that acceptance criteria is established and documented for all systems (including new, updated, and new versions). These must identify and incorporate acceptance testing requirements. The following items should be considered:

- Identification and authentication of human and system “users”,
- Control of access to information and services,
- Segregation of duties,
- Secure operation in degraded mode,
- Incorporation and analysis of audit trails,
- Data and system integrity protection,
- Use of encryption to prevent unauthorised disclosure and/or modification of data, and
- System resilience, including operation in fallback mode and recovery.

All software developed by or for Royal Mail Group Account must be acceptance tested based on proven methodologies which take care that:

- Input data validation is comprehensive and reliable,
- Processing protects against errors and attacks, and
- Integrity checking is performed.

POL00397070

24.0 Change Control Procedures

24.1 Change Control

There must be strict control over the implementation of changes to the software or hardware of any Royal Mail Group Account system, application or network. Such change control procedures must ensure that any changes do not compromise any security or control procedure. The Change Control Policy will mandate the course of action required for hardware, network, system and application changes. 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.
- Quality and content control.
- The maintenance of a full record of all changes (audit trail)
- The deletion of any temporary User IDs/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.

24.2 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.

24.3 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 cannot be compromised by the proposed changes.

25.0 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 miss-configuration

POL00397070

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.

Royal Mail Group Account must adopt industry standard best practise and BS ISO/IEC 17799: 2005 recommendations by implementing vulnerability management.

26.0 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 Royal Mail Group Account users must be made aware of the dangers of unauthorized or malicious software, and controls including the protection, based on the Computer Virus Policy RS/POL/04. Managers must where appropriate introduce controls to prevent, detect and remove malicious code and control mobile code (this applies to all workers and networks connecting to the Horizon network.)

There must be 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.

Precautions are required to prevent and detect the introduction of malicious code and unauthorised mobile code.

The AV security Policy must provide protection from unauthorised access from any utility operating system software and malicious software that is capable of overriding or bypassing system or application controls. Procedures against malicious software must be in place and kept up to date.

27.0 Control of Proprietary Software

Royal Mail Group Account uses proprietary software within the terms of the licence conditions.

Unauthorised copying of software and documentation is prohibited.

Royal Mail Group Account must 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 Royal Mail Group Account's Security Manager.

Royal Mail Group Account's configuration management system must maintain an inventory of all proprietary software used by all services.

28.0 Business Continuity

Royal Mail Group Account ensures that an effective business continuity plan is agreed with Horizon Security staff and implemented to reduce the risks from deliberate or accidental threats to deny access to vital services or information.

POL00397070

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 must be maintained, even if degraded conditions are in effect.

28.1 Contingency Planning

In order to minimise any disruption to the services managed by Royal Mail Group Account, contingency plans encompass:

- Handling emergency situations,
- Operating in fall-back mode, and
- Recovery (or Business Resumption) to full operational status.

28.2 Testing Contingency Plans

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

28.3 Subcontractor's Contingency Plans

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

29.0 Compliance

Royal Mail Group Account is required to comply with legislative requirements and commercial standards.

29.1 Compliance with RMGA Security Policy

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

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

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

These may be carried out by the Security Manager, the programme Assurance Manager or External companies who have a statutory right of access to information.

29.2 Independent Information Security Reviews

All areas of information security should be subject to regular reviews to ensure compliance with security policy control objectives, controls, policies, processes and procedures for information security. They should be independently reviewed annually or when significant changes to the security implementation occur.

POL00397070

29.3 Compliance with Legislative Requirements

Royal Mail Group Account must ensure compliance with all legislative requirements, including the:

- Computer Misuse Act (1990)
- Data Protection Act (1998),
- 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 must comply with data protection legislation and principles. Royal Mail Group 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 must 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 must be displayed to potential users prior to system log-on.

Royal Mail Group Account must protect against unauthorised copying of documentation and software.

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

29.4 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 Royal Mail Group Account Security Manager.

POL00397070

29.5 Compliance with BS ISO/IEC Standards

These controls are designed to provide a sound baseline for commercial organisations of many types and for security purposes are as follows:

- BS ISO/IEC 17799: 2005
- BS ISO/IEC 27001: 2006

Royal Mail Group Account must apply these controls to provide a baseline definition for information security encompassing the ten categories of controls. Royal Mail Group Account's Security Procedures, and work instructions must be based upon this document and associated documents and all PO contractual requirements and standards.