POL00401642

Document Title: Horizon Security Policy

Document Type: Policy

Release: BI3 S80 onward

Abstract: This security policy is applicable to the Horizon solution and specifies mandatory security requirements to be applied throughout Post Office Account

Document Status: APPROVED

Originator & Dept: Brian Pinder, POA Security Manager

Internal Distribution: As required via PVCS and BMS

External Distribution: Sue Lowther, Post Office Ltd

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

Name	Role	Signature	Date
Dave Baldwin	Business Unit Director		
Colin Lenton-Smith	Director, Commercial		
Peter Jeram	Director, System Integration		
Dave Baldwin	Director, Customer Service		
Gill Jackson	Programme Manager, Horizon		
Sue Lowther	Post Office Ltd		

POL00401642

0.0 Document Control

0.1 Document History

Version No.	Date	Reason for Issue	Associated CP/PEAK/PPRR Reference
0.1	27/5/96	Initial draft issued for comments	
0.2	31/5/96	Revised draft issued for comments	
0.3	26/6/96	Incorporates comments from the Pathway Management team	
1.0	16/8/96	Incorporates comments from DSS/BA and POL	
2.0	23/9/96	Incorporates further comments from Authority	
3.0	8/10/96	Approved	
3.1	24/11/97	Revised for internal review purposes	
3.2	10/01/98	Incorporates comments from internal review	
3.3	23/2/98	Incorporates further comments	
3.4	28/9/98	Minor updates	
4.0	30/4/99	Approved	
4.1	24/6/99	Removal of references to DSS/Benefits Agency relating to Contract changes.	
4.2	03/10/00	Incorporates changes following internal review and re-organisation of responsibilities.	
5.0	13/11/00	Approved Internally	
5.1	20/11/00	Incorporates clarification in respect of DPA and OBCS.	
6.0	20/11/00	Approved Internally	
6.1	08/08/01	Incorporation of changes in organisation. For review and circulation as a baseline to inform NWB contractual negotiations.	
6.2	30/04/02	Change from ICL branding to Fujitsu Services	
7.0	28/05/02	Approved	
7.1	12/07/02	Incorporation of the Network Banking Service. Minor typographical and contextual changes.	
7.2	15/08/02	Incorporation of comments from review.	
8.0	03/09/02	Approved	
8.1	Jan 2003	Updates in line with BS ISO/IEC 17799 and inclusion of the Debit Card System	
9.0	24/01/03	Approved	

POL00401642

9.1	30/4/04	To reflect change to Post Office Account and incorporate planned new products and services introduced by S50, S52, S52R, S60, S70 and S75. Introduction of Vulnerability Management and Technical Compliance Testing.	
9.2	30/9/04	Additions to legal compliance to cover Financial Services Authority requirements and Money Laundering Regulations.	
10.0	11/11/04	Approved	
10.1	23/12/05	Inclusion of Section 10.2 Compliance with Post Office Security Compliance Requirements	
11.0	24/02/06	Issued for approval.	

0.2 Review Details

Review Comments by :	
Review Comments to :	Originator & Document Management

Mandatory Review	
Director of Customer Service	Dave Baldwin
Director of Programmes	Peter Jeram
Horizon Programme Manager	Gill Jackson
Quality & Risk	Jan Holmes
CS Service Implementation Manager	Graham Welsh
CS Security	Bill Membery Peter Sewell
Post Office Ltd	Sue Lowther Alan Simpson

Optional Review

POL00401642

Customer Services	Peter Burden
	Carl Marx
RASD	Nial Finnegan
	Dave Tanner
	Glen Stevens
Core Services	Andrew Gibson
	Dave Jackson
	Barry Fleming

(*) = Reviewers that returned comments

0.3 Associated Documents

Reference	Version	Date	Title	Source
PA/TEM/001	---	---	Fujitsu Services Document Template	PVCS
BS ISO/IEC 17799-1: 2000	---	---	BS ISO/IEC 17799-1: 2000, Information Technology – Code of Practise for Information Security Management	External
BS 7799-2: 2002	---	---	BS 17799-2: 2000, Information Security Management Systems - Specification	External
ISO11568	---	---	Banking Key Management	External
PSO/000/GEN/SCO/105	---	---	Community Information Security Policy for Horizon	External
ISO9564	---	---	Banking PIN Management and Security	External
ISO13491	---	---	Banking Secure Cryptographic Devices	External
ANSI X9.24	---	---	Retail Financial Services Symmetric Key Management	External
ISO 9001:2000	---	---	Quality Management	External
---	---	---	LINK Information Security Standards	External

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

POL00401642

Abbreviation	Definition
ACP	Access Control Policy
BCP	Business Continuity Planning
CCD	Contract Controlled Document
CD	Compact Disk
DVD	Digital Video Disk
GUI	Graphic User Interface
ID	Identification
IS	Information Security
IT	Information Technology
ISO	International Standards Organisation
ITIL	Information Technology Infrastructure Library
PBX	Private Branch Exchange
PC	Personal Computer
PIN(S)	Personal Identification Number(s)
POA	Post Office Account
PSTN	Public Switched Telephone Network
RADIUS	Remote Authentication Dial-in User Services
TACACS	Terminal Access Controller Access Systems, TACACS
TCP/IP	Transmission Control Protocol / Internet Protocol

0.5 Changes in this Version

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

POL00401642

	the document.
10.1	Inclusion of Section 10.2 Compliance with Post Office Security Compliance Requirements

0.6 Changes Expected

Changes
Reviewers Comments, plus, confirmation of the approval authorities and expansion of the mandatory / optional reviewers to ensure programme coverage.

POL00401642

0.7 Table of Contents

POL00401642

POL00401642

POL00401642

POL00401642

POL00401642

POL00401642

1 INFORMATION SECURITY PRINCIPLES

The Post Office Account is dependent on computer systems for the majority of it's business activities. A high level of computer security must be maintained to ensure business continuity and minimise damage by preventing and reducing likelihood of security breaches. Information Security provides an enabling mechanism for information sharing and ensures the protection of information and computer assets.

Information assets are valuable and must be protected to ensure that their value is retained. Where information is held in computer systems, the information technology must also be protected for the security and integrity of the information to be maintained. An asset of the group includes buildings, computer hardware and software, communications equipment, personnel, data and documentation.

The essential element involved in securing any technology-based system is to address how confidentiality, integrity and availability are to be assured against the known threats.

- **Confidentiality** is ensuring that the information held by Post Office Account is accessible only to those who are authorised to have access.
- **Integrity** is safeguarding the accuracy and completeness of information and processing methods.
- **Availability** is ensuring that information and services are available when required.

1.1 SECURITY PHILOSOPHY

The essential overarching security requirements in this document are based on a number of basic security concepts that form the fundamental philosophy. These concepts, which are detailed below, are good guiding principles that are further developed throughout this document.

- **The Need-to-know Principle**. The need-to-know principle is widely used in many areas of commercial and government work. The principle states that information (in this case information relating to the networks) should only be made available to those individuals who have a legitimate need for it.
- **The Least Privilege Principle**. The principle of least privilege means that any user or system should only have the privileges that they require in order to perform their assigned tasks. For example, an ordinary user would not usually be given the privileges necessary to reconfigure network devices.
- **The Weakest Link Principle**. Security can be considered to be a chain that is only as strong as its weakest link. An advanced network security solution is completely invalidated if there is a weak point such as an alternative, unsecured means of access. The weakest link principle is that security resources are firstly directed at the weakest links in the security of a network.
- **The Fail-Safe Stance Principle**. The principle of fail-safe stance is that in the event that a system or network component should fail, then it should fail in such a way that access to data or network resources is denied, not allowed. For example, in the event of the failure of a firewall, the device should block all traffic, not pass it.
- **The Universal Participation Principle**. The principle of Universal Participation is that all the users, administrators and other personnel involved in the use of a network are involved in the security operation, each placing a high priority upon it and co-operating with one another to secure the network.

POL00401642

- **The Defence in Depth Principle**. The principle of defence in depth is that there should be several layers of security which together comprise the overall security solution for a network and no single technology or approach is enough. For example it is not acceptable to simply secure the perimeter of a network with firewalls: the systems inside the network must be hardened to prevent attack from inside the firewall, and intrusion detection systems should monitor the network internally.
- **Security at the Design Phase Principle**. Security should be incorporated at the design stage so that the entire design process is conducted with security in mind. Good secure design approaches such as the use of choke points and strategically placed firewalls are then incorporated from the beginning.

To achieve the above principles Post Office Account and its employees must adhere to the following codes of practice:

- Information security is the responsibility of the Post Office Account and cannot be delegated to any third party.
- Techniques and procedures will be maintained to measure the effectiveness of information security.
- The value of each major information asset will be determined by risk analysis.
- Each asset will be assigned a classification according to an agreed scheme.
- Protection given to each asset will be appropriate to its value and the threats it faces.
- Each asset will have an owner who will be responsible for its protection.
- Only authorised and licensed software will be used on Post Office Account systems.
- All users of Post Office Account information assets will receive appropriate training to ensure they are able to fulfil their individual responsibilities towards information security.
- Users of Post Office Account information assets must be aware of their value and safeguard them accordingly.
- Information security concerns and breaches must be reported in accordance with escalation procedures.
- Managers have prime responsibility for security in areas they manage.
- Users of Post Office Account information and systems will be responsible for the security of information and systems accessed by them.
- Failure to comply with the Information Security Policy will result in disciplinary proceedings.
- We will comply with all relevant regulatory, legal and licence obligations

POL00401642

2 SECURITY POLICY

2.1 INFORMATION SECURITY POLICY

This document seeks to address threats and weaknesses within Post Office Account by providing policy, standards and guidance that addresses the security risk to the electronic, physical and personnel security environments. Moreover, it will detail the security methodology that is to applied, outline respective security responsibilities and provide detail as to how security incidents should be handled.

It will also reflect any wider security requirements that have relevance and any agreed National or International security standards.

This security policy is compliant with, as far as practical, to BS7799/ISO 17799, The Code Of Practice for Information Security Management and adopts a similar security methodology as contained within the Security Management document which forms part of the Information Technology Infrastructure Library (ITIL).

This approach provides a recognised security standard in order that they can have a high degree of confidence in the Company's ability to operate the network securely and protect their information/processes from any form of unauthorised access or manipulation.

2.2 INFORMATION SECURITY POLICY STRUCTURE

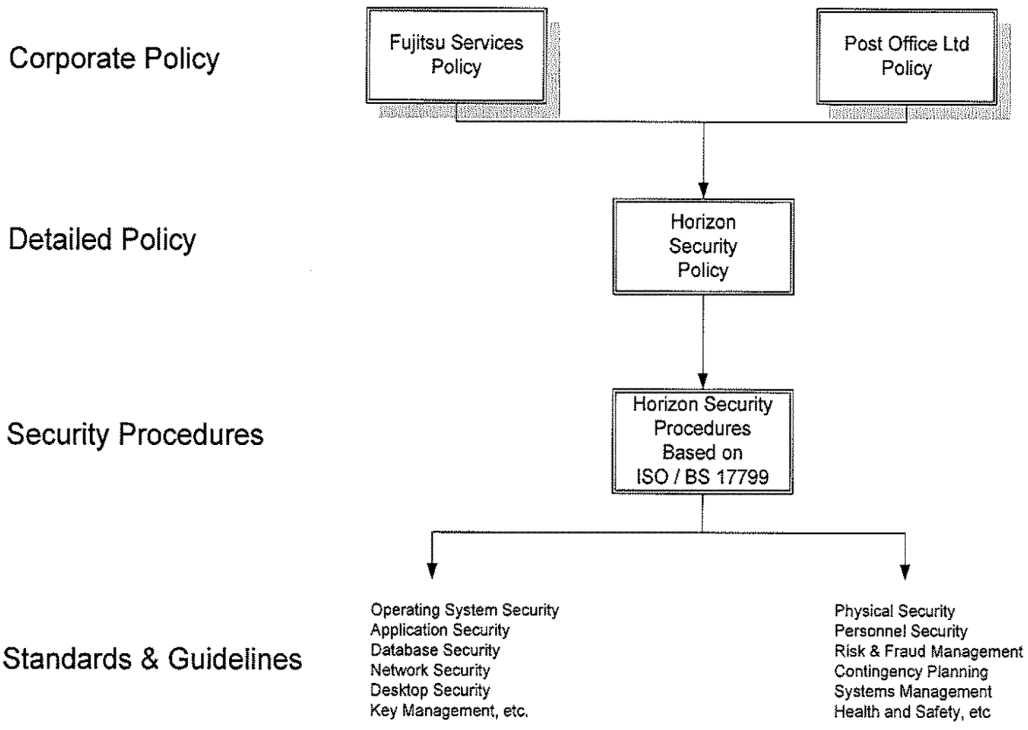

Figure 1 Post Office Account's Security Policy Structure

POL00401642

3 ORGANISATION

3.1 POLICY

Executive, management, specialist and staff responsibilities and accountabilities for information security will be defined and communicated. This management framework will initiate, maintain and control information security throughout the group.

3.1.1 General Principle

To ensure the effective and timely implementation of information security throughout the Post Office Account, responsibilities need to be defined clearly for all levels of management, information users and systems developers or operators. In this way, all staff and contractors, business partners and suppliers can properly execute their information security duties, and appropriate training and facilities can be provided to all concerned.

3.2 INFORMATION SECURITY ORGANISATION

3.2.1 Overview

There are a number of business responsibilities for information security. It is essential that responsibilities are defined within the Business Unit to ensure information security is being addressed locally within all divisions. The roles identified will mainly be incorporated into existing duties; however it may be necessary for some divisions to appoint a security administrator where the nature of the task justifies this.

3.3 SECURITY MANAGEMENT STRUCTURE

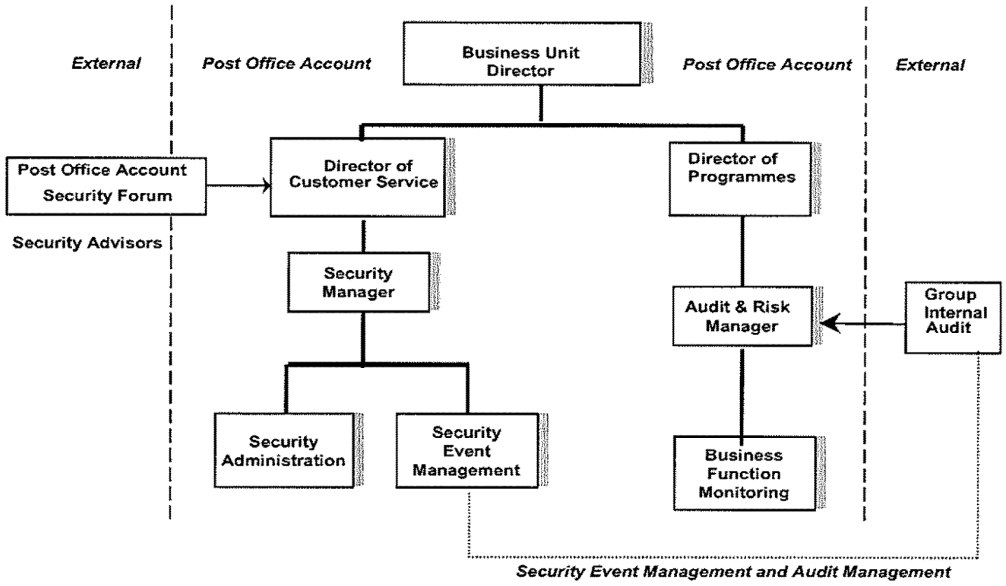

Figure 2 Post Office Account's Security Management Structure

POL00401642

3.4 INFORMATION SECURITY FORUM

Information security is a business responsibility shared by all members of the management team. An Information Security Forum to ensure that there is clear direction and visible management support for security initiatives should be formed. That forum should promote security within the organization through appropriate commitment and adequate resource. The forum may be part of an existing management body. Typically, such a forum undertakes the following:

- Reviewing and approving information security policy and overall responsibilities;
- Monitoring significant changes in the exposure of information assets to major threats;
- Reviewing and monitoring information security incidents;
- Approving major initiatives to enhance information security.
- Agrees specific roles and responsibilities for information security across the organization;
- Agrees specific methodologies and processes for information security, e.g. Risk assessment, security classification system;
- Agrees and supports organisation-wide information security initiatives, e.g. Security awareness programme;
- Ensures that security is part of the information planning process;
- Assesses the adequacy and co-ordinates the implementation of specific information security controls for new systems or services;
- Reviews information security incidents;
- Promotes the visibility of business support for information security throughout the organization.

The Post Office Account Security Manager will assume responsibility for all security related activities.

3.5 BUSINESS RESPONSIBILITIES FOR INFORMATION SECURITY

3.5.1 The Business Unit Director

The Business Unit Director is ultimately accountable to the Board for the security of the Post Office Account and its operations.

3.5.2 The Post Office Account Directors

The Post Office Account Directors are accountable for the security of information, systems and networks in operation in their parts of the business unit. This accountability should be delegated through line management, with a number of identified roles accepting responsibility and accountability for differing aspects of information security.

Overall responsibility for security throughout Post Office Account rests with the Director, Customer Services. The security related responsibilities of the Director, Customer Services, include:

- Overall control and management of security throughout Post Office Account,
- Provision of adequate resources for security,

POL00401642

- Chairman of the Post Office Account Security Forum,
- Owner of Post Office Account's Security Policy,
- Approval authority for Post Office Account's Security Policy,
- Approval authority for Post Office Account's Security Procedures,
- Establishing the security interface with Post Office Ltd, and
- Establishing the security interface with all subcontractors.

3.5.3 Security Manager

The Security Manager is responsible for ensuring implementation of policy and procedures, and maintaining "best practice", within the remit of Post Office Account. Post Office Account's Security Manager's responsibilities include:

- Physical and environmental security,
- Monitoring for compliance with post office account's security policy,
- Providing the point of contact for reporting all types of security incidents,
- Ensuring that security incidents are recorded and investigated,
- Ensuring that security relevant events are recorded,
- Ensuring that system audit trails are analysed on a regular basis,
- Documentation of post office account's security policy,
- Owner of post office account's security procedures,
- Documentation of post office account's security procedures,
- Communication of security policy and procedures throughout post office account,
- Authorisation and approval for system changes,
- Co-ordinating the evaluation of all new security products proposed,
- Specifying and arranging security education and training,
- Devising and conducting security awareness programmes,
- Maintaining a partnership approach to security with post office ltd security staff,
- Liaison with the post office ltd information security manager, external regulators and suppliers' security personnel,
- Reporting to the post office limited information security manager any actual or potential threats or breaches that may have a material effect on any service, and
- Recruitment selection of security administration personnel.

POL00401642

3.5.4 Responsibilities for Physical Security

The local Site Managers have responsibility for physical security at all sites used by Post Office Account.

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

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

3.5.5 Audit Manager's Responsibilities

Overall control of risk management functions is the responsibility of the Director of Programmes. The Post Office Account's Audit Manager is responsible for ensuring implementation of Post Office Account's Audit Policy and maintaining "best practice", within the remit of Post Office Account. The Audit Manager's responsibilities include:

- Planning and carrying out audits of Post Office Account's business functions,
- Examining and evaluating the results of (business function) audits,
- Developing and agreeing improvement programmes,
- Monitoring and reporting improvement activities,
- Monitoring for compliance with Post Office Account's Audit Policy,
- Providing the point of contact for all audit related matters,
- Overall responsibility for Minor amendment to Diagram in paragraph 4 to reflect revised Post Office Organisation Post Office Account's Audit activities,
- Documentation of Post Office Account's Audit Policy,
- Being the owner of Post Office Account's Audit Standards,
- Documentation of Post Office Account's Audit Standards,
- Communication of Audit policy and standards within Post Office Account,
- Co-ordinating the evaluation of all new audit products proposed,
- Specifying and arranging Audit education and training,
- Liaison with Post Office Ltd. Audit personnel,
- Liaison with Fujitsu Services Group Audit personnel, and
- Recruitment selection of Audit personnel.

3.5.6 Information Security Representatives

For each major part of the Post Office Account, a senior manager should be appointed as an Information Security Representative to oversee information security activity within their business division.

The representative should be influential within their division and knowledgeable about their business. The appointment will enable a two-way communication channel for the delivery of information

POL00401642

security between their business division and the specialist security, audit and IS staff. This will help in the creation of an information security conscious culture within their business area, and ensure Policies and Codes of Practice are developed in accordance with individual business needs.

Depending on the size, nature and risks involved this role may be incorporated into existing duties or a full-time information security specialist may be appointed. It is not intended that Representatives will be involved in day-to-day information security activity.

3.5.7 Line Managers

Working closely with their Security Representative, each Line Manager will deal with information security management at a local level. They will be responsible for ensuring that their staffs are aware of and competent to discharge their personal responsibilities towards information security. The managers will also be responsible for reporting any security breaches through the incident management process, to ensure necessary actions are enforced. These responsibilities will be incorporated within normal day-to-day business.

3.5.8 Information Users

All users of Post Office Account information (in all its forms), should be aware of, and comply with, any relevant information security controls or procedures. All information should be treated with due care, in a sensible and responsible manner. Any information security concerns or suggestions should be reported to their Line Manager.

3.6 SPECIALIST RESPONSIBILITIES FOR INFORMATION SECURITY

Within Post Office Account specialist security advice is provided by the POA Security Manager who has a dedicate staff in order to manage information security.

For maximum effectiveness and impact they should be allowed direct access to management throughout the organization. The information security adviser or equivalent point of contact should be consulted at the earliest possible stage following a suspected security incident or breach to provide a source of expert guidance or investigative resources. Although most internal security investigations will normally be carried out under management control, the information security adviser may be called on to give advice; lead or conduct the investigation.

3.7 CO-OPERATION BETWEEN ORGANISATIONS

Appropriate contacts with law enforcement authorities, regulatory bodies, information service providers and telecommunications operators should 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 of the organisation is not passed to unauthorized persons.

4 CLASSIFICATION OF INFORMATION

4.1 POLICY

All information and systems will receive a classification and where practical "owners" will be identified so that responsibility for information and system security can be properly assigned.

POL00401642

Accountability for implementing security measures will rest with the identified owner or responsible manager, the security classification scheme allowing security to be directed where it is needed most.

4.1.1 General Principle

Information security must be applied with due regard to the balance between the risk being reduced and the cost of implementing controls. A security classification process will enable the Post Office Account to differentiate between 'sensitive' information, and information regarded as less valuable. Security can be directed where it is most needed and not wasted where it is not justified.

The classification must take account of business needs for sharing or redirecting the information, and the impact associated with unauthorised access, damaged (incomplete or inaccurate) or non availability to the information.

4.2 INVENTORY OF ASSETS

4.2.2 Types of Assets

Information can be held in various forms, an asset inventory must be maintained for each. All information will be classified in general by subject, although it is anticipated that some subjects will have specific areas which may need a higher classification, these will be identified as special files. Assets have been grouped by type to enable a clear understanding of where boundaries lie. The necessary requirements for the inventory are also described below.

4.2.3 Information Assets

Information which is held on paper, in databases or data files, system documentation, user manuals, training material, operational or support procedures, continuity plans and fallback arrangements, backup files can all be categorised by subject. E.g. all staff, information held in any of the above forms will be classed as Personal. The inventory will hold the following information:-

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

4.2.4 Software Assets

All information systems which are built from application software, system software, development tools and utilities will be identified and classified by the IT facility name. E.g. all application software, system software, licenses, development tools and utilities which are used to provide the HORIZON system will be classed as HORIZON assets. The inventory should hold the following information:-

- The IT facility asset name and high level description
- The IT facility asset classification.
- The classification of special files in the IT facility.

POL00401642

- The IT facility owner.
- The IT facility custodian

4.2.5 Physical Assets

Physical assets which are critical to the continuity of business include computer and communications equipment, magnetic media (tapes and disks), specialist technical equipment (power supplies, air-conditioning units), furniture and accommodation. E.g. the critical physical components which enable business operation. The inventory should hold the following information:-

- The physical asset name and high level description.
- Date of physical asset purchase.
- The serial number of the physical asset and its components.
- The location of the physical asset.
- The division accountable for the asset.

4.2.6 Service Assets

All major services which the Post Office Account utilise include computing and communications services, heating, lighting, power, air conditioning, postal, distribution should be classified. E.g. the heating service within all corporate sites.

- The service asset name and high level description.
- The service providers contact name.
- The service contract commencement and expiry date.
- The person accountable for the asset.

4.3 INFORMATION OWNERSHIP

4.3.1 Ownership and Custodianship

All major information assets identified will where appropriate, have an assigned named owner who will be responsible for ensuring the integrity, availability and confidentiality of the asset.

Owners must have sufficient authority and knowledge to allow them to appreciate the value of their system and or information. They will 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.

4.4 SECURITY CLASSIFICATION

4.4.1 Classification Overview

Classification is the means used by Post Office Account of establishing and recording the value of its assets to ensure the correct level of protection is afforded. A group classification for each information

POL00401642

subject, IT facility, equipment or service asset will be given. Within each there may be elements which need to be classified at a higher level. These elements will be identified as special files.

It is essential that any classification scheme is simple to understand and easy to apply. It should match, as much as possible; the schemes of trading partners and suppliers, and it should describe the security controls associated with each level. It is also essential that information and systems are valued correctly. Over classification will lead to waste of effort. Under classification will reduce the protection afforded.

4.5 ASSESSMENT OF ASSETS

The criteria to be considered when assessing the value of the assets being classified include:

- **Strategic Value** - The degree to which the asset affects or reflects the Group's current or future strategy. The extent to which the disclosure of information, to the media or other parties, would disadvantage the Group.
- **Business Value** - The actual or potential value that the asset could have to other organisations. The effect on the Group's business if the information were lost or inaccurate.
- **Legal Liability** - Where disclosure or inaccuracy may result in legal action. In particular personal data, which is normally subject to data protection or data privacy laws, must not be classified lower than ***RESTRICTED***.
- **Embarrassment** - The extent to which the information, if disclosed, would undermine confidence in the Group.
- **Cost of Creation/Reconstruction** - Information that requires considerable effort to be created or reconstructed.

4.6 CLASSIFICATION SCHEME

Information should be valued ("classified") according to three main security attributes:

- **Confidentiality**: this rating measures the level of damage to the organisation that would result from unauthorised disclosure of information.
- **Integrity**: this rating measures the level of damage to the organisation that would result from loss, corruption or fraudulent modification of the asset.
- **Availability**: this rating measures the time criticality of the recovery mechanisms that must be applied if the asset was not available.

4.7 CLASSIFYING INFORMATION

4.7.1 Labelling of Assets

All assets which have been classified will be labelled with the classification. Any special files identified should also be labelled with an inventory reference.

4.8 SUMMARY OF FUJITSU CLASSIFICATIONS AND PRIVACY MARKINGS

Three classifications and two privacy markings for documents have been defined by Fujitsu and must be used where appropriate. Full details of the Fujitsu classification system are available at http://www.cafevik.fs.fujitsu.com/viewer.asp?/Content/0105/public/00002/HTML/stf_PolicyMap.htm

POL00401642

The system is tiered in order to ensure that information is appropriately protected in an ascending level of required protection, these levels are:

- Privacy Markings:

  Personal Addressee Only

  Staff Restricted

- Classifications:

  Eyes Only

  Commercial in Confidence

  Company Restricted

  Company Secret

Privacy Markings are used where information relates to an individual (although this includes the same document sent to a number of individuals) and where disclosure might be detrimental to that individual's interests.

Classifications are used where the information is not specific to an individual. If there is no risk to the company in disclosure of such material no classifications should be used.

4.8.1 Privacy Markings

PERSONAL ADDRESSEE ONLY - This privacy marking is for matters personal to the addressee. Examples include:

- Written warnings
- Salary and pension details.

STAFF RESTRICTED - This privacy marking applies to matters relating to employees and their services. Examples are:

- Bonus scheme details
- Disciplinary warnings not attributable to an individual

4.8.2 Classifications

EYES ONLY - This classification applies to information and material where unauthorised disclosure might cause minor embarrassment or be detrimental to the interests of the Company. This might include:

- Company Announcements
- Telephone Directories

Note: * EYES ONLY may be used with additional qualifications. These can be business specific, however, at company level; the following should be used and recognised:

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

POL00401642

- **FUJITSU SERVICES EYES ONLY** - Should be available only to employees of Fujitsu Services and trusted contractors.
- *country* **EYES ONLY** (e.g. NETHERLANDS EYES ONLY or UK EYES ONLY) - Should only be available to staff of Fujitsu Services and trusted contractors within the named *country*.

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.

COMPANY RESTRICTED - This applies to 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. This information would include.

- Sensitive customer information
- Negotiating positions
- Market assessments or competitive information
- Technical information that could impact the security of IT systems

COMPANY SECRET - This 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.

- High-level business and competition strategy and plans
- Very sensitive competitor, partner or contractor assessments
- Patent secrecy information
- Information, e.g. passwords, vital to the security of IT systems

4.9 SUMMARY OF POST OFFICE CLASSIFICATIONS AND PRIVACY MARKINGS

Strict care is to be taken when handling Post Office documents to ensure that they are handled correctly and afforded the proper levels of protection within Post Office Account.

4.9.1 Information Classification Labels

Post Office uses a system of classification labels and descriptors when classifying documentation. These classification labels and descriptors are:

- INTERNAL - Information accessible to all employees, agents and contractors relating to the ongoing business of Post Office.
- CONFIDENTIAL* - Information that has been assessed to be of a sensitive nature and likely to cause damage following unauthorised disclosure.
- STRICTLY CONFIDENTIAL* - Information that must meet the classification standards of government departments, the security services or clients, or has been assessed to be so sensitive that unauthorised disclosure would cause acute organisational damage.

POL00401642

4.9.2 Classification Descriptors

Descriptors can be used for the purpose of differentiation and categorisation. These descriptors are self explanatory, some examples of descriptors used by Post Office are:

- COMMERCIAL*
- FINANCIAL*
- LEGAL*
- MARKETING
- PERSONAL
- PERSONNEL

The format for applying classification labels and descriptors is label followed by descriptor as follows:

- Example: POST OFFICE CONFIDENTIAL - COMMERCIAL

4.9.3 Levels of Protection

When responding to a document received from Post Office it is essential to ensure the correct classification of the response and the levels of required protection. If this is unclear, enquiries should be made with the document owner to confirm the classification of the response level of protection and levels of protection required.

Post Office classifications and descriptors marked '*' are most likely to be seen by Fujitsu in the course of normal business, however, the possibility of receiving documents containing other markings should not be discounted

POL00401642

5 PERSONNEL SECURITY

5.1 POLICY

Security awareness will be addressed at the recruitment stage, and where appropriate referred to in job descriptions and contracts, and monitored during an individual's employment with the Post Office Account Users will be trained in security procedures and the correct use of information and systems.

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

5.1.1 General Principle

All Post Office Account permanent employees, suppliers, contractors, consultants, temporary staff and business partners have an important part to play in securing Post Office Account information (in all its forms), IT systems and networks. All such employees must be adequately equipped, trained and supervised, to contribute as required.

5.2 JOB DESCRIPTIONS

5.2.1 Permanent Staff

Where deemed appropriate, job descriptions or contracts of employment should contain a statement outlining the individual's responsibility for information security.

5.2.2 Temporary / Consultants / Contractors and Suppliers

All individuals contracted to work within the Post Office Account need to be aware of their responsibilities for information security. Each contract should include a statement stating these responsibilities.

5.3 Sensitive or Key Positions

A sensitive position is one in which the jobholder has regular and legitimate access to highly sensitive information. A key position is one where the job holder performs vital duties. Additional security measures need to be taken for such appointments.

Business and IT Managers should identify such sensitive or key positions in their areas. Additional security measures for these positions may include:

- Job Holders should be interviewed about the security requirements of the job
- Extra care in cross checking references
- Avoidance of use of temporary staff
- Specific consideration of segregation of duties / dual control
- Cross training
- Audit Trail monitoring
- Additional supervision by line management

POL00401642

5.4 RECRUITMENT SCREENING

5.4.1 General Screening

As part of the recruitment process, checks should be made on at least two previous employers or character references. All relevant educational qualifications should be confirmed.

Satisfactory replies should be received before employment commences. In instances where employment commences prior to satisfactory references being received conditional letters of employment should be issued.

Interviews should include questions to elicit the candidate's attitude towards information security and to assess his / her trustworthiness.

5.4.2 Additional Screening

Additional background screening such as criminal records checks and credit reference checks are to be carried out in order to meet contractual Post Office requirements for security clearances. Additional security checks carried out by the Post Office will be required before anyone employed with or on behalf of Post Office Account will be allowed access to the restricted areas of a Post Office. All security checks will be carried out with the full knowledge of the applicant.

5.5 CONFIDENTIALITY AGREEMENTS

5.5.1 Employment Contracts

All employment contracts (permanent and temporary) as well as consultant, contractor and supplier contracts should include clauses governing the treatment of Post Office Account information gained as a result of their employment, this may be achieved through signing a non-disclosure agreement or personal integrity form. In particular staff should be informed that the use or removal of customer data by ex-Post Office Account staff, gained during their employment, may result in prosecution by the Post Office Account or the Data Protection Commissioner.

Contracts should 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.

Access to the Information Security Policy and Standards should be given to all new employees, contractors and consultants.

5.6 TERMINATION PROCEDURES

5.6.1 Minimum Procedures

Procedures need to be established to re-define security responsibilities when staffs, including contractors and consultants, are moved within the Post Office Account or whenever their employment ceases for any reason.

Where staff in sensitive or key positions are dismissed, resign, made redundant or reach the end of their contract, consideration should be given to denying them access to areas, systems or any special privileges, or in extreme cases to escorting them immediately from Post Office Account premises. Each case must be considered carefully and dealt with tact and discretion.

Where staffs move within the Post Office Account, computer access should be modified or terminated as appropriate.

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

POL00401642

5.6.2 Return of Property

Line managers should establish formal procedures to ensure the:

- Return of all Post Office Account property on termination of employment;
- Removal of all access permissions (physical and logical).

The use of a checklist pro-forma should be considered to ensure consistency. The checklist should detail all Post Office Account Property, example are as follows:

- Lap Top Computers and Peripheral equipment
- Mobile phones and pagers
- ID Cards
- Access Permissions
- Mainframe sign-on
- LAN Access
- Dial In / Remote access capabilities

5.6.3 Access Removal

Line managers should ensure that individual access 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, should be changed on the departure of a member of the team.

5.7 INFORMATION SECURITY EDUCATION AND TRAINING

5.7.1 Induction

The induction process should ensure that all new employees are made aware of their information security responsibilities, the restrictions on computer access, and possible disciplinary procedures for failing to comply with the Post Office Account Information Security Policy.

5.7.2 Awareness Campaign

An on-going security awareness campaign should ensure that all employees are aware of basic security issues, and who to contact for advice and guidance on security matters. The campaign will also communicate and reinforce specific messages using the various media available within the Post Office Account

In addition, the use of training courses and workshops will be developed to ensure that the profile of information security is raised throughout the Group.

5.7.3 Security Related Positions

Staff in security related positions will be given appropriate technical and security management training for the performance of their roles. The training should commence upon appointment, with refresher courses and workshops provided at regular intervals.

POL00401642

A mechanism for communicating specific topics, issues and concerns should ensure that all security staffs are made aware of current developments and problems.

5.7.4 Sensitive or Key Positions

Staff in sensitive or key positions should be given additional security advice and training.

5.8 REPORTING OF SECURITY INCIDENTS, WEAKNESSES AND SOFTWARE MALFUNCTIONS

5.8.1 Reporting of Incidents

Employees, contractors or consultants who suspect or have knowledge of a possible security breach or violation of the Information Security Policy and Standards or related Codes of Practice must report the incident immediately to their Line Manager or Business Security Co-ordinator.

5.8.2 Incident Management

Each incident, and subsequent actions, should be recorded, assessed and escalated as appropriate by line managers. Details to be recorded include:

- The name of the individual involved in the event
- Date and time of the event
- Details of the event

Line managers should review these records on a regular basis and any unusual events, or trends in events, should be reported to the POA Security Manager. The Security Manager will maintain a database of all reported security incidents.

5.9 DISCIPLINARY PROCEDURES

5.9.1 Breaches of the Information Security Policy

Deliberate and accidental breaches of information security may be regarded as disciplinary offences, for which disciplinary action may be taken.

The severity of a particular violation will be assessed by the Personnel Department and the relevant line manager in consultation with Information Security Compliance. Where disciplinary actions are required, these will be both appropriate and equitable and in accordance with Fujitsu Services policy.

5.10 DISCIPLINARY PROCEEDINGS

5.10.1 Employees

Deliberate or repeated failure to comply with agreed policy and standards will result in disciplinary procedures being taken against the individual(s) in accordance with agreed Post Office Account standards. This may ultimately result in dismissal.

5.10.2 Third Parties

Third parties are governed by contractual agreements, deliberate or repeated failures to comply with agreed policy and standards will result in a review of the contract, and its possible termination or imposition of penalty clauses.

POL00401642

5.10.3 Information Security Compliance

Before disciplinary proceedings for any security related incident are begun, the Security Manager must be advised.

6 PHYSICAL AND ENVIRONMENTAL SECURITY

6.1 POLICY

Information and Systems which support critical Post Office Account business activities will be physically protected from environmental hazards, unauthorised access, and deliberate damage or interference. Measures will be commensurate with the classification of the information or system to be protected.

6.1.1 General Principle

There are minimum Codes of Practice for the physical security of Post Office Account computer installations and telecommunications networks. There are three categories of sites to which these practices apply:

- Data centres, such as SDC01 and SDC02, etc,
- Sites housing support functions or small multi-user systems, such as, HSH, SMC/SMG, BRA01, including SSC and IRE11, including Belfast Operations,
- Areas within Fujitsu Services premises with PCs, standalone or networked, or terminals connected to host systems.

When considering new construction or major alterations, physical security requirements must be evaluated against the importance of the installation, the data held and processed, and the threats to which the site is exposed.

6.2 PHYSICAL SECURITY PERIMETERS

6.2.1 Implementation of Physical Security Measures

The actual measures to be applied will vary with the nature and amount of information, IT systems and telecommunications facilities at the site.

6.3 DATA CENTRE LOCATION AND CONSTRUCTION

The location and design of data centres and computer rooms will take into account the possibility of damage from fire, flood, and explosions, civil unrest and other forms of natural or man made disasters. Consideration must also be given to any security threats posed by neighbouring accommodation.

The following security features must be considered and where appropriate included in the design and construction:

- A security fence around a free-standing data centre;
- Walls, ceilings and floors constructed to retard combustion;
- Doors to resist forced entry and retard combustion;

POL00401642

- Power and communications cables duplicated and physically separated from each other and from other utility services;
- Lightning conductors.

Contingency, alternate and backup sites must be located and equipped so that they will not be affected by the same incident that disrupts business at the prime site. Issues to be considered include power supplies, communications routing, physical distance between the locations etc.

6.4 SIGNAGE

Buildings housing IT equipment and facilities (data centres, areas housing IT hardware which support secret, essential and time critical applications) should be unobtrusive and give no indication of their purpose. Internal directories and telephone books must not indicate the location of facilities.

6.5 ENTRANCES AND EXITS

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. Unoccupied secure areas must be physically locked and subject to periodic checks.

6.6 INTRUSION DETECTION

Intrusion detection alarm systems must be used for installations which are left unattended. These may be either part of 24-hour security cover or connected to a security company or the Police. Alarm systems must be tested regularly and maintained to manufacturers' requirements.

6.7 SEPARATION OF FACILITIES AND SUPPLIES

Support functions and equipment, such as facsimile machines, photocopiers, etc, must be located away from secure areas to eliminate the need for, or prevent the risk of, unauthorised access.

Hazardous and combustible materials must be stored securely at a safe distance from sites. Computer supplies such as stationery must be retained in store rooms and not transferred to data centres until required.

Back up media must be stored at a safe distance to avoid damage from a disaster at the main site. Back up media must be verified and checked for completeness, then moved away from the prime site as soon as possible.

6.8 INTERNAL SECURITY

There must be an effective fire safety programme which adheres to all local and national fire regulations, which have been approved by the appropriate fire prevention advisor. Measures must minimise the risk of fire from occurring within an installation, or from spreading into the installation from an adjoining area.

Automatic fire detection systems must be installed in all critical computer facilities.

Inert fire suppressant systems must be fitted to computer areas supporting critical business processes, with the ability for automatic operation during periods when the buildings are unmanned. Where flammable material is present in inaccessible places, total flooding systems (inert suppression systems), should be used. Personnel must not be endangered by the operation of an automatic extinguishing system. Full training and documented procedures must be available to all staff working in areas protected by fire suppressant systems.

POL00401642

All fire detection and extinguishing equipment must be serviced and tested in accordance with the manufacturers' specifications or as required by British Standards, whichever is more stringent.

Automatic emergency lighting must be provided in data centres, and at other "sites" as appropriate and necessary.

Physical security measures implemented at a prime computer facility must also be provided at any backup sites.

Internal physical barriers must extend from floor to ceiling to prevent unauthorised entry and environmental contamination.

6.9 ENVIRONMENTAL CONSIDERATIONS

Computers may require clean, filtered air provided within specified temperature and humidity ranges. Whenever possible, there should be a separate heating and air conditioning system for computer mainframes and some types of mini systems.

Extremes of temperature and humidity for computer and telecommunications equipment must be maintained within manufacturers' specifications.

6.10 ELECTRICITY

Computers and telecommunications facilities require a dependable, consistent electrical power supply, free from surges and interference. Back-up power supplies may also be required for larger and/or critical systems.

Equipment supporting critical business applications must be protected by un-interruptible power supplies (UPS), together with a standby power facility capable of supporting the room and equipment for an extended period. UPS equipment must be tested on a regular basis.

Emergency power-off switches must be installed in data centres. Where fitted, they must be readily accessible with conspicuous notices showing their location.

6.11 CABLING

Cabling for computer and telecommunications equipment must be protected against unauthorised physical access. Power and telecommunications lines into data centres should travel underground to the point of entry to the facility and then be enclosed in secure ducting or risers within the building.

Access points to such risers and network, communications and power cable connection points must be secured.

Cabling plans must be developed and maintained for all major services.

Computers and telecommunication facilities should be protected from all forms of water damage.

6.12 LOADING AND DELIVERY AREAS

Loading and delivery areas must be designed to ensure that supplies can be delivered or loaded without compromising secure areas. The use of an interlocking door mechanism should be considered to prevent external doors being opened until internal doors are closed.

Incoming material must be inspected for potential hazards before it is moved to the point of use.

POL00401642

6.13 EMERGENCY PROCEDURES

Emergency procedures must be prepared to allow staff to react properly in the event of an emergency, to protect personnel, and limit damage to premises and equipment.

6.14 PROCEDURES AND DOCUMENTATION

Emergency procedures must exist to protect personnel in hazardous situations. All staff must be trained in the procedures and take part in regular practice drills. Such procedures, including the location of switches, alarms, extinguishers etc., must be documented and stored safely. Copies must be available off-site and immediately available in the event of an emergency.

Notices of evacuation procedures must be posted visibly in all locations. Notices of emergency staff contacts must also be posted visibly, and staff regularly informed of these contacts.

6.15 EQUIPMENT

All emergency equipment must be readily available and maintained properly.

6.16 TRAINING

All personnel with emergency roles must be properly trained and practised in such roles.

6.17 TESTING

Emergency procedures must be tested regularly, and results documented for review by line management.

6.18 SAFETY

Line management must ensure compliance with regulations with security implications, including Health and Safety regulations and Fire regulations. Line management must also ensure that the appropriate Fujitsu Services Health and Safety officers are consulted whenever new types of computer and telecommunications equipment are installed.

POL00401642

7 PHYSICAL ACCESS CONTROLS

7.1 SECURITY ACCESS RIGHTS

Access to all buildings housing Post Office Account facilities must be restricted to those individuals who have been granted specific authorisation.

7.2 SECURITY ACCESS CONTROLS

Access control must be enforced at all entry points to Post Office Account premises, except those open to the public, additional controls applied to areas containing secret, essential or time critical services.

Identity badges must be worn visibly by all persons at all times within Post Office Account premises, except those open to the public.

Access control mechanisms must be appropriate to the nature of the premises, the number of staff using those premises and the classification of the information, networks or applications contained within the site. Such mechanisms can be drawn from the following range:

- Guards
- Automatic access control
- Alarms and/or CCTV linked to a permanently manned guard service
- Card or token access control systems
- Receptionists
- Lock and key
- Restricting the number of entrances/exits for normal use

Access control to data centres and other premises or areas containing IT facilities must be designed to prevent 'tailgating'. Where this is not practical local procedures must emphasise that 'allowing any person to tailgate is not permitted'. Logs must be maintained which provides detail of all access to secure areas, to be retained for a minimum of 1 year for security and audit purposes.

Access rights must be revoked immediately for staffs that leave the Post Office Account

7.3 CONTROL OF VISITORS

Visitors must have a Post Office Account sponsor, who will be responsible for that visitor while they are within a Post Office Account facility.

All visitors to Post Office Account premises, except those open to the public, must be required to register and obtain visitor passes. Such passes must be worn visibly at all times and returned at the end of the visit.

Visitors must be supervised at all times.

A record of all visitors to Post Office Account premises, except those open to the public, will be kept which details:

- Name of visitor
- Name of person to be seen
- Car registration number

POL00401642

- Time of entry
- Time of Departure
- Pass number

Any injury sustained by the visitor while on Post Office Account premises must be reported to line management immediately and a full report submitted by the sponsor. Any damage caused by the visitor to Post Office Account property must be similarly reported.

7.4 ENFORCEMENT OF ACCESS CONTROL

All Post Office Account staff must be made aware of their right and duty to challenge unfamiliar persons, e.g. those individuals not displaying a valid permanent staff or visitors pass, or those behaving in a suspicious manner. However, it is stressed that Post Office Account staff must not place themselves at risk.

If in doubt, or if the response from the challenged individual is unsatisfactory, line management and Site Security must be informed immediately.

7.5 CLEAR-DESK POLICY

Every member of staff must be encouraged to apply a clear-desk policy:

All secret, private and confidential and valuable documents (paper and magnetic) must be locked away in cabinets or desk drawers when the desk is unattended for an extended period - for example when away for meetings, at lunch times or overnight. Computers must be logged off at cease work.

Offices must be kept as uncluttered as possible. Unwanted paperwork must not be retained, but disposed of securely (e.g. shredded).

The use of lockable fire proof cabinets must be considered for the storage of secret and confidential paper documents and magnetic media.

7.6 PROTECTION OF DOCUMENTS

7.6.1 Protection of Magnetic Media

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

7.6.2 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 (cheque forms, magnetic swipe cards etc.) must be handled "as if" they have that value.

7.6.3 Protection of Back-up Media

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

7.7 IT EQUIPMENT

IT equipment, including computers, telecommunications and other electronic equipment, must be sited and positioned safely. Access to such equipment must be minimised.

POL00401642

Centralised computing and associated equipment, information servers, Private Branch Exchange (PBX), telephone switch equipment packet switches, PSTN switches, gateways etc. must be located in secure areas.

The positioning of paper and screen based devices, such as printers, microfiche, PC's etc, should take into account the confidentiality of the information produced and be protected and sited accordingly to reduce the risk of accidental disclosure.

7.7.1 General Rules

Smoking, drinking, and eating are prohibited in all secure computer equipment areas.

With the exception of portable computers and equipment specifically intended for use off-site, documented authorisation from line management is required before equipment, data or software is removed from Post Office Account premises.

Equipment and media must not be left unattended in public places. Portable computers or hard disk drives must be carried as hand luggage.

The use of photographic, recording, and video equipment is prohibited within Post Office Account premises unless prior executive authorisation has been obtained

The use of mobile phones should be restricted within all data centres and at other sites as necessary.

Manufacturers' instructions regarding the protection of equipment, such as, temperature ranges, sunlight, water, etc. must be observed at all times.

7.8 MAINTENANCE OF IT EQUIPMENT

7.8.1 Manufacturers Specification

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

7.8.2 Fault Recording

A record of all faults and suspected faults must be maintained. Repairs and servicing must be carried out only by authorised maintenance personnel. Health and Safety regulations must be observed at all times.

7.9 Disposal of IT Equipment

7.9.1 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.

POL00401642

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

8 COMPUTER AND NETWORK MANAGEMENT

8.1 POLICY

Information, systems and networks will be managed effectively to ensure their integrity, availability and confidentiality, and to prevent their accidental or deliberate misuse. Appropriate operating procedures, controls, change management and monitoring will be implemented.

8.1.1 General Principle

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

8.2 OPERATING PROCEDURES

8.2.1 Documented 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, and where appropriate via a change management system.

POL00401642

8.3 INCIDENT MANAGEMENT

Incident management responsibilities and procedures must be established to ensure a quick, effective and orderly response to security incidents, including:

- System failures and loss of service.
- Errors resulting from incomplete or inaccurate data.
- Breaches of confidentiality.

Such procedures must include the identification of the cause of incidents, and the implementation of remedies to prevent recurrence. Audit trails and similar evidence about an incident must be collected and secured to assist in this, as evidence about breaches of contract or regulations, and for negotiating compensation from suppliers.

All emergency actions must be documented, escalated and reviewed in an orderly manner.

The integrity of information systems and networks must be confirmed as soon as possible after recovery.

8.4 SEGREGATION OF DUTIES

8.4.1 Minimise Risk of System Misuse.

To reduce the opportunities for unauthorised modification of Post Office Account information, data or services, the following functions should not be carried out by the same employee(s):

- Business system use.
- Computer operation.
- Network management.
- System administration.
- Systems development and maintenance.
- Change management.
- Security administration.
- Security audit.

8.5 DEVELOPMENT AND OPERATIONAL FACILITIES.

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

- Development and operational facilities should be segregated;
- Different logon procedures 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.

8.6 EXTERNAL FACILITIES MANAGEMENT.

Care is needed to ensure the security and reliability of Post Office Account information resources when undertaken by external facilities management companies ("out-source"). Such outsourcing arrangements must provide a level of security and safety at least to the same level provided in-house.

POL00401642

The Post Office Account must identify any particularly sensitive or critical applications and establish if these should remain in-house. Sensitive or key positions should remain in-house. Post Office Account data must be segregated and protected from the data of other organisations managed by the outsourcing agent.

Agreements must be in place to ensure the confidentiality of Post Office Account information, and to indemnify the Post Office Account against losses caused by the outsourcing agent. Responsibilities and procedures must be established for the reporting and handling of all security incidents.

All software produced externally must remain the property of the Post Office Account

Recovery from damage or loss of data at the contractor's site must be within agreed time-scales.

8.7 SYSTEM AND NETWORK PLANNING AND ACCEPTANCE

8.7.1 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 and storage remain available, and to identify and avoid potential bottlenecks.

8.8 SYSTEM ACCEPTANCE

Acceptance criteria must be established and documented for all new systems. These must identify and incorporate acceptance testing requirements. The following items should be considered:

- Performance and capacity requirements.
- Error recovery and restart procedures.
- Business continuity implications.
- Training in the operation and use of the system.

The installation of new systems must not adversely affect or impact existing systems, particularly during critical events (e.g. Year End) or peak processing times.

Businesses must be involved in all stages of the systems development life-cycle to ensure the operational efficiency of new systems.

8.9 FALLBACK PLANNING

Wherever possible, manual fallback procedures must be established and practised for each IT service to ensure at least minimum processing can continue in the event of damage or failure of information systems and networks

8.10 OPERATIONAL CHANGE CONTROL

To ensure that all changes to live systems have been properly evaluated, assessed and tested, change control and approval procedures must be established. Such procedures must apply to changes to hardware, software, firmware and application data.

Back-out and fall-back plans must be available for all changes.

POL00401642

8.11 VIRUS CONTROLS

8.11.1 Malicious and Unlicensed Software

Software must only be installed by authorised IS personnel. Such software must be compatible and the appropriate licences purchased.

All local and applicable International legislation governing software copyright must be complied with.

8.11.2 Virus Controls

Virus detection software must be installed and updated in accordance with agreed standards on all networked PCs, to scan all media on access. The software must provide the best possible protection against all known virus types (Macro, binary etc.). Unless there is a business requirement or local need, consideration should be given to disabling floppy drives or restricting them to prevent the loading of certain types of files (.exe, .bat, etc.)

Where virus protection is not provided on machines a stand alone virus detection ("sheep dip") machine should be provided to check all magnetic media (diskettes, CDs etc.) brought into the Post Office Account or loaded from a PC without virus protection. Clear instructions must be provided to all staff to ensure that disks are not introduced into the Post Office Account without being virus checked.

All machines, without virus protection, removed from Post Office Account premises must be scanned for viruses upon their return and prior to connection to any network.

All virus occurrences must be logged and treated as security incidents.

8.12 PROPRIETARY SOFTWARE

All purchased software must, where possible, before use be examined carefully on an isolated environment which does not contain essential, secret or time critical files.

Normal acceptance testing must be sufficient to detect viruses in bespoke or customised software. PC software obtained "shrink-wrapped" from a reputable supplier may be considered to be low risk (but not no risk!). PC software obtained from the public domain, or received unsolicited, must be considered to be high risk and must be verified in an isolated environment before use.

The downloading of free software or shareware by individual users must not be permitted. If such software is required for business purposes it must be requested via the system manager, licence fees paid, and tested.

Unsupported software should only be used with appropriate levels of authorisation.

8.13 USE OF GAMES/SHAREWARE/NON-PROPRIETARY SOFTWARE

Games software and applications which have no valid Post Office Account business purpose must not be used.

Software available free or cheaply ("shareware") must not be used on Post Office Account computers or networks unless a sound business case has been approved and appropriate security has been enforced.

Staff and contractors must not be permitted to run their own software on Post Office Account computers or networks unless there is a valid business purpose for the use of such non-proprietary

POL00401642

software. The software must be obtained through the approved Post Office Account purchase process. In such cases, line managers must:

- Confirm that the user holds a valid license to use the software for the intended purpose on Post Office Account equipment
- Obtain approval for this use from senior line management
- Ensure that the software is appropriately tested before it is loaded onto Post Office Account computers or networks
- Check periodically that the user continues to hold a valid license
- Delete the software as soon as the user leaves the Post Office Account or ceases to hold a valid license for the software

8.14 SYSTEM CONFIGURATION

System BIOS should be password protected to prevent unauthorised modification to the configuration of personal computers and network servers.

8.15 HOUSEKEEPING MEASURES

8.15.1 Data Back-up

To permit recovery from system failure, data corruption or virus infection, and to satisfy legal, system classification or nominated data owners' requirements, all data must be backed up.

Backed up data must be stored securely and off-site away from the prime source of information.

Off site storage must provide appropriate environmental and other (fire proof safe, access etc.) controls.

Retained information must be allocated a date when retention can cease, and a method of disposal (where appropriate) should be stated.

Back-up data must be regularly audited and tested to ensure that it can be relied upon in an emergency.

Procedures must be established to control movement of data between the prime and back-up locations. Documentation must also be retained at both sites which details the location and content of data.

Local data (stored on floppy or PC hard drives) must be reviewed, and where a classification of at least important, confidential or time significant is allocated then the data must be subject to local agreements to provide regular back-ups and off-site storage and testing.

Data stored on lap-top computers which is not subject to automated back-up routines, to minimise the potential loss of information additional backup routines must be implemented which ensure that:

Data is backed up regularly either to file servers or floppy disks.

Users are made aware of their responsibilities to back up data in relation to the frequency of taking backups and assistance in relation to the storage and security of these backups.

8.15.2 Operator Logs

Computer operators must maintain logs of all work carried out, to include as appropriate:

- Systems start and finish times.

POL00401642

- System errors and security incidents.
- Confirmation of the correct handling of data, files and computer output.

8.15.3 Fault Logging

All faults must be reported, logged, and corrective action taken. Corrective measures must not compromise security controls.

Reviews of the fault logs must be carried out by line management to ensure that the faults have been satisfactorily resolved, and to identify any trends.

8.15.4 Environmental Monitoring

Temperature, humidity and power supply quality must be monitored in accordance with manufacturers' specifications.

8.16 NETWORK MANAGEMENT

8.16.1 Network Security Controls

Operational responsibility for networks should be separated from computer operations where practical.

Responsibilities and procedures for the management and control of remote equipment, including equipment located in user areas, must be clearly established.

Controls must be established to safeguard the confidentiality, availability and integrity of data passing over public networks, and to protect connected systems.

Sensitive information travelling across a network must be encrypted. Essential information must be authenticated e.g. digital signature.

Computer and network management activities must be closely co-ordinated to optimise the service to business and to ensure that security measures are consistently applied across the IS infrastructure.

Networks must be designed to avoid a single point of failure, and configured to automatically re-route around failures. Tables containing the routing options of operational networks must be maintained, and protected as secret documents.

8.16.2 External Connections

External connections must be routed through appropriate controls (physical isolation, logical access controls, message checking, Firewalls, auditing etc.) to ensure system and network security,

8.17 CRYPTOGRAPHIC STANDARDS

Post Office Account will comply with industry best practise with regard to the protection of sensitive data. It also complies with relevant regulatory requirements and with ISO standards

POL00401642

for the handing of cryptographic key material in accordance with agreed contractual obligations.

Only nationally or internationally recognised encryption algorithms will be used on Post Office Account systems and networks. However, where appropriate, Post Office Account will follow recognised financial industry guidelines on all matters concerning cryptography. This includes:

- Choice of encryption algorithms,
- Strength of mechanisms,
- Encryption of information stored on disks within post offices, and
- Encryption key management (including key generation, distribution and change).

8.17.1 Manual Cryptographic Key Management

Cryptographic master keys are the highest level of key, used to encrypt other keys. They must be held in at least two component parts, each held by a different person. It must not be possible to derive the master key from one part.

Master key components must be stored in dual-controlled fire-proof safes. Each component must be stored in a separate location and never be available to, or under the control of, a single person. Master key components must be transported separately in a secure manner, and such movements must be subject to a detailed audit log. Master key changes must be subject to change control.

Duplicate keys for cryptographic hardware devices must be stored at physically separate secure locations.

8.17.2 Automated Cryptographic Key Management

Automated key management processes must conform to the same levels of security as those required by the Manual Cryptographic Key Management.

8.18 MEDIA HANDLING PROCEDURES

8.18.1 Management of Magnetic Media

Media must be stored in a safe and secure environment in accordance with manufacturers specifications. Magnetic media labels must be non-descriptive.

8.18.2 Data Handling Procedures

Procedures must be established for the secure handling of all secret and confidential input or output media to protect it from accidental or deliberate disclosure or misuse, to cover:

- Electronic Media
- Documents
- Tapes
- Disks

POL00401642

- Reports
- Sensitive items, e.g. cryptographic material

Procedures must provide evidence that the data is complete and it has been received / distributed intact.

Regular reviews of distribution and authorisation lists must be carried out to ensure they remain valid.

8.18.3 Security of System Documentation

System documentation must be physically locked in appropriately designed cabinets.

Distribution of system documentation must be authorised by the application owner and only in accordance with an agreed distribution list.

8.18.4 Disposal of Media

Magnetic media no longer required by the Post Office Account must have all data removed or erased before it is removed from Post Office Account premises. Where this is not possible, the media must be physically destroyed. An audit trail must be maintained.

Other media containing confidential or secret or system information must be destroyed by incineration or shredding.

Manufacturer's guidelines and environmental legislation must be followed when disposing of any hazardous material.

8.19 DATA AND SOFTWARE EXCHANGE

8.19.1 Agreements

Formal agreements must be established for the exchange of data or software between the Post Office Account and any third party. The agreement must specify appropriate security conditions relating to:

- Responsibilities for controlling and notifying transmission, despatch and receipt
- Standards for packaging and transmission
- Courier identification standards
- Responsibilities and liabilities in the event of loss of data
- Data and software ownership
- Data protection, software copyright, compliance and similar considerations
- Technical standards for recording and reading data and software
- Special measures to protect secret items.

POL00401642

8.19.2 Media in Transit

Controls must ensure that all media in transit remains safe and secure from corruption, damage or disclosure. The following list provides a number of options:

- Use of reliable transport or courier services
- Use of locked containers
- Delivery by hand
- Tamper proof packaging
- Splitting of the consignment for large, confidential or secret items
- Obtain confirmation of receipt
- Use of double enveloping (outer envelope states delivery address, inner envelope is marked addressee only and contains a return address or contact number)
- Registered or recorded delivery

8.19.3 Electronic Data Interchange Security

Electronic Data Interchange is vulnerable to interception. Strong security controls must be applied to ensure the integrity and accuracy of the data, and to safeguard connected computer systems.

The security controls applied to EDI transactions must be agreed with the trading partners.

8.20 SECURITY OF ELECTRONIC MAIL

E-mail systems are inherently insecure. Access control is weakened by the tendency of users to leave themselves connected, and by personal authentication only being password-based. Great care must be taken before such systems are used.

External electronic mail must not be used to transmit secret information for Post Office Account use and knowledge only.

8.20.1 Security of Electronic Office Systems

The security of electronic office facilities must consider:

- Policy and controls to manage information-sharing on electronic bulletin boards.
- The suitability of the system to support critical business applications.
- Back-up and fall back arrangements.
- The categories of staff, contractors or business partners allowed to use the system, and the locations from which it may be accessed.

8.21 ACCEPTABLE USAGE POLICIES

8.21.1 Internet & Email Usage Policy

Fujitsu have published a policy on the acceptable usage of Email and the Internet facilities within all areas of Fujitsu this policy is available to all Post Office Account staffs via CafeVik.

POL00401642

9 SYSTEM ACCESS CONTROL

9.1 POLICY

Access to Post Office Account business Information, systems and networks will be restricted to authorised persons only, in order to prevent and detect unauthorised use or abuse. Monitoring will take place to in order to ensure adherence to this policy

9.1.1 General Principle

To maintain effective security within the Post Office Account it is vital to ensure that data can be accessed and processed by authorised people. To provide this level of protection, clear and concise procedures and standards must be documented and communicated to all employees. This section contains general principles regarding access to systems and data. Specific detailed access controls will be published with the Horizon Access Control Policy (ACP).

9.2 ACCESS TO COMPUTER SERVICES AND DATA

9.2.1 Documented Access Policy

Line managers must strictly control access to information systems and networks under their direction or ownership. They must implement a formal process for requesting, authorising, granting, reviewing and revoking access rights to Post Office Account business information, systems and networks.

Business managers, through their nominated system, application and network owners ("owners"), must maintain a clearly defined access policy. This policy must define the access rights to each information system, application and network under their direction or ownership, for each user or group of users (based upon agreed role profiles).

Access to each system, application and network must only be granted in response to a formal application via the owner. Lists must be maintained of all users or groups of users for each information system, application and network.

Lists of users or groups of users for each information system, application and network must be maintained by designated systems security administrators ("administrators"), who must manage user access in accordance with the access policy.

When approving access rights, business managers must consider a user or group of users':

- Need for access
- Potential conflict due to overlapping responsibilities (segregation of duties)
- Incompatible job functions
- The level of access required (read, update, delete)
- The period of access.

9.3 IDENTIFICATION

In order to establish individual accountability for all activities, each user of a shared computer system or network should have a unique UserID allocated by the appropriate system or network security administrator e.g. except in exceptional circumstances the sharing of userids will not be allowed.

POL00401642

9.4 AUTHENTICATION

It is necessary to verify that the user is the authorised user (owner of the UserID). This can be carried out by a number of means, including passwords, tokens and Personal Identification Numbers (PINS).

Each system must verify that a UserID is valid and is authorised to perform the task.

9.5 AUTHORISATION

Each system must allow access to computer resources only to users who have valid authority. Such access must be based on the principles that

Access to computer services, data and networks will be assumed to be not required unless specifically requested.

The owner of an information resource decides who should have access to that resource and in what mode (read, write etc.) and supplies confirmation to users of their access privileges.

Whenever a user attempts to access a resource, the access control system checks and verifies that the access can be authorised. If access is forbidden the access violation must be recorded and investigated.

9.6 ALLOCATION OF ACCESS RIGHTS

9.6.1 User Registration

Access to all multi-user IS services must be controlled through a formal user registration and de-registration procedure operated by the administrators.

Access to information systems and networks must only be granted by the administrators once a written request (or an alternative agreed method Email etc.) has been received and authorised by the owner or nominated deputy. A record of all requests to grant access must be retained by the administrator in accordance with agreed Post Office Account document retention standards.

Owners must provide users with a written statement of their access rights, together with guidelines which detail users' security responsibilities.

Owners must ensure that controls are in place to prevent access until the authorisation procedures are complete.

Periodic checks must be carried out to identify inactive user accounts. Access rights for these accounts must be revoked until the validity of the account has been determined.

Controls must be in place to ensure that user accounts are removed immediately for any user who has changed jobs or left the Post Office Account

In addition to the access controls and procedures for individuals who join, transfer within or leave the Post Office Account, owners must ensure that user access rights are reviewed on a regular basis (at least annually).

9.6.2 User Profiles and UserIDs

In order to establish individual accountability for all activities, each user of a shared computer system or network must have a unique identification (UserID) allocated by the system security administrator. The UserID should be the employees Post Office Account staff ID, in the case of temporary or contract staff a unique identifier should be agreed with the security administrator. Associated with this UserID must be a user profile detailing:

POL00401642

- The UserID
- The users name
- Details of access privileges
- Other information as appropriate

These user profiles may then be used to control the activities of authorised users on the system. They must be regularly monitored by the appropriate systems security administrator, to confirm their validity and accuracy.

9.6.3 New Users and Alterations to an Existing UserID

System security administrators must carry out the following actions when authorising a new UserID, or when altering/suspending/removing an existing UserID:

- Only perform the changes following a written management authorisation
- Send confirmation of the changes to the user and his/her line manager.
- Forward an initial password for temporary use to new users under separate cover.
- Release of Locked-Out UserIDs

System security administrators must carry out the following actions when processing requests for releasing a UserID following its being locked out by the system:

- Investigate the reason for the lock out.
- Consult with the user, and if necessary the users line management.
- Reactivate the UserID only when satisfied that such reactivation is appropriate.
- Document each incident. When an incident is unexplained, or in repeated cases, line management must be informed.

9.7 PASSWORDS

Unless other secure and agreed verification methods are present, biometrics, tokens, etc, passwords must be in place to control access to all information systems, applications and networks. User passwords must:

- Be kept private, individuals will be held accountable for all activities undertaken by their UserID.
- Be a minimum of 6 characters in length.
- Include at least one alphabetic and one numeric character.
- Expire after 30 days.

An initial password assigned to a new or re-instated user must automatically expire when first used and require the entry of a new password chosen by the user. System, application and network parameters must prevent:

- The reuse of previous passwords (the previous twelve passwords must be checked).
- The use of weak passwords (user id, user name, system name, no more than two consecutive characters are the same etc.)

POL00401642

- User access after the entry of three consecutive incorrect passwords

Passwords must not be incorporated into any automated log on process or stored in a macro or function key.

All passwords stored on computers must be protected by one way encryption, and must not be displayed in clear-text on printouts, screens etc. Passwords must also be protected to at least the same level as the information to which they allow access.

The use of distress passwords should be considered where members of staff may be put under duress through, threat, kidnap, burglary, etc. A distress password is a pre-arranged password, different from a user's usual password that is used to signal that the user is being coerced to access the system under duress.

9.8 ISSUE AND REISSUE OF PASSWORDS

System security administrators must carry out the following actions when issuing / reissuing passwords:

- The new password must be delivered to the correct person by a secure means and separate from its associated UserID.

New passwords must only be provided to people who have forgotten their password only after verifying that the person requesting a new password is in fact the owner of the UserID. This will require that the request is made:

- In person
- By an authorised line manager or supervisor
- Use of an independent authentication system

9.9 SPECIAL AND PRE-SET PASSWORDS AND USERIDS.

Default passwords and/or UserIDs issued with new software or hardware must be changed as soon as possible, and before operational use of the software or hardware. Revised passwords must be as long in length as possible and include both alphabetic and numeric characters.

System manager and other powerful privileged passwords and UserIDs must be strictly controlled.

9.10 TOKENS

Tokens are physical objects such as plastic cards or smart cards which a user holds for authentication purposes. On their own they are more secure than passwords since owners will be aware of their loss. However, tokens are normally used in conjunction with PIN numbers or passwords thus providing an even greater level of security.

Token/PIN administration must be under dual control, and must be segregated from other functional tasks. It must ensure that:

The process of creating, updating or enabling host records is under the control of at least two individuals

Users must acknowledge receipt of the token/PIN before the token is enabled

Token/card and PIN issuing and distributing facilities must be completely physically separated, and controlled separately. The despatch of tokens/cards and PINs must be separated by at least three working days, unless such separation is achieved by different methods of delivery. Token systems must:

POL00401642

- Permit the PIN number to be user changeable
- Ensure that the PIN is at least four characters in length
- Ensure that the PIN and UserID are different
- Permit a maximum of three attempts allowed for PIN entry
- Ensure that PINs sent across transmission lines are encrypted
- Ensure that tokens are resistant to tampering and duplication

A record of all tokens issued must be retained and employees required to sign for the token. A document must be issued with all tokens which details acceptable uses and the consequences for misuse.

Tokens must be recovered when a staff member is reassigned or on termination of their employment.

9.11 BIOMETRICS

The use of biometric verification should be considered, subject to risk analysis, to provide additional levels of security for all commercially sensitive or critical information.

A biometric is a physical characteristic or piece of information unique to an individual that can be used in preference or in addition to a password. Examples of such biometrics include fingerprints, signature dynamics, retina scans and speech characteristics.

9.12 AUTHENTICATION FAILURES

After the maximum number of consecutive attempts allowed to provide the correct authentication, by password, token or biometric, has been exceeded, a user's ID must be locked out until restored by the appropriate system security administrator. All authentication failures must be logged, and the appropriate administrators informed.

9.13 EMERGENCY ACCESS RIGHTS

Emergency situations, escalation procedures and emergency actions must be defined, approved and documented.

Owners must nominate in advance those users to whom emergency system, application or network access may be granted.

Such emergency passwords and UserIDs can provide powerful privileges and must therefore be strictly controlled. Where these are pre-allocated, they must be retained securely under lock and key.

9.14 EMERGENCY PASSWORDS MUST BE CHANGED AFTER EACH USE.

Use of emergency access rights must be strictly monitored and audited, and the reasons for their use reviewed by line management after the event.

Owners must log all use of emergency access rights. Such logs must be reviewed regularly by business managers.

9.15 LOGON PROCESS

Systems, applications and networks must identify and verify the identity of each user when access is requested. If necessary the terminal or location of the access request must also be matched against the user's profile.

POL00401642

The logon process must require the entry of a unique UserID and some form of secret or unique authentication information (password, token, biometrics etc.) No system or application identifiers must be displayed until the logon process is complete.

A general notice must be displayed before logon to indicate that Post Office Account systems, applications and networks must only be used by authorised personnel for business purposes only.

Post Office Account systems must not indicate which part of a failed access request was incorrect, or provide any assistance. The session must be disconnected immediately.

Systems, applications and networks must maintain a record of all failed logon attempts to allow audit and investigation.

9.16 SYSTEM AND NETWORK USERS

9.16.1 User Responsibilities

Users must be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use and selection of passwords together with the security, protection and maintenance of user equipment.

Awareness updates will be made to staff, these will utilise all available communications methods CafeVik, POA Web Site, Message Cascades, etc, to reinforce the security message and to ensure staff are kept aware of the latest developments.

9.17 SYSTEM ACCESS CONTROLS

9.17.1 User Controls

Access to computer systems must be restricted to authorised users.

Where appropriate, systems must restrict connection times and duration of user sessions.

Each system user must be given a unique system identifier (UserID). The use of generic or departmental UserIDs must not be used unless there is a specific system restriction or an overriding business need. In all such instances, a waiver will be required.

Inactive sessions should be automatically terminated (timed out) after 15 minutes, unless the time out would result in delays to customer service, in these instances a password protected screen saver must be used.

9.18 APPLICATION ACCESS CONTROLS

9.18.1 User Controls

Access to applications and their data must be restricted to authorised users, to the minimum level required for them to undertake their duties. Access must be denied by default.

To ensure that user access is limited to approved privileges, user access to applications must wherever possible be via controlled menus or graphical user interfaces (GUIs).

Applications must control access rights of users, e.g. read, write, delete, execute etc.

Applications must control distributed management functions via a GUI.

POL00401642

9.18.2 System Utilities

System utilities provide high level access rights, which may be capable of overriding system and application controls. The number of authorised users for each system utility must be kept to a minimum, and regularly reviewed.

All system utilities must be password protected.

All unnecessary utility and system software must be removed from the system or network. Compilers, editors and other utility software must not be stored alongside operational systems when not in use.

9.18.3 Applications Development

All applications must be reviewed during their development and testing to ensure that they comply with the Information Security Policy and Standards, and that they do not compromise or invalidate the effectiveness of current system security measures.

9.18.4 Program Source Libraries

Program source libraries must not be held in operational systems.

Access to program source libraries must be restricted to authorised staff only. IS support staff must not have unrestricted access to the library.

Programs under development or maintenance must not be held in operational program source libraries.

The updating of program source libraries and the issuing of program sources to programmers must be strictly controlled via a release management process, and be subject to formal change control procedures.

Program listings must be held in a secure environment and be subject to regular audit.

Old versions of source programs must be archived, with a clear indication of the dates and times that they were operational.

9.18.5 Production Executable Code

Production executable code must only be updated via a formal change control process.

Updates to executable code libraries must only be performed by authorised staff, together with operators and job scheduling systems to execute the programs and backup the libraries.

All updates to production executable code must be recorded for audit trail purposes.

9.18.6 Sensitive Applications

Sensitive applications must run on their own dedicated resources. Alternatively, they may share resources with trusted applications and systems with the agreement of all involved parties.

The sensitivity of an application must be identified and documented by the application owner but will usually apply to all applications with a category of:

POL00401642

- Time Critical
- Essential
- Secret
- Network Access Controls

9.19 USER CONTROLS

All access to Post Office Account networks must be restricted to authorised users, and only to services, applications files or data for which those users are authorised.

Terminal or node identification must be enforced for all secret, essential or time critical information so that sessions may only be initiated by users from defined locations.

9.20 REMOTE ACCESS CONTROLS TO POST OFFICE ACCOUNT SYSTEMS

All remote access to Post Office Account systems, applications and data, irrespective of access route, must be restricted to authorised users, and only to services, applications files or data for which those users are authorised. Such remote access must require verification and authentication of UserIDs, passwords, tokens, biometrics and where possible location details before connection is allowed.

Transmissions of data between remote users and Post Office Account systems and applications must be encrypted to prevent accidental or deliberate interception.

The use of industry standard remote access controls, e.g. Remote Authentication Dial-in User Services (RADIUS) and Terminal Access Controller Access Systems, TACACS, must be adopted where Post Office information is being transmitted.

New technologies and facilities must be developed with built-in security to maintain the integrity of Post Office Account information, systems, applications and networks.

All remote logon attempts, successful and unsuccessful, must be recorded. Such logs must be audited on a regular basis to allow identification of usage patterns, unusual activities and unauthorised attempts to access protected files.

Virus protection software must be installed to filter any viruses contained within any incoming data before it is accepted into Post Office Account systems.

Consideration must be given to the encryption of all data held on remote support laptops or remote home based computers.

Guidelines for the use of external access facilities must be issued to all remote users.

Remote logon methods must be regularly tested to ensure that it is resilient against new and existing methods of unauthorised access.

Appropriate security measures must be applied to systems accessed using dial-in technology, these must include

Token-based challenge response technologies providing one-time passwords

Configured to call only a predefined number, care must be exercised in view of the possible use of call-forwarding facilities at the remote terminal.

Caller Line ID to validate the incoming call number against an internal database of authorised numbers.

POL00401642

The maximum permissible duration of logon must be specified to disconnect inactive users and disrupt any unauthorised users who may have gained access to the system.

Access to Post Office Account corporate networks provided through third party managed systems must provide security which provides verification and encryption for all remote users.

UserIDs and all access privileges must be revoked immediately for staff and contractors with remote access who leave the employ of the Post Office Account Under certain circumstances, dial-in telephone numbers may need to be changed. All equipment provided by the Post Office Account must be returned by such individuals.

9.21 REMOTE ACCESS TO POST OFFICE ACCOUNT SYSTEMS

Appropriate security measures must be applied to systems accessed using dial-in technology, these must include

Token-based challenge response technologies providing one-time passwords

Configured to call only a predefined number, care must be exercised in view of the possible use of call-forwarding facilities at the remote terminal.

Caller Line ID to validate the incoming call number against an internal database of authorised numbers.

The maximum permissible duration of logon must be specified to disconnect inactive users and disrupt any unauthorised users who may have gained access to the system.

Access to Post Office Account corporate networks provided through third party managed systems must provide security which provides verification and encryption for all remote users.

UserIDs and all access privileges must be revoked immediately for staff and contractors with remote access who leave the employ of the Post Office Account Under certain circumstances, dial-in telephone numbers may need to be changed. All equipment provided by the Post Office Account must be returned by such individuals.

User guidelines for all remote users must be issued, to include a statement that such users are responsible for the security of the traffic they originate.

9.22 ENCRYPTION OF TRANSMITTED DATA

Unique message identification to prevent the replaying of messages and audit records must be retained in accordance with statutory and regulatory requirements

9.23 THIRD PARTY CONNECTIONS AND LEASED LINES

Sharing of secret, and private and confidential information needs to be carried out carefully, especially during activities such as:

- Dealing with trading partners, suppliers and customers which involves exchanging sensitive strategies, marketing plans, commercial information and product plans.
- Contracting out work which is likely to involve secret information or operations that are essential or time critical.

9.24 NEGOTIATING WITH OTHER ORGANISATIONS.

Formal contracts, including confidentiality clauses as appropriate, must be in place for the provision of third party connections and dedicated leased lines. Third parties must enforce standards of

POL00401642

information security at least equal to those applied in-house. Effective security will only be in place if everyone involved follows the Post Office Account security standards and practices.

All external electronic connections into Post Office Account information systems, applications and networks must be via an approved, centrally-managed gateway.

Gateway systems must provide protection to the highest available commercial standards, incorporating reputable 'firewall' capabilities to restrict electronic traffic to approved message types and/or users. Gateway systems and fire walls must be located in physically secure premises.

User access via third party connections and dedicated leased lines must be authorised in accordance with user access policy.

When information is passed to a third party, it must be marked with the appropriate classification to ensure that the receiving organisation can handle and protect it correctly. In some circumstances it may be necessary to provide the recipient with specific and/or additional advice and build special security provisions into contracts.

A combination of proactive management and verification by Post Office Account line management must be used to check that recipients of Post Office Account information are protecting that information correctly.

9.25 REMOTE DIAGNOSTICS

Remote diagnostic ports must be configured only as dial-out, and remain at all times under the control of Post Office Account personnel. They must only be activated when a problem requiring remote diagnostics has been detected, and must be disconnected after use.

Before remote diagnostic sessions are started, production applications must be stopped and the host system isolated.

9.26 ACCESS TO THE INTERNET

Access to the Internet from Post Office Account business systems and networks must only be granted in response to a justified business requirement. Such Internet access must only be for Post Office Account business purposes.

Suitable protection must be enforced to ensure that any web content may only be altered by authorised personnel.

The provision of services over the Internet must be controlled to ensure the confidentiality of customer information and the protection of the Post Office Account information systems and networks.

Suitable practises and procedures must be in place to ensure the secure management of the e-commerce channel. Internet applications must ensure:

9.27 STRONG AUTHENTICATION AND IDENTIFICATION

All access to Post Office Account information, networks and systems must be authorised. Customer Account identification information such as Account numbers, PINS, Tokens etc. which if revealed would allow unauthorised use of the account must be encrypted and an audit trail of all access provided.

POL00401642

9.28 NON-REPUDIATION

To verify the authenticity of messages and transactions the use of technologies such as digital signatures must be used where appropriate.

9.29 AVAILABILITY

Unless a service is reliable, it must not be offered, Customer frustration over banking systems that do not work on demand may result in loss of business.

9.30 CONFIDENTIALITY OF RECORDS

To protect all customer and Post Office Account data from being accessed by unauthorised users.

9.31 OTHER ELECTRONIC STORAGE MEDIA

Post Office Account data must not be stored on other electronic devices, palm top computers, personal organisers, etc, unless the device has been approved and the data is stored in an encrypted format.

Dial in access numbers to Post Office Account networks must not be programmed into mobile phones.

9.32 SECURITY ACCESS NETWORK

A Security Access Networks, consisting of firewall, access routers, intrusion detection or prevention and anti-virus and content checking facilities will be implemented to protect the Post Office Account's networks from attacks by sources external to the Post Office Account

All external TCP/IP network traffic into Post Office Account's information, systems and networks must pass through a security access network. Firewalls and associated technologies, hardware, software, etc, must be capable of restricting electronic traffic to approved ports, protocols, source and destination addresses and users, and must be capable of filtering computer viruses as well as preventing:

- Address spoofing
- Syn Floods
- Denial of service attacks

Any other electronic links not using the TCP/IP protocol must use appropriate measures, e.g. hardware encryption to ensure the confidentiality and integrity of the transmitted data.

Audit functions must be enabled to provide a record of all communications to or though the firewall. The firewall must also generate an alarm whenever suspicious activity is detected.

The traffic passing through the firewall may contain information which is required to verify a transaction. To ensure compliance with appropriate legislation, such information must be archived for the appropriate statutory period.

All configuration changes to Post Office Account Firewalls must be managed by a formal change control process

POL00401642

9.33 MONITORING SYSTEM ACCESS AND USE

9.33.1 Audit Trails

Security audit trails are required to provide traceable evidence of all activities affecting information system, application and network resources. This must include both transaction and system audits. The audit trail must include all violations and exceptional events as required by both the owner and audit functions. The audit logs must be retained for a minimum period commensurate with the requirements of the system or any regulatory authorities. Audit Trails must be designed to enable management to monitor:

- All attempted violations of the system, such as failed password or access attempts.
- Actions of security administrators.
- The actions of all systems users.
- All access to information with a classification of confidential or secret.
- Access lists for all resources with a classification of confidential or secret.

Audit trails must record as a minimum:

- UserID
- Date and time of event
- Terminal identity or location
- Detail of event including system error codes (where applicable)

Events that must be logged and highlighted to administrators include:

- Failed logon attempts
- Failed access attempts
- Tracking of selected transactions
- Use of resources classified as confidential, important or above.

Audit trails and logs must be protected to minimise the risk of unauthorised manipulation. They must be monitored regularly to detect unusual or unauthorised access attempts, and investigated. Information which is subject of an investigation or audit must be preserved and specially protected as it may be required as evidence in a court of law.

9.34 CLOCK SYNCHRONISATION

The Horizon network and all systems operating within Horizon will be synchronised on Greenwich Mean Time.

Procedures must be established and followed to ensure all systems clocks and therefore logs reflect the correct date and time in respect of Greenwich Mean Time and that during periods of British Summer Time that Horizon remains synchronised on Greenwich Mean Time.

POL00401642

10 SYSTEM DEVELOPMENT AND MAINTENANCE

10.1 POLICY

Appropriate security features will be incorporated at the design stage, and then maintained during the life-cycle of all applications, systems and networks.

10.1.1 General Principle

Security countermeasures are substantially cheaper and more effective if incorporated in application systems at the requirements specification and design stages.

10.2 SECURITY REQUIREMENTS FOR APPLICATIONS SYSTEMS AND NETWORKS

10.2.1 Project Development

A development environment, where application or other system software is being developed and tested prior to being used 'live', must be subject to strict security. Of particular importance are access controls, separation from 'live' systems, and change/version control.

An analysis of security requirements must be undertaken at the development stage of any new systems, application or network project. Business requirements for such projects, or for enhancements to existing systems, applications and networks, must specify the requirements for security controls, both automated and manual.

Security controls must reflect the business value of the information assets to be protected, together with an identification of the potential loss or damage which may result from a failure or absence of security.

Security controls must protect the confidentiality, integrity and availability of information assets. All types of control (manual and automatic, technical and traditional) should be used, to prevent, detect and recover from all potential security incidents and breaches. Security controls must:

- Control access to information and services
- Segregate duties
- Produce audit trails
- Verify and protect the integrity of data
- Satisfy back-up requirements
- Ensure business continuity
- Protect the data from unauthorised or accidental amendment, modification and access

10.2.2 Risk Assessment

System owners and project managers must conduct risk assessments for each new project, or for important modifications to existing systems, to consider:

- Business Risk
- Project Risk
- Security Risk

POL00401642

In this way, the potential risks to the system can be identified, and the countermeasures needed to minimise these risks can be designed and implemented. As part of this risk assessment, measures to address the following security requirements must be considered:

- Control of access to networks.
- Protection of transmitted information against unauthorised disclosure, alteration, destruction or interference.
- Personal authentication of communicating parties who are carrying out transactions or exchanging messages.
- Message authentication of transactions and messages between communicating parties.

10.2.3 End User Computing

Business systems developed by user departments must be designed and implemented in accordance with this policy. Particular attention must be given to the following areas

- System design
- Acceptance testing
- Change control
- Access control
- Backup and restore requirements
- Documentation

10.3 SECURITY IN DEVELOPMENT AND SUPPORT ENVIRONMENTS

10.3.1 Control of Operational Software

The updating of operational program libraries must be restricted to authorised personnel. An audit log of all changes or updates to operational program libraries must be maintained.

Executable code should not be implemented until it has been successfully tested, and user acceptance has been obtained.

As a contingency measure, an archiving mechanism must be in place to ensure all previous versions of software are retained.

10.3.2 System Test Data

Control procedures for operational application systems must also apply to test application systems. Live data must be erased from test applications immediately after all testing is complete.

Authorisation must be obtained from data or application owners before live data is copied to a test application. Such events must be logged for audit purposes.

10.3.3 Third Party Software

Wherever possible, code in third party software packages should not be modified - any changes could affect the security functionality of the software or invalidate vendor support agreements.

POL00401642

Redevelopment might also be necessary when implementing new versions of the package. Before any changes are made to third party software, applications owners should consider the following:

- Will vendor support be available after changes are made?
- Has vendor consent for changes been obtained?
- Are the proposed changes available from the vendor as standard program updates?
- How will changes be made to future versions of software?
- Will internal expertise be available when further changes or updates are required?
- Are there any legal implications to the changes?
- Are the proposed changes necessary and cost effective?

10.3.4 Separate Development Environments

Development environments must be separated physically and logically from live environments to protect the live environments from unauthorised access or modification.

10.4 CHANGE CONTROL PROCEDURES

10.4.1 Change Control

There must be strict control over the implementation of changes to the software or hardware of any Post Office Account system, application or network. Such change control procedures must ensure that any changes do not compromise any security or control procedure. Change control 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 UserIDs/passwords, data and linkages when the system becomes live.
- Changes only carry out their required function and nothing more.
- Only those changes that have been tested are implemented on the live system.
- Changes meet operational requirements.

10.5 EMERGENCY CHANGES

Change controls procedures must exist which permit the controlled correction of live systems in emergencies in order to meet production deadlines. At least two persons must implement such changes. The change must be reviewed and approved by the appropriate line management as soon as possible. After review, emergency changes must be removed from the live environment or consolidated via the normal change control procedure.

POL00401642

10.6 OPERATING SYSTEM CHANGES

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

POL00401642

11 BUSINESS CONTINUITY PLANNING

11.1 POLICY

Business continuity plans will be available to protect critical business processes from the effects of major failures or disasters.

11.1.1 General Principle

In most areas of the Post Office Account, Information Technology is a critical element of the business. Business Continuity Planning (BCP) provides a framework for the identification and implementation of commercially effective contingency arrangements so that the Post Office Account is able to survive any IT related disaster without major financial loss or damage to its reputation.

11.2 APPROPRIATE PLANS

11.2.1 Business Continuity Planning Process

Plans for the continuation of business processes and operations in the event of the destruction or unavailability of information systems, networks, accommodation, communications and business resources will be developed and maintained. Guidelines and support should be provided by members of the Business Continuity Planning team to ensure consistency of plan development and a co-ordinated approach across the Post Office Account. The business continuity planning process will cover the following:

- Identification and prioritisation of business processes
- Determination of the potential impact upon the business process of various major incidents and disaster scenarios.
- Identification and agreement of all responsibilities and emergency arrangements
- Documentation of agreed procedures, processes and re-instatement timescales.
- Education of staff in the execution of plans
- Exercising of plans
- Maintenance of Plans

11.3 CONSISTENT PLANS

11.3.1 BCP Framework

A single framework of plans will be maintained to:

- Ensure that all levels of plans are consistent.
- Identify priorities for testing and maintenance.

There will be three main components to this framework:

- **Emergency procedures** describing the immediate actions to be taken following a major incident in order to protect human life and business processes.
- **Fallback Procedures** describing the actions to be taken to provide continuity of service without normal IT facilities, accommodation, personnel and communications.

POL00401642

- **Contingency procedures** describing the actions to be taken to move business activities and support services to alternate facilities.

The business impact analysis will identify the maximum elapsed time that individual services, processes or operations may be unavailable, following some form of major incident, before the Post Office Account suffers significant harm.

The BCP plan will then specify how the services, processes and operations are to be reinstated to an acceptable level within defined time scales. The BCP and business recovery plans will state:

- Individual responsibilities
- Emergency procedures which describe the invocation process following a major incident
- Fallback procedures which describe the action required to move essential services and personnel to alternative temporary locations
- Resumption procedures to describe the actions required to return to full normal service .
- An exercise schedule which specifies how and when the plan will be exercised
- The contingency arrangements and facilities that are available and how these are to be used.
- The main resources to be covered will include:
- Buildings and accommodation
- Personnel
- Computer Hardware
- Computer software and applications
- Data, whether held on magnetic or other media
- Terminals
- Voice or Data communications and networks
- Manual processes which depend on or support IT functions
- Critical non IT records

Business function plans will be developed in conjunction with specialist business functions (e.g. Personnel, Premises etc.) Where there are dependencies on areas outside of the department, these will be identified and appropriate requirements passed to the other party to ensure that the plan is cohesive and feasible. Interdependencies will be co-ordinated by the Business Continuity Planning team to ensure availability.

For critical (essential, important or time critical) activities and services which must be continued, continuity plans must detail how and whether alternative (and possibly less efficient) practices are to be followed to mitigate adverse business impacts. Plans will detail resource requirements to restore both reduced and full capabilities. Plans will rank customers and service providers by order of priority to optimise usage of the limited resources available.

Non critical services where recovery can be delayed will be listed, and agreed.

POL00401642

11.4 IMPLEMENTATION

Line managers, with the help and advice of the Business Continuity Planning team, are responsible for ensuring that appropriate plans are developed, implemented and maintained within their business divisions.

Suppliers of IT services must comply with the Post Office Account BCP requirements. Contract terms and conditions should specify suppliers' obligations in this respect.

11.5 SAFEGUARDING KEY PERSONNEL

Key personnel will be identified. Plans will cover the possibility that such key individuals may be unavailable and provide for alternatives. Travel arrangements should limit the number of key personnel travelling together.

11.6 EXERCISING OF PLANS

11.6.1 Responsibilities

Business function plan owners are responsible to line management for:

- The definition of the scope and objectives of all tests
- Frequency of exercises
- Evaluation of exercises
- Preparation and execution of contingency exercises
- Co-ordination of updates to plans.

Such exercises will be planned to minimise the impact of the business, whilst ensuring individual components of the plan are exercised in accordance with the value of the assets being exercised.

The Business Continuity Planning Team will be involved and co-ordinate all exercising of ECT business function and service recovery plans.

11.7 ERRORS AND OMISSIONS

The exercising process must incorporate a mechanism to identify errors or omissions in the plans and for these to be investigated and where appropriate the plans updated. This will be co-ordinated by the Business Continuity Planning Team.

11.8 UPDATING OF PLANS

11.8.1 Regular Updates

Business function, BCP and Service Recovery plans can quickly become out of date because of changes to the business or organisation and must be subject to regular updates. Examples of changes which may necessitate updating of plans include:

- Acquisition of new equipment
- Upgrading of operational systems
- Staff or organisational changes
- Change of contractors or suppliers

POL00401642

- Changes of address or telephone numbers
- New or obsolete business processes
- Changes in legislation
- Revised or new operating practices

Formal change control processes will ensure that implications to business function; BCP and Service Recovery plans of any change are identified, so that plans are kept up to date.

12 COMPLIANCE

12.1 POLICY

The Post Office Account is subject to both statutory legal and contractual requirements which will be explicitly defined and documented. The specific controls countermeasures and individual responsibilities to meet these requirements will be defined, documented and communicated.

12.1.1 General Principle

To meet legal requirements and to satisfy obligations to the customers, employees and shareholders the Post Office Account will utilise cost effective security measures to protect its information.

All employees must be aware that there are legal requirements relating to information which must be met. These requirements will be embodied in the procedures and controls.

12.2 COPYRIGHT, DESIGNS AND PATENTS ACT 1998

Copying of proprietary or organisational software for use on computers that do not belong to the Post Office Account or authorised organisation for any purpose is a breach of organisational policy and may be a breach of copyright.

Unauthorised copying of software or the use of unlicensed software is effectively theft, therefore within the Post Office Account are explicitly banned, any breaches of this may be subject to disciplinary actions.

All software must be installed by authorised staff who will ensure that the appropriate licenses are held by the Post Office Account and also that the introduction of new software does not compromise existing systems.

Regular audits of software will be undertaken and a register of software must be maintained.

12.3 DATA PROTECTION ACT 1998

The Post Office Account acknowledges and will comply with the Data Protection Act 1998, its Principles and the Data Protection Commissioners Guidance. Additional information on the subject can be obtained from the Security Manager.

12.4 COMPUTER MISUSE ACT 1990

Information systems, networks and equipment are provided by the Post Office Account for business purposes. Any use of these facilities for unauthorised purposes will be regarded as improper use of the facilities and may result in disciplinary action.

The Post Office Account will also comply with all relevant legislation including the Computer Misuse Act 1990, the act defines three offences:

POL00401642

- Deliberate unauthorised access to gain information
- Unauthorised access with the intent to commit a further serious crime
- Unauthorised modification, deletion or insertion of computer data or programs

12.5 FREEDOM OF INFORMATION ACT 2000

Any person making a request for information to a public authority is entitled to be informed in writing by the public authority whether it holds information of the description specified in the request, and if that is the case, to have that information communicated to him.

For the purposes of the Freedom of Information Act 2000 the Post Office is considered to be a public body and must therefore conform to the requirements of the act, consequently Post Office Account information held by Post Office Ltd may be subject to disclosure and Post Office Ltd may request assistance from Post Office Account is the provision of data held within the Horizon System.

12.6 REGULATION OF INVESTIGATORY POWERS ACT 2000

Regulation of Investigatory Powers Act 2000 makes provision for and about the interception of communications, the acquisition and disclosure of data relating to communications, the carrying out of surveillance, the use of covert human intelligence sources and the acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or accessed

It is an offence for a person intentionally and without lawful authority to intercept, any communication in the course of its transmission by means of a public postal service or a public telecommunication system.

It is also an offence for a person to intentionally and without lawful authority, other than in circumstances in which his conduct is exempt from criminal liability, to intercept any communication during its transmission over a private telecommunication system.

12.7 FINANCIAL SERVICES AND MARKETS ACT 2000

Financial Services and Markets Act 2000 makes provision regarding the regulation of financial services and markets, to provide for the transfer of certain statutory functions relating to building societies, friendly societies, industrial and provident societies and certain other mutual societies and other connected purposes.

12.8 MONEY LAUNDERING REGULATIONS 2003

The Money Laundering Regulations 2003, and amending orders to the Proceeds of Crime Act 2002 and Terrorism Act 2000, expand businesses in the regulated sector to include among others estate agents, casinos, accountants, tax advisers, auditors, insolvency practitioners, lawyers and anyone conducting a business of dealing in goods accepting cash of €15,000 (euros) or more in a single transaction.

Additional information on the subject of legal compliance can be obtained from the Security Manager.

12.9 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.

POL00401642

- 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

12.9.1 Other Legislation

The Post Office Account is obliged to comply with all legislation passed into law by the government of the United Kingdom and is committed to best practices to ensure the security and safety of its information. Regulatory and Legislative policies with which the Post Office Account will comply include:

- BS ISO/IEC 17799 A Code of Practice for Information Security Management
- Companies Act 1989

12.9.2 Regular Reviews

All areas of the Post Office Account will be subject to regular reviews to ensure compliance with security policy and standards together with all regulatory and legislative requirements. These may be carried out by the Security Manager, the programme Assurance Manager or External organisations who have a statutory right of access to information.

12.10 SYSTEM AUDITS

12.10.1 Requirements

Audit requirements including the scope of checks will be agreed and controlled with the appropriate management agreement; checks must be limited to read only access of the software and data. The resources required for system audits must be explicitly identified and made available. Care must be exercised to ensure the minimum risk of disruption to services.

Requirements for special or additional processing must be identified and agreed with the service providers. System audit access must be monitored and logged to produce an audit trail.

12.10.2 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

POL00401642

vulnerabilities in the system and for checking how effective the controls are in preventing unauthorized access due to these vulnerabilities. Caution should be exercised in case success of a penetration test could lead to a compromise of the security of the system and inadvertently exploit other vulnerabilities.

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

12.10.3 System Audit Tools

Access to system audit tools, e.g. software or data files, must be safeguarded to prevent any possible misuse or compromise. Audit tools must be separated from development and operational systems, and not held in tape libraries or other general access areas unless given an additional level of security protection.

13 WAIVERS, EXCEPTIONS AND VARIATIONS

13.11.1 Issue

It is expected that the Post Office Account Information Security Standards and Codes of Practice will be adhered to, however, it is recognised that technology or circumstances may make compliance impractical in a limited number of instances. A waiver process has been developed to deal with these instances. Where compliance cannot be practically achieved a waiver must be requested.

A waiver can be requested by the project manager, and agreement to proceed obtained from the nominated system owner with agreement also being sought from the Security Manager. Once agreed the waiver will be lodged with the Security Manager, who will then ensure that they are reviewed regular basis.

This should be viewed as a temporary measure, therefore should the conditions which gave rise to the waiver change; there is still a requirement to adhere to standards irrespective of the existence of a valid waiver.

13.11.2 Additional Measures

Compensatory measures must be put in place to minimise the impact of any failure to comply with the Security Policy and Standards. Plans must be developed to reduce or remove as quickly as possible the need for such waivers, exceptions and variations to policy.