POL00394583

Community Information Security Policy for Horizon

Author	Head of Information Security	Sue Lowther
Reviewers	Royal Mail Information Security Fujitsu Services Prism Information Security Team Business Solutions Director Group Internal Audit	Mike G Harris Bill Mitchell Ian Sayles Mike A Wells Peter Thompson
Sign off authority	Business Solutions Director	Mike A Wells
Reference configuration	PSO/000/GEN/SCO/105	
Operational Baseline Number		

POL00394583

Version	1.0	
Status	Baseline	
Classification	Working Document	
Date	Date Issued	
Circulation		

Document Control

Version History

VERSION	DATE	CHANGE DETAILS
0.1		Initial Draft
0.2		Response to comments from Fujitsu Services and RMG Information Security.
1.0	08/06/05	Base-lined

Change Control

All changes to this document are to be sent to the Change Controller named below:

Name Elaine Hollingsworth-Clarke
Job Title PSO Document Management Team Manager
Business Address No. 1 Future Walk
West Bars
Chesterfield
S49 1PF

Telephone Number(s) GRO

POL00394583

References / Related / Dependent / Parent Documents

REFERENCE	DOCUMENT REFERENCE	TITLE	VERSION	DATE

See §1.3.

Electronically Distributed Documents
Any problems, comments or improvement opportunities are to be sent to Change Controller above. If not receiving this document direct from the PSO, readers may wish to ensure it is the latest version by checking with the Change Controller.

POL00394583

Contents

POL00394583

POL00394583

POL00394583

Terms and Abbreviations

TERM	MEANING

POL00394583

1. Introduction

1.1 Purpose and Scope

This document provides policy and direction in information security for those responsible for initiating, implementing or maintaining security for Horizon. This document describes for these systems:

- End-to-end security management process and physical requirements
- End-to-end technical security requirements.

1.2 Readership

This document is intended for systems and application designers, systems managers, security and compliance managers associated with Horizon and its related systems.

1.3 Related Documents

Documents to be read in conjunction with this policy are:

- Information technology – Code of practice for information security management, ISO 17799:2000, 1 December 2000
- Link Information Security Standard, version 1.0, January 2001
- ISO 9564 Parts 1 to 3: Banking — Personal Identification Number (PIN) management and security
- ISO 11568 Parts 1 to 3: Banking - Key management (retail)
- APACS Chip & PIN Recommendation No. 12
- Post Office Ltd. Policies:
  - Information Security Policy, Post Office Ltd.
  - Clear Desk Policy, Post Office Ltd.
- Royal Mail Group Centre Technology & Information Systems policies:
  - *e-Handbook*: "Your Guide to Information Security", Information Security Intranet site, RMG
  - Freedom of Information Act policy (G30)
  - Information security (S1)
  - Investigation and Prosecution Policy (S2)
  - Royal Mail Group Human Resources – Personnel Vetting Policy
  - Security Policy (S3)
  - Information Classification Policy (S4)
  - Mobile Security Policy (S5)
  - Logical access control (S6)
  - Penetration testing (S7)

POL00394583

- Wireless LAN (S8)
- IS/IT Compliance (T1)
- Disposal policy (V4.dc)
- Anti-virus policy (T3)
- 3rd Party Connectivity Standard (S16)
- Security Architecture (S17)
- Security Design & Testing (S18)

- Legal & Regulatory (see also §12.1)
  - Freedom of Information Act 2000
  - The Data Protection Act 1998
  - The Official Secrets Act 1989
  - The Computer Misuse Act 1990
  - The Copyright, Designs and Patents Act 1988
  - Financial Services and Markets Act 2000
  - Regulation of Investigatory Powers Act 2000
  - Electronic Communications Act 2000 as amended by the Communications Act 2003
  - Money Laundering Regulations 2003

1.4 Document Classification

The policy is classified as INTERNAL and may be distributed within relevant organisations. The policy may refer to associated documents that deal specifically with sensitive security controls classified as CONFIDENTIAL. Those secondary CONFIDENTIAL documents may only be distributed and copied on a "need to know" basis.

1.5 Document Review

The owner of the policy is responsible for its maintenance and review.

2. Definitions

For the purposes of this document, the definitions below apply.

The term "**must**" identifies mandatory policy statements. The term "**should**" identifies a recommendation. The term **"will"** signifies matters that can be assumed.

Domain supplier: an organisational entity responsible for the systems and applications under its specific control and operation.

Horizon: The information system used to capture and process business transactions originating in Post Office branches. It extends:

- from the counter positions that provide the interface between the Post Office and members of the public that use its services,

POL00394583

- to the boundary with specialist service providers such as LINK, Card Account, DWP and Streamline who are outside the contractual scope of Horizon.

Post Office branch: A location where Horizon services are offered. It includes directly managed branches, franchised branches and sub-postoffices.

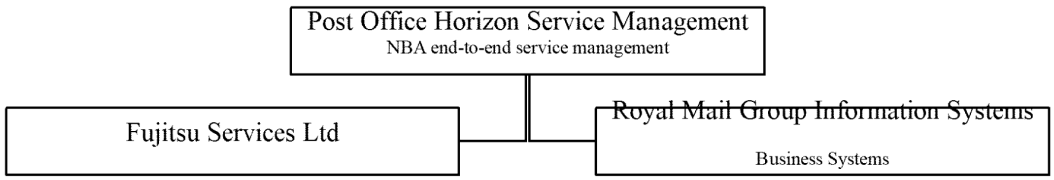
Branch staff: Those people who use the Horizon Branch Terminal. They consist of clerical staff who actually transact business and administrative staff (e.g. the sub-postmaster) responsible for managing branch specific aspects of the Horizon service.

Branch terminal: A terminal used to enter Horizon transactions typically (but not always) located at a branch counter position. The definition includes back-office Branch Terminals (used for cash accounting etc) and mobile Branch Terminals.

The **Horizon community**: all domain suppliers involved in the provision of Horizon Services, including:

- Royal Mail Group Information Systems[1]
- Fujitsu services
- Post Office Horizon end-to-end service management.

The organisation is shown below.



NOTE: Where this policy refers to the Royal Mail Group, it includes Post Office Ltd unless the context makes it clear that Post Office Ltd is excluded.

Information security: the preservation of confidentiality, integrity and availability of information:

- **Confidentiality:** ensuring that information is accessible only to those authorised to have access.
- **Integrity**: safeguarding the accuracy and completeness of information and processing methods. Integrity controls include those used to protect against fraud and those, which ensure the accountability of individuals.
- **Availability**: ensuring that authorised users have access to information and associated assets when required

Risk assessment: assessment of threats to, impacts on and vulnerabilities of information and information processing facilities and the likelihood of their occurrence

Risk management: the process of identifying, controlling and minimising or eliminating security risks that may affect information systems, for an acceptable cost.

[1] For provision and operation of Post Office backend systems, Royal Mail Group infrastructure and applications. Currently outsourced to Prism.

POL00394583

Third party: An individual or organisation that is neither:

- A domain supplier employee or contractor involved in Horizon delivery, nor
- A Post Office employee or contractor.

Third party personnel: employees or contractors of a third party.

User: Anyone involved in Horizon service delivery, including those who interact with the Horizon application, administrators, system programmers, network managers, security administrators and Horizon terminal operators.

WAN (Wide Area Network): Any communications network that extends outside the bounds of a domain's physical security area.

3. The Policy

Post Office Ltd.'s support and commitment to information security is demonstrated by enforcing and maintaining the information security policy defined in this document.

3.1 The mandate

Information Security is mandated by Royal Mail Group; it is not an option. Accordingly, all Post Office Ltd. personnel and its suppliers have a responsibility for Information Security and are bound by a number of legal obligations.

Security is only as strong as the weakest component. The Horizon community must individually and together maintain the appropriate level of information security necessary for the end-to-end Horizon services.

3.2 Objective

The Horizon Information Security Policy objective is to ensure that all the Horizon systems are protected from significant threats such that the business needs of Post Office Ltd. can be met economically, efficiently and effectively.

Each domain in the Horizon Community must establish and abide by the following policy requirements:

- to maintain an organisation to direct and manage IT security for that part of the Horizon which is within its remit.
- to ensure that the risks are reduced to an acceptable level by applying the appropriate protective measures, which are based on risk assessment, the information classification scheme and which conform to agreed standards
- to ensure Post Office Ltd are advised of all relevant breaches of security together with recommendations for recovery
- to ensure that all personnel involved with Horizon are aware of their responsibilities under this information security policy (and associated practices and procedures), and that they fully understand those responsibilities including their legal obligations

POL00394583

- to monitor and review information security arrangements to provide assurance that policy, standards and procedures remain relevant and effective.

The mandatory elements of the policy set out the minimum level of security to be adopted throughout the Horizon Community, and represent industry best practice.

The policy recognises that the measures taken by each domain may vary according to the responsibilities and risks associated with the domain. Each domain must establish and document an information security policy, consistent with this policy, which sets out the policy and responsibilities for information security within the domain.

3.3 ISO 17799 baseline

Royal Mail Group requires that Post Office Ltd. implements and operates in accordance with ISO/IEC 17799:2000, *Information Security Management: Code of Practice for Information Security Management* as a baseline, together with other approved technical and procedural standards where appropriate.

Accordingly, the Horizon community must apply ISO 17799 as the baseline for Information Security. The recommendations in ISO 17799 must be considered a statement of best practice by each domain, unless explicitly modified in this document. Post Office Ltd domains and other domains contracted to comply with ISO 17799 must comply with all applicable controls recommended in ISO 17799.

Post Office Ltd. requires all parties to apply the mandatory requirements and controls specified in this document.

There is no specific requirement to undertake certification to ISO/IEC 17799:2000.

It is the domain suppliers' responsibility to identify and comply with the relevant standards.

This document follows the ISO 17799 categories of control.

3.4 Review and evaluation

The controls documented in this document are classified as either mandatory or recommended. The mandatory controls must be complied with unless the Post Office Ltd Information Security Manager agrees a waiver. Waivers will only apply for a limited, and defined, period.

The policy will be reviewed annually. The review process will be capable of responding to any changes affecting the risk assessment. The review will consider:

- The policy's effectiveness, demonstrated by the nature, number and impact of recorded security incidents
- The cost of controls and their impact on business efficiency
- The effects of changes in technology and processes
- New and emerging risks.

The owner of the policy is responsible for its maintenance and review.

POL00394583

4. Security Organisation

Objective: To manage information security within the Horizon community.

4.1 Information security infrastructure

A management framework must be established within each domain to monitor and control information security within the domain. Suitable management forums with management leadership should be established to review the domain's information security policy, assign security roles and co-ordinate the implementation of security for the domain. Where appropriate, sources of specialist information security advice must be established and made available within the domain. Contacts with external security specialists should be developed to keep up with industrial trends, monitor standards and assessment methods and provide suitable liaison points when dealing with security incidents. A multi-disciplinary approach to information security is encouraged, e.g. involving the co-operation and collaboration of managers, users, administrators, application designers, auditors and security staff, as well as specialist skills in areas such as insurance and risk management.

4.1.1 Management Information Security Forum

Information security should be a business responsibility shared by all who have a responsibility for delivering the Horizon service. A management forum should therefore be considered by each domain to ensure that there is clear direction and visible management support for security initiatives. That forum should promote security within the domain through appropriate commitment and adequate resourcing. The forum may be part of an existing management body. Typically, such a forum undertakes the following:

a) reviewing this information security policy and approving overall responsibilities;

b) monitoring significant changes in the exposure of information assets to major threats;

c) reviewing and monitoring information security incidents;

d) approving major initiatives to enhance information security.

In each domain, one manager must be identified to be responsible for all information security activities related to that domain's delivery of the Horizon service.

4.1.2 Information security co-ordination

Within each domain an experienced security professional must have the responsibility for coordinating security for that part of Horizon that is within the domain's remit. Tasks must include:

a) agreeing specific roles and responsibilities for information security within that part of the Horizon that is within the domain's remit;

b) agreeing specific methodologies and processes for information security within that part of Horizon that is within the domain's remit, e.g. risk assessment, security classification system;

c) agreeing and supporting information security initiatives within that part of Horizon that is within the domain's remit, e.g. a security awareness programme;

d) ensuring that security is part of the domain's change management process for Horizon;

POL00394583

e) reviewing Horizon-related information security incidents arising within the domain and communicated to the domain, agreeing a classification of the severity of each and, where appropriate, agreeing a recommended recovery plan and coordinating recovery within the domain;

f) liaison with the Post Office Head of Information Security,

g) promoting the visibility of business support for information security throughout that part of the Horizon that is within the domain's remit;

h) Maintaining an awareness of good security practice within the industry and promoting it throughout that part of the Horizon that is within the domain's remit.

4.1.3 Allocation of information security responsibilities

Responsibilities for the protection of individual assets and for carrying out specific security processes must be clearly defined and documented. Each domain must have a system information security policy, consistent with this policy, which provides general guidance on the allocation of security roles and responsibilities in its organisation. This must be supplemented, where necessary, with more detailed guidance for specific sites, systems or services. Local responsibilities for individual physical and information assets and security processes, such as business continuity planning, must be clearly defined.

Areas for which each manager is responsible must be clearly stated; in particular the following must take place:

a) The various assets and security processes associated with each individual system must be identified and clearly defined.

b) The manager responsible for each asset or security process must be agreed and the details of this responsibility must be documented.

c) Authorisation levels must be clearly defined and documented.

4.1.4 Authorisation process for information processing facilities

The ISO/IEC 17799 clause describing controls for authorisation of new information systems is not relevant to Horizon. See clause 8.1 re authorisations of changes to Horizon.

4.1.5 Specialist information security advice

There must be a source of information security expertise within each domain. Where the expert feels unqualified to advise on a particular issue, suitable external advisers must be used.

The information security adviser or equivalent point of contact should be consulted at the earliest possible stage following a suspected serious 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 advise, lead or conduct the investigation.

4.1.6 Cooperation between organisations

Post Office Ltd will maintain appropriate contacts with law enforcement authorities, regulatory bodies and others to ensure that this information security policy is effective.

POL00394583

4.1.7 Independent review of information security

The Horizon Information Security policy and all referenced technical controls will be subject to quality checks by an external qualified body and Horizon will be audited against the policy and technical controls.

Each domain's information security policy sets out the policy and responsibilities for information security within its remit. Its implementation must be reviewed independently to provide assurance that organisational practices properly reflect the policy, and that it is feasible and effective.

Such a review may be carried out by an internal audit function, an independent manager or a third party organisation specialising in such reviews, where these candidates have the appropriate skills and experience.

4.2 Security of third party access

Objective: To maintain the security of information processing facilities and information assets accessed by third parties.

4.2.1 Identification of risks from third party access

Access to Horizon information processing facilities must be controlled. There must be a demonstrable need for third party access. A risk assessment must be carried out to determine the security implications and control requirements for any forms of physical and electronic access by third parties. In particular, this policy is based on risk assessments that assume that:

- Any third party access to transaction data must be "read-only" and must not breach the confidentiality requirements of this policy.
- Transactions initiated at a Branch Terminal must have a corresponding application process in Horizon and must not use Horizon only as a communications path to business applications operated by third parties. As a minimum, the application must address audit trail and financial reconciliation (see §12.3).

Any variations from these assumptions must be carefully explored in the risk assessment. Additional controls to address any risks arising from the assessment must be documented and agreed with Post Office Information Security.

Third party access to systems shall also mean any form of electronic access to Horizon systems or services from outside the Horizon estate and data centres without limitation and it must be taken to include all members of all suppliers and all Post Office users other than authorized branch staff.

On-site contractors

On-site third parties must be identified and documented. A risk assessment must be conducted wherever any on-site third party services are proposed[2].

[2] Examples are hardware/software maintenance and support staff, cleaning, security guards and other outsourced support services, consultants.

POL00394583

All security requirements resulting from third party access or internal controls must be reflected in the third party contract. Where there is a special need for confidentiality of the information, non-disclosure agreements must be used.

Access to information and information processing facilities by third parties must not be provided until the appropriate controls have been implemented and a contract has been signed defining the terms for the connection or access.

4.2.2 Security requirements in third party contracts

If third parties are to be provided with access to Horizon systems there must be a formal contract containing, or referring to, all the security requirements to ensure compliance with this policy. The contract must ensure that there is no misunderstanding between the domain and the third party. See ISO 17799 §4.2.2 for a checklist list of security-relevant terms.

For all information systems developed and implemented for and on behalf of Royal Mail Group and Post Office Ltd, by their internal suppler, the group standard *Logical Access Control* (S6) must be applied.

4.3 Outsourcing

Objective: To maintain the security of information when the responsibility for information processing has been outsourced to another organisation.

4.1.1 Security requirements in outsourcing contracts

Where any outsourcing of aspects of Horizon takes place, the security requirements defined in this policy must be addressed in the contract between the parties, including:

a) How legal requirements are to be met, e.g. data protection legislation (see §12.1).

b) What arrangements will be in place to ensure that all parties involved in the outsourcing, including subcontractors, are aware of their security responsibilities (see §6.2).

c) How the integrity and confidentiality of the Post Office Ltd.'s business assets (including data) are to be maintained and tested.

d) Segregation between Post Office Ltd components and any other systems operated or managed by the contractor, e.g. on behalf of Post Office Ltd competitors (see also §8.1 and §8.5.1 concerning the separation of development, test and live operations).

e) How security incidents are to be reported and escalated (where necessary) (see §6.3).

f) What physical and logical controls will be used to restrict and limit the access to the Post Office Ltd.'s sensitive business information to authorised users.

g) How the availability of services is to be maintained in the event of equipment failure, communications failure or a disaster (see §8.5 and §11).

h) What levels of physical security are to be provided for outsourced equipment (see §7).

i) The right of audit (see §12.3).

The terms referenced in §4.2.2 must also be considered as part of the outsourcing contract. The contract must allow the security requirements and security procedures to be expanded in documentation to be agreed between the two parties.

POL00394583

5. Asset classification and control

5.1 Accountability for assets

Objective: To maintain appropriate protection of organisational assets

Each domain within the Horizon community must maintain an inventory of its assets. This supports the risk management process by providing a record of asset value and importance.

Each asset must be clearly identified, along with its ownership, security classification and current location. Assets identified for Horizon include:

- Information assets: databases and data files, system documentation, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements, archived information
- Software assets: application software, system software, development tools and utilities
- Physical assets: computer equipment, communications, magnetic media , other technical equipment (power supplies, air-conditioning units), furniture, accommodation
- Services: computing and communications services, general utilities.

5.2 Information security classification

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

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

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

- **CONFIDENTIAL**: Information that has been assessed to be of a sensitive nature and likely to cause damage following unauthorised disclosure. Personal data (as defined by the Data Protection Act) is classified as confidential. Personal data includes customer account numbers and any transaction data associated with them. FAD codes are sometimes used for authentication purposes and must therefore be treated as confidential. Transaction records that do not identify a person are confidential on bulk data/reports only. Transaction receipts for individual transactions do not need to be labelled as CONFIDENTIAL, since they are intended as a receipt for a transaction by an individual.
- **STRICTLY CONFIDENTIAL**: Information meeting the classification standards of government departments, the security services, clients, or assessed to be so sensitive that unauthorised disclosure would cause acute organisational damage. PIN data and all encryption keys are interpreted as strictly confidential.

All other information must be classified as INTERNAL unless specifically authorised for release. See §12.1.3 for INTERNAL information which may need to be released under the Freedom of Information Act.

POL00394583

DN: Does the statement "All other information must be classified as INTERNAL unless specifically authorised for release" stand up under FoI?

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

There are also legal requirements concerning the release of information – see §12.1 for more information.

6. Personnel security

6.1 Security in job definition and resourcing

Objective: To reduce the risks of human error, theft, fraud or misuse of facilities.

6.1.1 Security responsibilities in resourcing and job definition

Security responsibilities must be addressed at the recruitment stage, included in contracts, and monitored during an individual's employment.

Security roles and responsibilities must be documented in individual job descriptions. The description must include any general responsibilities for implementing or maintaining security policy as well as any specific responsibilities for the protection of particular assets, or for the execution of particular security processes or activities.

6.1.2 Personnel screening policy

Potential recruits must be adequately screened, especially for sensitive roles.

Verification checks on permanent staff must be carried out at the time of job applications. For Royal Mail Group and Post Office Ltd domains, reference should be made to Royal Mail Group vetting policy (owned by Human Resources)

Where a job, either on initial appointment or on promotion, involves the person having access to sensitive information, e.g. financial information or highly confidential information, a credit check should also be conducted. For staff holding positions of considerable authority this check should be repeated periodically.

A similar screening process must be carried out for contractors and temporary staff. Where these staff are provided through an agency, the contract with the agency must clearly specify the agency's responsibilities for screening and the notification procedures they need to follow if screening has not been completed or if the results give cause for doubt or concern.

For Royal Mail Group and Post Office Ltd domains, if any aspect of Horizon is classified as Strictly Confidential, it may be necessary to carry out the National Security vetting procedures as per the Royal Mail Group's Vetting Policy. The Head of Security for Post Office Ltd. must be consulted before such vetting procedures are invoked.

POL00394583

6.1.3 Confidentiality agreements

All users of Horizon facilities must sign a confidentiality (non-disclosure) agreement emphasizing their security responsibilities either as part of their contract of employment or as a separate agreement. Employees must sign such an agreement as part of their initial terms and conditions of employment.

Casual staff and third party users not already covered by an existing contract (containing the confidentiality agreement) must be required to sign a confidentiality agreement.

Confidentiality agreements should be reviewed when there are changes to terms of employment or contract, particularly when employees are due to leave the organisation or contracts are due to end.

6.1.4 Terms and conditions of employment

Although terms and conditions of employment are likely to be different in each domain, employees must be aware of their responsibilities in respect of information security and protecting organisational assets.

6.2 Information security training and awareness

Objective: To ensure that users are aware of information security threats and concerns and are equipped to support organisational security policy in the course of their normal work.

All staff including employees, contract staff and third party personnel must receive training and regular updates on policies and procedures. This includes security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities e.g. log-on procedures, use of software packages, before access to information or services is granted.

For the Royal Mail Group and Post Office Ltd. domains, all employees must be aware of the contents of the *e-Handbook* on the Information Security Intranet site and undertake the Information Security user-awareness training module, when available. System owners must be aware of the contents of the *System Owners Manual* on the Information Security intranet site.

Information Security training and awareness must be made available to Branch staff as a mandatory specific subject area within any Horizon training facility.

6.3 Responding to security incidents and malfunctions

Objective: To minimise the damage from security incidents and malfunctions, and to monitor and learn from such incidents.

6.3.1 Interaction between domains

When domains interact with each other, there is always a possibility that a security incident in one domain will have an adverse impact on another domain. The impact may extend to businesses that have no direct contractual agreement with the domain(s) suffering the

POL00394583

security incident and must therefore be reported to Post Office Ltd for onward communication.

6.3.2 Reporting security incidents

Security incidents must be reported through appropriate management channels as quickly as possible. See also §4.1.2 and §8.1.7.

6.4 Disciplinary process

Each of the Horizon domains must have their own disciplinary processes to manage security violations of policy and procedure. At a minimum the disciplinary process acts as an effective deterrent to employees who might otherwise be inclined to disregard security procedures.

The process must also ensure correct, fair treatment for employees who are suspected of committing serious or persistent breaches of security.

7. Physical and environmental security

7.1 Secure areas

Objective: To prevent unauthorised access, damage and interference to business premises and information.

Central Facilities

Horizon data centres and any location hosting other Horizon infrastructure facilities must be protected by at least two layers of physical security:

- An outer *Security Perimeter* that restricts access by the general public.
- An inner *Secure Area* that applies additional restrictions and which must be located within a Security Perimeter.

Horizon information processing facilities must be housed in secure areas, protected by a defined Security Perimeter, with appropriate security barriers and entry controls. They must be physically protected from unauthorised access, damage and interference. The protection provided must be commensurate with the identified risks. A clear desk and clear screen policy is recommended to reduce the risk of unauthorised access or damage to papers, media and information processing facilities.

Secure Areas must be used for housing all processing, storage and networking equipment and all network termination points used by the Horizon service. Secure areas must also be used to house key management facilities and master consoles (i.e., interactive devices providing a command interface to the operating system without having identification and authentication of the operator).

Users of shared information processing facilities must not be located in the same secure area as the information processing facility. They may be located within the same Security Perimeter.

Domains are referred to ISO 17799 for specific controls covering:

POL00394583

- Physical security perimeter
- Physical entry controls
- Securing offices, rooms and facilities.
- Working in secure areas
- Isolated delivery and loading areas.

Branch Facilities

- Horizon facilities located in branches must be considered to be in an insecure area. Facilities located behind the screen designed to protect branch staff and valuables may be considered to be secure from general public access but still require controls to protect against unauthorised access by Branch Staff. See also the policy on siting of branch equipment in §7.2.

7.2 Equipment security

Objective: To prevent loss, damage or compromise of assets and interruption to business activities.

General Policy on Equipment Security

Equipment must be physically protected from security threats and environmental hazards. Protection of equipment is necessary to reduce the risk of unauthorised access to data and to protect against loss or damage. This must also consider equipment siting and disposal. Special controls may be required to protect against hazards or unauthorised access, and to safeguard supporting facilities, such as the electrical supply and cabling infrastructure.

Domains are referred to ISO 17799 for specific controls covering:

- Equipment siting and protection (Also see the branch policy below)
- Power supplies
- Cabling security
- Equipment maintenance
- Security of equipment off-premises
    i) For the Royal Mail Group domain, all movement of equipment by Royal Mail Group staff and third parties must be controlled by effective measures commensurate with the value of the equipment and sensitivity of the data it might contain.
    ii) For Royal Mail Group owned assets on customer/supplier sites, the Mobile Security Policy (S5) and the Mobile Security Guidelines must be observed. Post Office Ltd. reserves the right to examine the suitability of all third party sites. See §8.7 for specific controls for Branch Terminals
- Secure disposal or re-use of equipment (including Branch equipment)
    i) For all domains, reuse of devices or media containing plain text PINs, keys or any data that could lead to their exposure must be controlled as required by ISO9564 and ISO 11568.

POL00394583

ii) Storage devices containing operational business data or other sensitive information must be physically destroyed or securely overwritten rather than using the standard delete function. All items of equipment containing storage media, e.g. fixed hard disks, should be checked to ensure that any sensitive data and licensed software have been removed or overwritten prior to disposal. Damaged storage devices containing sensitive data may require a risk assessment to determine if the items should be destroyed, repaired or discarded.

iii) For the Royal Mail Group domain, Disposal Policy (V4.dc) must be observed. Storage media must not be incinerated, due to the toxicity of the fumes released into the atmosphere. Re-use of storage devices that contain sensitive information must be preceded by secure deletion and overwriting. Advice can be obtained from Royal Mail Group Information Security on secure deletion.

Branch Policy on Equipment Siting & Protection

For Horizon equipment located in Branches, the following additional policy statements apply:

a) All Counter clerk operated equipment e.g. Branch Terminal equipment, printers, smart card or magnetic stripe readers etc, whether in a secure or open area, must be sited such that information and data is visible only by authorised operators. This represents no change in Post Office practice or policies for existing secure screened locations but must be addressed in any open offices or mobile installations.

b) All Branch Terminals must have a facility to quickly and simply suspend operation of the terminal e.g. in the event a clerk has to leave it momentarily. Operation must only resume once the operator has been re-authenticated or another operator is authenticated in accordance with the access control policy.

c) PIN pads must be sited such that the cardholder can prevent anyone from observing the PIN value as it is being entered. The installation must take account of any video surveillance cameras so that PIN entry cannot be observed and/or recorded. See the APACS Chip & PIN Recommendation No. 12 for further advice on assuring cardholder privacy at the counter. This represents no change in Post Office practice or policies for existing secure screened locations but must be addressed in any open offices or mobile installations.

d) The configuration of Branch Terminals must be strictly controlled such that branch staff are unable to alter the configuration or run applications other than those specifically authorized as part of the Horizon service.

e) Consideration must be given to the siting and protection of branch networking facilities, including WAN termination points, especially where such facilities are not located behind a secure screen. Where there is a significant risk arising form unauthorised access by the public or by Branch Staff, the facilities must be physically protected.

f) Consideration must be given to the security of Branch Terminal cables and ports so as to minimise the opportunity to intercept or capture clear text data passing through or between terminal components or ports.

7.3 General controls

Objective: To prevent compromise or theft of information and information processing facilities.

7.3.1 Clear desk and clear screen policy

Individual domains are also referred to the corresponding section of ISO 17799.

POL00394583

All domains must recognise the information security classifications of this policy (see §5.2).

All Post Office Ltd. employees must always observe the Post Office Ltd. Clear Desk Policy. On Post Office Ltd premises, all suppliers, contractors and third parties must observe The Post Office Ltd. *Clear Desk Policy*, to reduce the risks of unauthorised access, loss of, and damage to, information during and outside normal working hours.

7.3.2 Removal of property

Equipment, information or software should not be taken off site without authorisation. Where necessary and appropriate, equipment should be logged out and logged back in when returned. Spot checks should be undertaken to detect unauthorised removal of property. Individuals should be made aware that spot checks will take place.

8. Communications and operations management

8.1 Operational procedures and responsibilities

Objective: To ensure the correct and secure operation of information processing facilities.

Responsibilities and procedures for the management and operation of all information processing facilities must be established. This includes the development of appropriate operating instructions and incident response procedures. Segregation of duties must be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse.

Domain suppliers are referred to specific controls recommended in the corresponding section of ISO 17799, subject to the specific provisions, interpretations and highlights below.

8.1.1 Documented operating procedures

The operating procedures identified by the security policy must be documented and maintained. Operating procedures must be treated as formal documents and changes authorized by management.

Documented procedures must also be prepared for system housekeeping activities associated with information processing and communication facilities, such as computer start-up and close-down procedures, back-up, equipment maintenance, computer room and mail handling, management and safety.

8.1.2 Operational change control

Changes to information processing facilities and systems must be controlled. Inadequate control of changes to information processing facilities and systems is a common cause of system or security failures. Formal management responsibilities and procedures must be in place to ensure satisfactory control of all changes to equipment, software or procedures.

Operational programs must be subject to strict change control. When programs are changed, an audit log containing all relevant information must be retained. Changes to the operational environment can impact on applications. Wherever practicable, operational and

POL00394583

application change control procedures should be integrated (see also §10.5.1). In particular, the following controls must be implemented:

a) identification and recording of significant changes;

b) assessment of the potential impact of such changes;

c) formal approval procedure for proposed changes, including agreement with Post Office Ltd;

d) communication of change details to all relevant persons;

e) procedures identifying responsibilities for aborting and recovering from unsuccessful changes.

8.1.3 Incident management procedures

Procedures must exist to cover all potential types of security incident affecting

- Confidentiality
- Integrity, including errors resulting from incomplete or inaccurate business data
- Availability, including information system failures and loss of service, denial of service.

Each domain must establish a formal reporting procedure, together with an incident response process, setting out the action to be taken on receipt of an incident report. All suppliers, employees and contractors must be made aware of the procedure for reporting security incidents, and should be required to report such incidents as quickly as possible.

Suitable feedback processes must be implemented to ensure that those reporting incidents are notified of results after the incident has been dealt with and closed.

An escalation process must be established to ensure that incidents are managed across the Horizon community.

Security breaches and incidents must be reviewed regularly by the Information Security Management Forum to establish cross-community awareness.

Escalation procedures to the Royal Mail Group Crisis Management organisation must be put in place.

Security incidents must be assessed for their likely impact on other parties involved in the Horizon service. Serious incidents must be reported to Post Office Ltd. at the earliest opportunity. A summary of other incidents must be reported to Post Office Ltd. as part of the regular service review.

Each domain must take responsibility for reporting, investigating and resolving security incidents within its own domains that present an actual or potential threat to the Horizon environment or to any of the Horizon participants.

8.1.4 Segregation of duties

Segregation of duties is a method for reducing the risk of accidental or deliberate system misuse. Separating the management or execution of certain duties or areas of responsibility, in order to reduce opportunities for unauthorized modification or misuse of information or services, must be considered – see also §8.5.1.

Care must be taken that no single person can perpetrate fraud in areas of single responsibility without being detected. The initiation of an event should be separated from its authorization. The following controls should be considered.

POL00394583

a) It is important to segregate activities which require collusion in order to defraud, e.g. raising a purchase order and verifying that the goods have been received.

b) If there is a danger of collusion, then controls need to be devised so that two or more people need to be involved, thereby lowering the possibility of conspiracy.

c) The principle of dual control and split responsibility must be applied to the management of all cryptographic keys that directly or indirectly protect banking PINs – see ISO 11568.

8.1.5 Separation of development, test and operational facilities

Development, test and operational facilities must be separated to achieve segregation of the roles involved and to protect the security of the operational system and its data (also see §8.5.1(j)). Rules for the transfer of software from development to operational status must be defined and documented.

8.1.6 External facilities management

The risks should be identified in advance, and appropriate controls agreed with the domain operator and incorporated into the contract (see also §4.2.2 and §4.3 for the policy on third party contracts involving access to organizational facilities and outsourcing contracts).

8.1.7 Inter-domain facilites management

Any risks associated with the interoperability of Horizon domains must be identified in advance through a risk assessment. Appropriate controls must be agreed by all parties and incorporated into the partnership contracts.

Issues that must be addressed are:

(a) Business continuity

(b) Security standards to be specified and the process for measuring compliance

(c) Allocation of specific responsibilities and procedures to effectively monitor all relevant security activities

(d) Responsibilities and procedures for reporting and handling security incidents

8.2 System planning and acceptance

Objective: To minimise the risk of systems failures.

Advance planning and preparation are required to ensure the availability of adequate capacity and resources. Projections of future capacity requirements must be made, to reduce the risk of system overload.

Domains are referred to ISO 17799 for specific controls covering:

- Capacity planning
- System acceptance.

POL00394583

8.3 Protection against malicious software

Objective: To protect the integrity of software and information.

All hosts and terminals carrying Operational Business data must be protected against malware[3] attacks. Such protection must be commensurate with the risk.

Domain suppliers are referred to the corresponding section of ISO 17799 for appropriate controls. Specifically:

(a) Precautionary measures must prevent and detect the introduction of malicious software. In particular, it is essential that precautions be taken to detect and prevent computer viruses on personal computers and servers using related technology.

(b) The use of software that has not been authorised for use in Horizon systems must not be permitted.

(c) Detection and prevention controls to protect against malicious software and appropriate user awareness procedures must be implemented where appropriate.

(d) Anti-virus detection and repair software must be installed on platforms where there is a significant risk of virus attack. It must be operated and regularly updated. Appropriate procedures and responsibilities must be in place to manage virus protection, training in its use, reporting and recovery from virus attacks.

(e) Communications processes must be in place to verify all information relating to malicious software and to ensure that warning bulletins are accurate and informative.

For the Royal Mail Group domain, the Royal Mail Group Anti-Virus Policy (T3) must be observed.

8.4 Housekeeping

Objective: To maintain the integrity and availability of information processing and communication services.

8.4.1 Information back-up

Back-up copies of essential business information and software must be taken regularly. Adequate back-up facilities must be provided to ensure that all essential business information and software can be recovered following loss or corruption due to, for example, a disaster, malicious attack, equipment failure or media failure. Back-up arrangements for individual domains must be regularly tested to ensure that they meet the requirements of business continuity plans (see §11).

Domain suppliers are referred to the corresponding section of ISO 17799 for specific controls.

Restoration following a failure must be in accordance with the change control procedures – see §10.5.

[3] Malware includes viruses, trojan horses, worms and other malicious attempts to introduce unintended functionality into Horizon.

POL00394583

The retention periods for essential data and information must be determined in order to fulfil all Legal requirements and meet the retention schedule expressed for Royal Mail Group.

8.4.2 Operator logs

Log records documenting access to systems, resources, or selected functions must be retained to ensure they are available for review or use during the investigation of unauthorised access – see §12.3. Operational and support staff must maintain activity logs, these should include:

a) System starting and finishing times

b) System errors and corrective action taken

c) Confirmation of the correct handling of data files and computer output

d) The identity of the person making the log entry

Operator logs should be subject to regular, independent checks against operating procedures – see §12.2.

8.4.3 Fault logging

There must be a process for reporting and handling faults and ensuring that corrective action has been taken.

There must be a subsequent process to ensure that fault logs are reviewed and that faults have been satisfactorily resolved.

8.5 Network management

Objective: To ensure the safeguarding of information in networks and the protection of the supporting infrastructure.

Domain suppliers are referred to the corresponding section of ISO 17799, which is subject to the specific provisions, interpretations and highlights below.

8.5.1 Network controls

Operational responsibility for networks should be separated from computer operations. Network managers must implement controls to ensure the security of data in networks, and the protection of connected services from unauthorized access. In particular:

(a) The Horizon network configuration must permit traffic to flow between clearly defined security boundaries only as specifically required for Horizon applications and their associated management.

(b) Unauthorised access from non-Horizon systems and networks must be prevented, including unauthorised access from:

- any public networks used,
- networks connecting to Third Parties,
- networks connecting Horizon to Post Office Ltd and/or Royal Mail Group,
- other systems operated by the domain supplier on behalf of itself or other clients and

POL00394583

- Unauthorised access via the Branch LAN

(c) Controls must protect against denial-of-service attacks originating from non-Horizon systems including those listed in (b).

(d) The type and location of network security controls addressing points (a), (b) and (c) must reflect both the likelihood of breach via a particular network connection and the likely impact of any successful breach on the overall security of the Horizon service.

(e) Network management staff within each domain must be alerted to any attempt to reach the Horizon systems in their domain from unauthorised network addresses. Individual attempts must be treated as a minor security breach. A concerted attempt or a successful breach of network security controls must be treated as a major security breach.

(f) A domain supplier may wish to disconnect a link in a security emergency. Any such enforced disconnection facilities must be agreed with Post Office Ltd. and documented in an Operational Level Agreement with the Post Office.

(g) WAN connections must be encrypted unless specifically agreed in writing by Post Office Information Security. Encryption key management must be independent of network configuration such that the confidentiality of Post Office Ltd traffic is not compromised by a single configuration error of either the WAN or the encryption system.

(h) Back-up network facilities should be provided to protect any single network communications, equipment, or configuration failure. They must be provided where such a failure would have a significant impact on the ability of Post Office Ltd to transact business.

(i) Any backup or alternate network must be secured to the same level as the primary network.

(j) Test systems must only share network connections with operational systems in carefully controlled circumstances. Test systems must only be configured to connect in this manner for the minimum duration necessary to support testing and must be logically separated from connections carrying live data. The connection must only be permitted after an assessment has confirmed that live operation will not be adversely impacted.

(k) The use of wireless technologies within or associated with Horizon systems or services must be excluded with the exception of public telecommunications services provided by UK licensed public telecommunications operators or as otherwise agreed by Post Office Ltd. in response to a security risk assessment.

8.6 Media handling and security

Objective: To prevent damage to assets and interruptions to business activities.

Domain suppliers are referred to the corresponding section of ISO 17799, which is subject to the specific provisions, interpretations and highlights below. For information, the topics covered in this section of ISO 17799 are:

- Management of removable computer media
- Disposal of media
- Information handling procedures
- Security of system documentation

POL00394583

All removable computer media, such as tapes, disks, cassettes and printed reports must be managed to ensure that essential information is not lost or disclosed in an unauthorised manner (§7.2).

8.7 Exchanges of information and software

Objective: To prevent loss, modification or misuse of information exchanged between organisations.

Domain suppliers are referred to the corresponding section of ISO 17799. The topics covered in this section of ISO 17799 are:

- Information and software exchange agreements
- Security of media in transit
- Electronic commerce security
- Security of electronic mail
- Security of electronic office systems
- Publicly available systems
- Other forms of information exchange.

The following specific provisions apply:

a) The source of any data that is intended to result in the movement of funds must be cryptographically authenticated unless a risk assessment identifies that there is a negligible residual risk to Post Office Ltd after taking into account any other countermeasures or related business processes that are implemented.

b) Horizon must be protected against stolen or cloned Branch Terminals (i.e. an appropriately configured PC running an unauthorised copy of the Horizon application software). The protection mechanism must not be solely reliant on the username and password entered by Branch Staff (or any other individual attending the Branch other than maintenance staff using one-time passwords or other dynamic authentication techniques).

c) Any Sensitive Personal Data (as defined by the Data Protection Act 1998 – see 12.1.4) must only be transmitted across any network, internal or external, in encrypted form. Consideration must be given to the encryption of other personal data (as defined by the Act) prior to transmission over public networks. Any other data that is considered to be sensitive (including passwords and any data identified as Strictly Confidential - see 5.2) must be transmitted across any network, internal or external, only in encrypted form, unless a risk assessment identifies that there is a low residual risk to Post Office Ltd.

d) All Horizon domains are likely to use electronic systems other than those directly concerned with Horizon. Each domain (including Post Office Ltd.) must ensure that Post Office Ltd. data stored on such systems is secure. Clear segregation must be maintained between Horizon and non-Horizon systems.

e) Live Horizon data must not be used for test or debug purposes unless specifically authorised by Post Office Ltd and then only once it has been "sanitised".

f) All Horizon domains must have appropriate measures in place to ensure that their public facing connections or customer access points are configured to ensure total separation from internal systems that contain Horizon data.

g) Any access by a third party must be evaluated case by case on the basis of need and a risk assessment.

POL00394583

h) Any messaging application (e.g. e-mail) used to communicate with branch staff via Horizon must be configured such that it cannot be used to attack the integrity or availability of any Horizon system including those in the branches and the data centres.

i) If any other systems are used, data on them must be secured.

9. Access control

Objective: To control access to Horizon resources.

Domain controllers are referred to the corresponding section of ISO 17799, which is subject to the specific provisions, interpretations and highlights below. The topics covered in this section of ISO 17799 are:

- Policy and business requirements
- Access control policy
- User access management
- User responsibilities
- Network access control
- Operating system access control
- Application access control
- Monitoring system access and use
- Mobile computing and teleworking.

General Requirements

Control of access to all Post Office Ltd systems interfacing with Horizon must be in accordance with the Royal Mail Group Logical Access Control Policy (S6).

Each Horizon domain must have its own Access Control Policy. This Access Control Policy defines the policy for controlling access to resources involved in Horizon in line with the overall objectives specified in this policy.

The policy must take account of the following:

(a) Security requirements of Horizon applications

(b) Identification of all information related to Horizon applications

(c) Policies for information dissemination and authorisation, e.g. the need to know principle and security levels and classification of information

(d) Relevant legislation and any contractual obligations regarding protection of access to data or services

(e) Standard user access profiles for common categories of job

(f) Management of access rights in a distributed and networked environment, which recognises all types of connections available.

Wherever technically possible, a process must be in place for authorizing user access to Horizon systems. When a user leaves his/her company, goes on leave of absence and is not expected to return to regular employment, or no longer has a valid business need, the user's manager must promptly notify the relevant UserId administrator(s). The Userid

POL00394583

administrator(s) must have a process or technical controls in place to prevent the user's access to the system(s) immediately following the manager's notification.

UserIds and passwords must not be shared, unless in very specific circumstances for which a specific exception would need to be agreed with Post Office Ltd Information Security. In the exceptional circumstances of a shared userid or password, an audit trail must be available to enable a specific individual's access to be determined for Royal Mail Group staff.

Passwords must not be transmitted in plain text over any Horizon network.

The Mobile Security Policy (S5) and the Mobile Security Guidelines must be observed for security of laptops allocated to or used by Post Office staff.

Horizon Branch Terminal - Specific Requirements

a) All users of Branch Terminals must be identified and authenticated before using the Branch Terminal. Each identity must be capable of being traced to a specific individual such that each individual can be held accountable for their actions.

b) Permission to access Horizon data and functionality must be based on roles that reflect the duties of staff accessing the system. Branch Terminal users must only be allocated permissions based on being allocated to such a role and not based on their individual identity.

c) Branch Clerical Staff must only have access to Horizon business application(s); they must not have access to any operating system level functionality or to any utilities that could be used to modify or attack the system.

d) A role must be provided such that authorized branch staff (e.g. the Postmaster) can be made responsible for administering all stages in the life-cycle of Branch Clerical Staff, from the initial registration of new users to the final de-registration of users who no longer require access to Horizon.

10. Systems Development and Maintenance

10.1 Security Requirements of Systems

Objective: To ensure that security is built into Information Systems

10.1.1 Security Requirements Analysis and specification

All security requirements must be identified, justified, agreed and documented as part of the overall business case.

The security controls must be specified within the statements of business requirements for Horizon and enhancements, both the need for automated and manual controls must be specified.

Security controls must reflect:

- the business value of the information assets involved
- the potential business damage
- Security requirements and controls should be identified from risk assessment. Within the Post Office domain[4]:

POL00394583

- a Business Impact Assessment must be conducted at the feasibility stage of a development project, and
- a Security Risk Assessment must be conducted at the Conceptual Design stage of project development.

The following must be considered during the analysis:

- identification and authentication of human and system "users"
- control of access to information and services
- segregation of duties
- secure operation in degraded mode
- incorporation and analysis of audit trails
- data and system integrity protection
- use of encryption to prevent unauthorised disclosure of data
- system resilience, including operation in fall-back mode and recovery.

10.2 Security in Application Systems

Objective: To prevent loss, modification or misuse of user data in application systems.

Domain suppliers are referred to the corresponding section of ISO 17799. The topics covered in this section of ISO 17799 are:

- Input data validation
- Control of internal processing
- Message authentication
- Output data validation.

In particular:

a) Where Horizon business applications are implemented using Java, the domain supplier must define a Java security model for approval of Post Office Ltd.

b) Any ActiveX or Java applets must be signed or otherwise verified before the Terminal operating system allows their installation.

c) Applications requiring passwords must comply with the password policy shown on the right unless otherwise approved by Post Office Ltd Information Security.

d) The security of data, especially business data, transaction data, sensitive data (see §5.2) and audit data (see §12.3), must be maintained in accordance with this policy during any migration from a live Horizon system or component to a new or replacement one.

Password Policy

a) Where passwords are used for authentication, the user must be forced to change the initial password before any other access to the system is permitted.

b) Passwords must expire in 30 days.

c) Re-use of the same password must not be permitted for either a specified time or until at least 3 other passwords have been used.

d) Passwords must be a minimum of 6 characters long and must be alphanumeric (i.e. a mix of letters and numbers). There must not be more than two consecutive identical characters. The password must not be the same as the username.

e) After 3 consecutive unsuccessful attempts to log-on, the user must be locked out.

[4] See Harmony (for PRISM projects) and JWISL (for Fujitsu Services projects).

POL00394583

10.3 Cryptographic Controls

Objective: To protect the confidentiality, authenticity and integrity of information.

Horizon must operate within the framework of the Royal Mail Group Cryptographic policy and follow the recognised financial industry guidelines on cryptography which includes:

- Encryption
- Digital Signatures
- Non-repudiation services
- Key Management
- Security of system files.

Cryptographic systems and techniques must be used for the protection of information that is considered at risk and for which other controls do not provide adequate protection.

Unless otherwise agreed with Post Office Ltd, cryptographic controls must be used as follows:

(a) Once entered by a cardholder, plain text PINs must only be processed in a physically secure device as defined in ISO 9564. At all other times, PINs must be encrypted as defined in ISO 9564.

(b) Any cryptographic key knowledge of which could directly or indirectly reveal plain text PINs must be managed in accordance with ISO 11568 Parts 1 to 3.

(c) Unless point (d) applies, Banking MACs must be used to authenticate the source of all messages or files that may result in the transfer of funds.

(d) Banking MACs may be omitted where there is a cryptographically authenticated circuit (e.g. a VPN) between the source and destination of the payment data. The encryptor must be located within the physical security of the data centre hosting the payment application.

(e) Any link carrying information classified as "confidential" in clause §5.2 must be encrypted outside the physical security of a data centre unless agreed in writing by Post Office Ltd Information Security and, for personal data, the Data Controller. See also §8.5.1.

(f) Government specified algorithms and key lengths must be used where specifically required by HM Government. Post Office Ltd. must ensure that the contract with domain suppliers contains or references any such HM Government requirements.

(g) Subject to (f), industry standard commercial algorithms and protocols should be used. Cryptographic key lengths for commercial algorithms must be at least 112 bits for symmetric keys and at least 1024 bits for public keys. Triple-DES (ANSI X9.52) is the only approved symmetric algorithm for protecting banking PINs (see ISO 9564).

(h) Encrypted traffic must only pass through firewalls where it is agreed with Post Office Ltd. Information Security that it does not represent a significant threat to the security of Horizon – See §8.5.1. Selectively encrypted fields such as PINs, passwords and cryptographic key management fields are not considered such a threat.

POL00394583

10.4 Security of system files

Objective: To ensure that IT projects and support activities are conducted in a secure manner.

Domain suppliers are referred to the corresponding section of ISO 17799. The topics covered in this section of ISO 17799 are:

- Control of operational software
- Protection of system test data
- Access to program source library

In particular:

a) Horizon users must not have any access to add, modify, delete or execute any operating system or application files without first being properly authorised, authenticated and audited. Controls must be in place to prevent this requirement being bypassed by any new or upgraded application or system build.

10.5 Security in development and support processes

Objective: To maintain the security of application system software and information.

Project and support environments must be strictly controlled.

Managers responsible for application systems must also be responsible for the security of the project or support environment. They must ensure that all proposed system changes are reviewed to check that they do not compromise the security of either the system or the operating environment.

10.5.1 Change control procedures

In order to minimize the corruption of information systems, there must be strict control over the implementation of changes – see §8.1.2. Formal change control procedures must be enforced. They must ensure that security and control procedures are not compromised, that support programmers are given access only to those parts of the system necessary for their work, and that formal agreement and approval for any change is obtained. Wherever practicable, application and operational change control procedures should be integrated

10.5.2 Maintenance procedures

In order to maximize the availability of the system there must be strict control over the maintenance of all operational Horizon systems:

a) Wherever practical, maintenance activities must be planned in advance and scheduled to take place at times of low traffic.

b) Where any maintenance task requires a system outage, the timing of the outage must be agreed in advance with Post Office Ltd.

c) From time to time, product and service suppliers will issue details of security vulnerabilities and recommend workarounds and / or fixes. Domain suppliers must apply recommended workarounds and fixes in a timescale commensurate with the risk to Horizon and in accordance with the change control procedures.

POL00394583

10.1.3 Further development & support policies

Domain suppliers are referred to the sections 10.5.2 to 10.5.5 inclusive of ISO 17799. The topics covered in this section of ISO 17799 are:

- Technical review of operating system changes
- Restrictions on changes to software packages
- Covert channels and Trojan code
- Outsourced software development

11. Business Continuity

Objective: To counteract interruptions to business activities and to protect Post Office Ltd. critical business processes from the effects of major failures or disasters.

Business continuity for Horizon concerns the provision of appropriate processes across the Horizon Community to develop and maintain the continuity of all Horizon business functions.

There must be a process in place, involving the Horizon community, to develop and maintain business continuity of the end-to-end Horizon service.

Similarly, individual domains must have a process in place for the development and maintenance of their own business continuity plans in support of their responsibilities for end-to-end business continuity, including integration with other Horizon domains.

Key elements of the business continuity planning process include:

- Understanding the risks, their likelihood and impact
- Understanding the impact of interruptions on Post Office Ltd. as a whole
- Formulating and documenting a business continuity strategy consistent with the agreed business objectives and priorities
- Regular testing and updating of the plans and amended processes put in place where necessary.

An end-to-end Horizon business continuity plan must define the responsibilities of and interactions between, the individual domains of the Horizon Community, and must be integrated within an overall Crisis Management framework agreed between all parties.

Individual Horizon domains must each develop and maintain business continuity plans as defined within the end-to-end plan.

All relevant security provisions must be retained even if degraded operating conditions are in effect.

End-to-end business continuity must comply with ISO 17799. Individual Horizon domains are referred to the appropriate section of ISO 17799. The topics covered in this section of ISO 17799 are:

- Business Continuity Management Process

POL00394583

- Business continuity and impact analysis
- Writing and implementing continuity plans
- Business continuity planning framework
- Testing, maintaining and re-assessing business continuity plans

12. Compliance

12.1 Compliance with legal requirements

Objective: To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements.

12.1.1 Applicable Legislation

Horizon must ensure compliance with all legislative requirements including the:

- Freedom of Information Act 2000
- Data Protection Act 1998
- Official Secrets Act 1989
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Financial Services and Markets Act 2000
- Regulation of Investigatory Powers Act 2000
- Electronic Communications Act 2000 as amended by the Communications Act 2003
- Money Laundering Regulations 2003

All Horizon domains must clearly identify compliance measures, legislation and industrial standards that surround them. Each domain must identify how compliance is going to be monitored and how often compliance checks are going to be carried out. The specific controls and individual responsibilities to meet the requirements must be defined and documented. Where appropriate, advice on specific legal requirements must be sought from the domain's legal advisers, or suitably qualified legal practitioners.

12.1.2 Intellectual property rights (IPR)

Appropriate procedures should be implemented to ensure compliance with legal restrictions on the use of material in respect of which there may be intellectual property rights, such as copyright, design rights, trade marks.

Proprietary software products are usually supplied under a licence agreement. They must only be used in accordance with any such licence. Domain suppliers must ensure that sufficient licences are available to fulfil their contractual obligations.

POL00394583

12.1.3 Safeguarding of organizational records

Important records of an organization must be protected from loss, destruction and falsification. See also §8.4.1 and §11.

12.1.4 Data protection and privacy of personal information

Account identifiers, such as the PAN in a banking transaction, can be considered to identify an individual in the context of the Data Protection Act 1998[5]. The body responsible for maintaining the account is deemed to be the Data Controller as defined by the Act. For instance, Alliance & Leicester is the Data Controller for personal data relating to transactions involving cards it has issued. Similarly, other Horizon transactions containing an account identifier, or other data capable of identifying an individual, may have a Data Controller who is a Third Party in the context of Horizon. Where Post Office Ltd is not the Data Controller it must ensure it has the authority to delegate Data Processing to a domain. All other Horizon domains are a Data Processor as defined by the Act and must only process personal data for the purposes specified in the relevant Horizon contract and associated specifications.

Any data associated with an account identifier must be treated as personal data as defined by the Act. Any person claiming to be the data subject and requesting access to the personal data must be referred to the organisation responsible for the account as the body capable of authenticating the request. Any other requests for access to the personal data, other than by authorised Post Office staff, must be declined unless supported by a duly authorised legal warrant.

The Data Protection Act also identifies certain personal data as Sensitive Personal Data[6]. The relevant Data Controller is responsible for identifying such data as Sensitive Personal Data and must inform those responsible for implementing the Horizon system so that appropriate additional security measures can be taken – see 8.7c).

Post Office Ltd. must develop a policy covering the handling of Freedom of Information requests by customers for third party services delivered over the Counter. The Freedom of Information Act does not permit the release of personal data covered by the Data Protection Act.

DN: For Post Office internal information, Martin Rush is the temporary RMG FoI contact at the time of writing.

12.1.5 Prevention of misuse of information processing facilities

The Horizon facilities are provided strictly for business purposes. Any use of these facilities for non-business or other purposes not associated with Horizon, will be regarded as improper use of the facilities. If such activity is identified by monitoring or other means, it must be brought to the attention of the individual manager concerned for appropriate disciplinary action (see §6.4). The security incident reporting procedures (see §6.3.2) must be used where one domain detects misuse by staff of another domain.

---

[5] See the advice concerning the scope of the definition of personal data in the guidelines issued by the Information Commissioner.

[6] In particular, see Section 3.1.2 of "Data Protection Act 1998: Legal Guidance" issued by the Information Commissioner, and available from http://www.informationcommissioner.gov.uk

POL00394583

12.1.6 Regulation of cryptographic controls

Some countries have implemented agreements, laws, regulations or other instruments to control the access to or use of cryptographic controls. Such control may include:

a) import and/or export of computer hardware and software for performing cryptographic functions;

b) import and/or export of computer hardware and software which is designed to have cryptographic functions added to it;

c) mandatory or discretionary methods of access by the countries to information encrypted by hardware or software to provide confidentiality of content.

Before encrypted information or cryptographic controls are moved to another country, legal advice should be taken.

Legal advice should also be sought to ensure compliance with the Regulation of Investigatory Powers Act 2000. Note that PINs are an authentication mechanism as defined by the act and thus the act does not apply to PINs or the keys used to protect them.

12.1.7 Collection of evidence

It is necessary to have adequate evidence to support an action against a person or organization. Whenever this action is an internal disciplinary matter the evidence necessary will be described by internal procedures.

Where the action involves the law, either civil or criminal, the evidence presented must conform to the rules for evidence laid down in the relevant law or in the rules of the specific court in which the case will be heard.

To achieve admissibility of the evidence, domains must ensure that their information systems comply with any published standard or code of practice for the production of admissible evidence.

To achieve quality and completeness of the evidence, a strong evidence trail must be maintained.

Post Office Ltd will agree the level of support it requires from domains in cases it prosecutes.

12.2 Reviews of security policy and technical compliance

Objective: To ensure compliance of systems with relevant security policies and standards.

The security of information systems must be regularly reviewed. Such reviews must be performed against the Horizon security policy and any other applicable security policies, and the technical platforms and information systems must be audited for compliance.

LINK requires an annual statement of compliance with the LINK Information Security Standard. Post Office Ltd must produce and submit the statement. Domains must co-operate with Post Office Ltd in the preparation of the statement.

POL00394583

12.3 System Audit Considerations

Post Office Ltd retains the right to review activity records of all Horizon domains for any evidence of authority misuse or other failure to comply with this policy and associated procedures.

Audit requirements and activities must be planned to minimise the risk of disruption to Horizon.

An audit trail of all transactions and events (including failed ones) must be maintained. Transactions which are abandoned prior to submission to the Data Centre only need an audit record where there is a reasonable customer expectation that the transaction might proceed[7].

As a minimum, the audit trail for transactions must be able to identify at least the following:

a) the type of transaction,

b) the transaction result,

c) the transaction value,

d) the identity and location of the person who initiated it, and

e) the date and time at which the transaction occurred.

Transactions must be uniquely identified in the audit trail. Transactions must be traceable from end to end i.e. from the receipt produced for the customer at the Branch Terminal to the point at which they cross the Horizon boundary.

The audit trail must be maintained securely for a period agreed contractually with Post Office Ltd. The audit trail may be archived after an agreed period. It must be possible to extract relevant audit data, including archived audit data, such that it is fit for use as legal evidence in support of a prosecution. It must still be possible to extract data during the agreed period, even if the technology originally used to generate the trail has been upgraded or replaced. See §7.2 for the policy on destruction of data including audit data and any extracts thereof. See §8.4.1 for the policy on back-up of data including audit data.

Access to system audit tools must be safeguarded to prevent any possible misuse or compromise.

--- End of Policy ---

[7] Such expectation will not exist, for example, when a customer receipt clearly shows the transaction has been cancelled or prior to the PIN entry for a card-based transaction.