POL00397117

Community Information Security Policy for Horizon & Horizon Online

Author	Information Security Policy Manager	Sue Lowther
Reviewers	Post Office Fujitsu Services Prism Information Security Team IT Strategy & Architecture Manager Group Internal Audit	Dave King Adam Martin Tom Lillywhite Peter Watts David Gray Steve Webb
Sign off authority	Post Office Head of Security	John Scott
Reference configuration	POL/HNG/CIS/001	

POL00397117

Operational Baseline Number		
Version	~~1.3~~2.0	
Status	~~Draft~~Approved	
Classification	Working Document	
Date	~~29/01/2010~~28 March 2010	
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
1.1	22/05/08	Restructured to align with ISO17799:2005
1.2	05/09/2008	Update to align with ISO 27001 and incorporate changes referenced in HNG-X security requirements, v1.6 of LiNK ATM Scheme Security Standard and PCI DSS v1.1.
1.3	29/01/2010	Changes to reflect Horizon Online development and PCI DSS v1.2
2.0	22~~0~~8/03/2010	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
GRO

POL00397117

References / Related / Dependent / Parent Documents

Reference	Document Reference	Title	Version	Date
	ISO/IEC 27001:2005	Information technology – Security Techniques – Information Security Management Systems – Requirements.		
	ISO/IEC 27002:2005	Information technology – Code of practice for information security management, (also known as ISO/IEC 17799:2005).		
	ISO / IEC 27005:2008	Information technology -- Security techniques -- Information security risk management		
	ISO/IEC 24762:2008	Information technology – Security techniques – Guidelines for information and communications technology disaster recovery services		
	LiNK ASISS	Link ATM Scheme Information Security Standard	1.6	Dec 2006
	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		
	PCI DSS	Payment Card Industry Data Security Standard	v1.1	
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		
	G30	Freedom of Information Act policy		
	S1	Information security		

POL00397117

	S2	Investigation and Prosecution Policy		
		Royal Mail Group Human Resources – Personnel Vetting Policy		
	S3	Security Policy		
	S4	Information Classification Policy		
	S4	Information Classification Guidelines		
	S5	Mobile Security Policy		
	S6	Logical access control Policy		
	S7	Security Health Check Policy		
	S8	Wireless Connectivity Policy		
	S9	Cryptographic Services Policy		
	S10	Clear Desk Policy		
	S11	Generic Account Policy		
	S15	Incident Management Policy		
	S16	Third Party Access Policy		
	S17	Security Architecture Methodology		
	S19	Personal Computer Backup Policy		
	S20	Third Party Provisioning Policy		
	T1	IS/IT Compliance		
	V4.dc	Disposal policy		
	T3	Anti-virus policy		
Legal & Regulatory (see also §[REF _Ref206228986 \r \h])				
		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		

POL00397117

		Money Laundering Regulations 2003		

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.

POL00397117

Contents

[TOC \o "1-3" \h \z \u]

POL00397117

Terms and abbreviations

Term	Meaning
See §2	

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 Online including its migration from Horizon. This document describes for these systems:

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

ISO 17799 was updated in 2005 to align with the newly published ISO 27001. This policy was updated at version 1.1 in order to match the re-organisation of controls between ISO 17799:2000 (on which version 1.0 of this policy was based) and ISO 17799:2005[1] (and thus ISO 27001) on which this version is be based.

1.2. Readership

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

1.3. 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] ISO 17799:2005 has subsequently been renumbered ISO 27002:2005.

POL00397117

1.4. Document Review

The owner of the policy is responsible for its maintenance and review - see §[REF _Ref206412463 \r \h].

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.

Where the text requires actions to be taken "**promptly**", "**regularly**" or "**periodically**", domains should perform them in a timescale that reflects the associated security risks. Where there are contractual or regulatory requirements on Post Office to perform the actions at a specific frequency, those responsible for performing the actions must be advised in writing.

Branch staff: Those people who use an Horizon Online or Horizon Branch Terminal. They consist of clerical staff who actually transact business, administrative staff (e.g. the sub-postmaster) responsible for managing branch specific aspects of the Horizon or Horizon Online service and global users who may visit any branch (e.g. auditors and support engineers).

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

Cardholder Data Environment: A part of the Horizon Online system that possesses Cardholder Data or Sensitive Authentication Data together with those systems and segments that directly attach or support cardholder processing, storage, or transmission. Adequate network segmentation, which isolates systems that store, process, or transmit Cardholder Data from those that do not, may reduce the scope of the Cardholder Data Environment and thus the scope of the PCI DSS audit.

Cardholder Data: means the Primary Account Number (PAN) of a payment card or the PAN plus any of the following:

- cardholder name
- expiration date
- Service Code
- start date
- issue number;

Client: An organisation with which Post Office Limited contracts for the supply of

POL00397117

goods or services delivered to Customers via Horizon / Horizon Online.

Customer: An individual (or organisation) to whom goods or services are delivered via Horizon / Horizon Online.

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

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

Horizon: The information system used to capture and process business transactions originating in Post Office branches prior to its migration to Horizon Online.

Information security management system (ISMS): That part of an the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security.

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 that ensure the accountability of individuals.
- **Availability**: ensuring that authorised users have access to information and associated assets when required

PCI DSS: Payment Card Industry – Data Security Standard

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

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.

Sensitive Authentication Data: security related information used to authenticate cardholders appearing in plain text or otherwise unprotected form. This information can be any of the following:

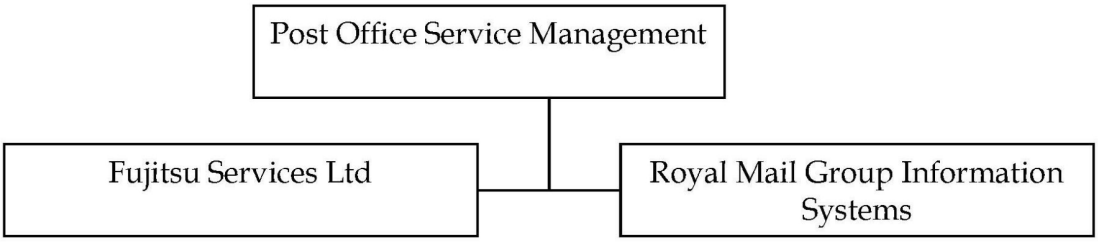
POL00397117

- The full contents of the magnetic stripe of a payment card (from the back of a card, the equivalent from a chip or elsewhere).
- The card-validation value or code (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions[2].
- The personal identification number (PIN) or the encrypted PIN block associated with a payment card.

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

- Royal Mail Group Information Systems
- 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.

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

Third party: An individual or organisation that is neither:

- A domain supplier (or one of its employees or contractors) involved in Horizon or Horizon Online service delivery, nor
- Post Office Limited (or one of its employees or contractors).

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

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

[2] Not to be confused with the similarly named field on a magnetic stripe (or its chip equivalent) that protects the integrity of the magnetic stripe data.

POL00397117

3. Structure of this document

This document follows the ISO27001:2005 categories of control. It is derived from the control objectives and controls listed in Annex A of ISO27001:2005. These objectives and controls are highlighted in shaded boxes throughout the document.

Where appropriate, the ISO27001 controls are expanded to provide a more detailed policy (based on the ISO27002:2005 Code of Practice) and/or to communicate detailed control requirements placed on Post Office Limited by its clients.

4. Risk assessment and treatment

All domains must operate a formal process of risk management (of which risk assessment and risk treatment are a part) as an integral part of an ISO/IEC 27001 compliant Information Security Management System. The process should comply with ISO/IEC 27005. See §[REF _Ref206413799 \r \h] for the role of risk assessment in identifying the security requirements in this policy.

This policy is based on a risk assessment which assumes:

- There is no access to Horizon / Horizon Online applications from the Internet.
- There is no general purpose web-surfing or e-mail facilities at branch terminals
- There is no use of wireless technologies such as Wi-Fi or Bluetooth within the Horizon / Horizon Online system boundary.[3]

5. Security 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.

5.1. Information security policy

5.1.1. 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 and Horizon Online community must individually and together maintain the appropriate level of information security necessary for the end-to-end Horizon / Horizon Online services.

[3] This does not prohibit the use of wide area networks that may use wireless technology and are operated by licensed public telecoms operators.

POL00397117

5.1.2. Objective

The Horizon Community Information Security Policy objective is to ensure that all the Horizon and Horizon Online 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 / Horizon Online 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 / Horizon Online 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
- to monitor and review information security arrangements to provide assurance that policy, standards and procedures remain relevant and effective.

Control A.5.1.1: Information Security Document

The mandatory elements of this policy set out the minimum level of security to be adopted throughout the 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.

5.1.3. ISO/IEC 27001 baseline

Royal Mail Group requires that Post Office Ltd. implements and operates an Information Security Management System (ISMS) in accordance with ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements*, together with other approved technical and procedural standards where appropriate.

Accordingly, the Horizon / Horizon Online community must apply ISO/IEC 27001 as the baseline for managing Information Security in their domain. In interpreting the controls required by ISO27001, the recommendations in ISO/IEC 27002 must be considered a statement of best practice by each domain, unless explicitly modified in

POL00397117

this document.

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 27001. Domains contracted to comply with ISO 27001 should seek formal certification to ISO 27001 in order to be able to demonstrate compliance with the contractual requirement.

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

5.2. Review and evaluation

Control A5.1.2: Review of the Information Security Policy

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.

This 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.

6. Organisation of information security

6.1. Internal organisation

Objective: To manage information security within the Horizon / Horizon Online community.

An Information Security Management System 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

POL00397117

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.

6.1.1. Management commitment to information security

Control A6.1.1: Management must actively support security within their domain through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.

Information security should be a business responsibility shared by all who have a responsibility for delivering the Horizon / Horizon Online 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 the effectiveness of the implementation of the domain's information security policy and controls.

b) approving overall security responsibilities;

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

d) reviewing and monitoring information security incidents;

e) approving major initiatives to enhance information security and information security awareness.

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 / Horizon Online service.

6.1.2. Information security co-ordination

Control A6.1.2: Information security activities must be co-ordinated by representatives from different parts of each domain with relevant roles and job functions.

Within each domain an experienced security professional must have the responsibility for coordinating security for that part of Horizon Horizon Online 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 / Horizon Online that is within the domain's remit;

POL00397117

b) agreeing specific methodologies and processes for information security within that part of Horizon / Horizon Online 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 / Horizon Online that is within the domain's remit, e.g. the security awareness programme;

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

e) reviewing Horizon /Horizon Online-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 / Horizon Online 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 / Horizon Online that is within the domain's remit.

6.1.3. Allocation of information security responsibilities

Control A6.1.3: All information security responsibilities must be clearly defined.

Responsibilities for the protection of individual assets and for carrying out specific security processes must be clearly defined and documented. Each domain must document and disseminate 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 and documented.

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.

POL00397117

6.1.4. Authorisation process for information processing facilities

Control A6.1.4: A management authorisation process for new information processing facilities shall be defined and implemented.

*The ISO/IEC 27001 control for authorisation of new information systems is not relevant to Horizon / Horizon Online as it is an existing system. See §[REF _Ref199309597 \r \h * MERGEFORMAT] re authorisations of changes to Horizon / Horizon Online.*

6.1.5. Confidentiality agreements

Control A6.1.5: Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information must be identified and regularly reviewed.

All users of Horizon / Horizon Online 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.

6.1.6. Specialist information security advice

Control A6.1.6: Appropriate contacts with relevant authorities must be maintained.

There must be a source of information security expertise within each domain. Where the expert has insufficient experience 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.

POL00397117

6.1.7. Cooperation between organisations

Control A6.1.7: Appropriate contacts with special interest groups or other specialist security forums and professional associations must be maintained.

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

6.1.8. Independent review of information security

Control A6.1.8: The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) must be reviewed independently at planned intervals, or when significant changes to the security implementation occur.

The Community Information Security Policy for Horizon & Horizon Online and all referenced technical controls will be subject to quality checks by an external qualified body and Horizon / Horizon Online 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.

6.2. External parties

Objective: To maintain the security of information processing facilities and information assets accessed, processed, communicated to or managed by third parties.

6.2.1. Identification of risks related to external parties

Control A6.2.1: The risks to the organization's information and information processing facilities from business processes involving external parties must be identified and appropriate controls implemented before granting access.

Access to Horizon / Horizon Online 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 or electronic access by third parties. In particular, this policy is based on risk assessments that assume that:

POL00397117

- 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 / Horizon Online and must not use Horizon / Horizon Online 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 §15.3).

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 / Horizon Online systems or services from outside the Horizon / Horizon Online 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.

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.

6.2.2. Addressing Security when dealing with customers

Control A6.2.2: All identified security requirements must be addressed before giving Post Office customers or clients access to Horizon / Horizon Online information or assets.

Post Office customers must not be granted remote access to Horizon / Horizon Online information or assets. Security requirements for any customer operated terminals connected to Horizon / Horizon Online must be identified and specified prior to contracting for their supply and installation.

Security requirements for clients of Post Office Limited must be addressed as specified in §[REF _Ref205721619 \r \h] and §[REF _Ref205721677 \r \h].

POL00397117

6.2.3. Addressing security in third party agreements

Control A6.2.3: Agreements with third parties involving accessing, processing, communicating or managing Post Office information or Horizon / Horizon Online information processing facilities, or adding products or services to information processing facilities must cover all relevant security requirements.

If third parties are to be provided with access to Post Office information and/or Horizon / Horizon Online 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 the corresponding section of ISO/IEC 27002 for a checklist list of security-relevant terms.

Domain suppliers should require third parties to implement an Information Security Management System compliant with ISO/IEC 27001. Where the third party has access to Cardholder Data, third parties must be required to comply with the Payment Card Industry Data Security Standard (PCI DSS) and acknowledge that they are responsible for the security of all Cardholder Data and Sensitive Authentication Data that they possess.

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 *Third Party Access Policy* (S16) must be applied.

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

a) How legal and regulatory requirements are to be met, e.g. data protection legislation (see §[REF _Ref206228986 \n \h]).

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 §[REF _Ref206229012 \n \h]).

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 §[REF _Ref199331541 \n \h], §[REF _Ref199331482 \n \h], and §[REF _Ref199224556 \n \h]).

e) How security incidents are to be reported and (where necessary) escalated (see §[REF _Ref206229086 \n \h]).

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 (see §[REF _Ref199320474 \n \h]).

POL00397117

g) How the availability of services is to be maintained in the event of equipment failure, communications failure or a disaster (see §[REF _Ref199233886 \n \h] and §[REF _Ref204169468 \n \h]).

h) What levels of physical security are to be provided for outsourced equipment (see §[REF _Ref206229156 \n \h]).

i) The processes for monitoring and reviewing security arrangements (see §[REF _Ref251946424 \r \h]).

j) The right of audit (see §[REF _Ref206229176 \n \h]).

The contract must allow the security requirements and security procedures to be expanded in documentation to be agreed between the two parties.

The following additional security requirements apply in the event that a domain supplier wishes to outsource any development work for Horizon Online offshore. The domain supplier must carry out an assessment of the potential risks involved in such work being undertaken offshore. The domain supplier must agree with Post Office Information Security details of the processes, procedures, systems and controls the developer has (or intends to put in place) to address the risks identified in the assessment prior to any such development taking place. [SEC-3270]

See also §[REF _Ref206229223 \n \h], third party service delivery management.

7. Asset classification and control

7.1. Responsibility for assets

Objective: To maintain appropriate protection of Post Office and Horizon / Horizon Online assets

7.1.1. Inventory of assets

Control A7.1.1: All assets must be clearly identified and an inventory of all important assets drawn up and maintained.

Each domain within the Horizon / Horizon Online community must maintain an inventory of its assets.[4] It must be possible to identify assets from their entry in the inventory e.g. by by clearly marking physical assets.

Assets identified for Horizon / Horizon Online include:

- Information assets: databases and data files, system documentation, user manuals, training material, operational or support procedures, continuity plans,

[4] This supports the risk management process by providing a record of asset value and importance.

POL00397117

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.

7.1.2. Ownership of assets

Control A7.1.2: All information and assets associated with information processing facilities must be 'owned' by a designated part of the organisation.

Each asset or group of assets identified in §7.1.1 must be clearly identified, along with its ownership within the domain, security classification and current location. The term ownership refers to an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. It does not mean that the person actually has property rights to the asset.

7.1.3. Acceptable use of assets

Control A7.1.3: Rules for the acceptable use of information and assets associated with information processing facilities must be identified, documented, and implemented.

*See §[REF _Ref206223802 \n \h * MERGEFORMAT] for technologies that are not currently supported under this policy. Also see §[REF _Ref206225085 \n \h * MERGEFORMAT] for the policy concerning equipment off site.*

7.2. Information security classification

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

7.2.1. Classification guidelines

Control A7.2.1: Information must be classified in terms of its value, legal requirements, sensitivity and criticality to the organization.

Horizon / Horizon Online information that is generated, processed, communicated or stored within the Horizon / Horizon Online 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

POL00397117

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. Information identifying cash handling staff, routes and/or timings is STRICTLY CONFIDENTIAL. PIN data and all encryption keys are also interpreted as STRICTLY CONFIDENTIAL.

All other information must be classified as INTERNAL unless specifically authorised for release.

There are also legal requirements concerning the release of information – see §15.1 for more information.

7.2.2. Information labelling and handling

Control A7.2.2: An appropriate set of procedures for information labelling and handling must be developed and implemented in accordance with the classification scheme adopted by the domain.

All documentation, displayed output and storage media from systems containing information classified as CONFIDENTIAL or STRICTLY CONFIDENTIAL must carry an appropriate classification label.

A chain of custody must be established for any such information and any security relevant event logged.

8. Human resources security

8.1. Security in job definition and resourcing

Objective: To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risks of human error, theft, fraud or misuse of facilities.

POL00397117

8.1.1. Roles and responsibilities

Control A8.1.1: Security roles and responsibilities of employees, contractors and third party users must be defined and documented in accordance with each domain's information security policy.

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.

8.1.2. Screening

Control A8.1.2: Background verification checks on all candidates for employment, contractors, and third party users must be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

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 Post Office business data or other sensitive information, e.g. financial information or highly confidential information, screening must include checks on identity, qualifications and financial circumstances. Criminal record checks must be performed where legally permitted [SEC-3255]. A credit check must also be conducted. For staff holding positions of considerable authority this financial and criminal record checks 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 / Horizon Online 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.

POL00397117

8.1.3. Terms and conditions of employment

Control A8.1.3: As part of their contractual obligation, employees, contractors and third party users must agree and sign the terms and conditions of their employment contract, which must state their and the domain's responsibilities for information security.

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. Also see the requirement for confidentiality agreements in §[REF _Ref206237551 \r \h] and security awareness training in §[REF _Ref206238952 \r \h].

8.2. During Employment

Objective: To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support the domain's security policy in the course of their normal work, and to reduce the risk of human error.

8.2.1. Management responsibilities

Control A8.2.1: Management must require employees, contractors and third party users to apply security in accordance with established policies and procedures of the domain.

8.2.2. Information security awareness, education and training

Control A8.2.2: All employees of each domain and, where relevant, contractors and third party users must receive appropriate awareness training and regular updates in the domain's policies and procedures, as relevant for their job function.

All staff including employees, contract staff and third party personnel must receive adequate training on how to:

- operate the technology and information systems provided to them
- understand the importance of information security (including the security of all personal data – see §[REF _Ref206236498 \r \h]),
- use the security features provided within their information systems,
- select, manage and safeguard passwords (see §[REF _Ref204163435 \r \h]),
- prevent the spread of malicious software and data (see §[REF _Ref199310581 \r \h]),
- identify and safeguard important records from loss, destruction and falsification (see §[REF _Ref199325690 \r \h]),
- identify and report information security incidents (see §[REF _Ref206236896 \r

POL00397117

\h]), and

- ensure the physical security of their desktop and other information assets.

A formal security awareness program must be established to educate employees, contract staff and third party personnel on appointment (see §[REF _Ref206237403 \r \h * MERGEFORMAT]) and at scheduled intervals thereafter. The content of security awareness programs should be related to the current issues detected by the monitoring processes within Information Security Management System. The importance of the security of personal data (including Cardholder Data) must be emphasised at least annually.

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 / Horizon Online training facility.

8.2.3. Disciplinary Process

Control A8.2.3: There must be a formal disciplinary process for employees who have committed a security breach.

Each of the Horizon / Horizon Online domains must have their own disciplinary processes to manage violations of security 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.

8.3. Termination or change of employment

Objective: To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.

8.3.1. Termination responsibilities

Control A8.3.1: Responsibilities for performing employment termination or change of employment must be clearly defined and assigned.

POL00397117

8.3.2. Return of assets

Control A8.3.2: All employees, contractors and third party users must return all of the domain's assets in their possession upon termination of their employment, contract or agreement.

Domains must ensure that any physical or software assets under their control and which belong to Post Office Limited or the Royal Mail Group are returned to the domain upon termination or redeployment outside the Horizon / Horizon Online domain. Information assets must be either returned or, at management discretion, securely destroyed (see §[REF _Ref204171048 \r \h * MERGEFORMAT] and §[REF _Ref204169269 \r \h * MERGEFORMAT]).

8.3.3. Removal of access rights

Control A8.3.3: The access rights of all employees, contractors and third party users to information and information processing facilities must be removed upon termination of their employment, contract or agreement, or adjusted upon change of role.

Also see §[REF _Ref199319275 \n \h] - Access control policy.

9. Physical and environmental security

9.1. Secure areas

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

9.1.1. Physical security perimeter

Control A9.1.1: Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) must be used to protect areas that contain information and information processing facilities.

Central Facilities

Horizon / Horizon Online data centres and any location hosting other Horizon / Horizon Online 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.

POL00397117

Horizon / Horizon Online 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 (see §11.3.3).

Secure Areas must be used for housing all processing, storage and networking equipment and all network termination points used by the Horizon / Horizon Online 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/IEC 27002 for specific controls covering the physical security perimeter.

Branch Facilities

Horizon / Horizon Online 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 §[REF _Ref199326016 \r \h * MERGEFORMAT].

9.1.2. Physical entry controls

Control A9.1.2: Secure areas must be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

a) The date and time of entry and departure of all visitors must be recorded and retained securely for at least three months. All visitors must be supervised unless their access has been previously approved; they should only be granted access for specific, authorized purposes and must be issued with instructions on the security requirements of the area and on emergency procedures.

b) Access to areas where sensitive information is processed or stored must be controlled and restricted to authorized persons only; authentication controls, e.g. access control card plus PIN, must be used to authorize and validate all access; an audit trail of all access must be securely maintained;

c) Cameras must be used to monitor sensitive areas. Collected data must be audited and correlated with other entries. Collected data must be stored for at least three months, unless otherwise restricted by law.

POL00397117

d) All employees, contractors and third party users and all visitors must be required to wear some form of visible identification and should immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification;

e) All physical access tokens / identity badges must be surrendered on leaving the premises or when no longer valid.

f) Third party support service personnel must be granted restricted access to secure areas or sensitive information processing facilities only when required; this access must be authorized and monitored;

g) Access rights to secure areas should be regularly reviewed and updated, and revoked when necessary (see §[REF _Ref204166900 \r \h * MERGEFORMAT]).

9.1.3. Securing offices, rooms and facilities

Control A9.1.3: Physical security for offices, rooms, and facilities must be designed and applied.

Domains are referred to ISO/IEC 27002 for specific controls covering securing offices, rooms and facilities.

9.1.4. Protecting against external and environmental threats

Control A9.1.4: Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster must be designed and applied.

Equipment must be physically protected from environmental hazards. Special controls may be required to protect against hazards and to safeguard supporting facilities, such as the electrical supply and cabling infrastructure.

9.1.5. Working in secure areas

Control A9.1.5: Physical protection and guidelines for working in secure areas must be designed and applied.

Domains are referred to ISO/IEC 27002 for specific controls covering working in secure areas.

9.1.6. Public access, delivery and loading areas

Control A9.1.6: Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises must be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

Domains are referred to ISO/IEC 27002 for specific controls covering isolated delivery and loading areas.

POL00397117

9.2. Equipment security

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

9.2.1. Equipment siting and protection

Control A9.2.1: Equipment must be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

General Policy on Equipment Siting & Protection

Equipment must be physically protected from security threats and environmental hazards (see also Section §[REF _Ref204167843 \r \h]). Protection of equipment (including network access and termination points) 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. Domains are referred to the corresponding section of ISO/IEC 27002 for specific controls covering equipment siting and protection. Also see the branch policy below.

For Horizon Online, all PIN Data Processing Devices, used in the Data Centres, must comply with the requirements of Federal Information Processing Standard Publication 140-2, Security Level 3 or higher (FIPS PUB 140-2 Level 3) [SEC-3217].

Branch Policy on Equipment Siting & Protection

For Horizon and Horizon Online 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.

POL00397117

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 / Horizon Online 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.

9.2.2. Supporting Utilities

Control A9.2.2: Equipment must be protected from power failures and other disruptions caused by failures in supporting utilities.

Equipment in data centres and associated support must be protected. Equipment in Branches does not need protection. Domains are referred to the corresponding section in ISO/IEC 27002 for specific controls covering utilities such as power supplies, telecommunications, water supplies, and heating / ventilation.

9.2.3. Cabling Security

Control A9.2.3: Power and telecommunications cabling carrying data or supporting information services must be protected from interception or damage.

*Domains are referred to the corresponding section of ISO/IEC 27002 for specific controls covering cabling security. See [REF _Ref199326016 \r \h * MERGEFORMAT](f) for cabling security in Branches.*

9.2.4. Equipment maintenance

Control A9.2.4: Equipment must be correctly maintained to ensure its continued availability and integrity.

Domains are referred to the corresponding section of ISO/IEC 27002 for specific controls covering equipment maintenance.

9.2.5. Security of equipment off-premises

Control A9.2.4: Security must be applied to off-site equipment taking into account the different risks of working outside the domain's premises.

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

POL00397117

value of the equipment and sensitivity of the data it might contain.

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 §[REF _Ref199326016 \n \h * MERGEFORMAT] for specific controls for Branch Terminals

9.2.6. Secure disposal or re-use of equipment

Control A9.2.6: All items of equipment containing storage media must be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.

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 ISO 9564 and ISO 11568.

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, must be checked prior to disposal to ensure that any sensitive data and licensed software have been removed or overwritten. Damaged storage devices containing sensitive data may require a risk assessment to determine if the items should be destroyed, repaired or discarded.

Paper records and reports containing operational business data or other sensitive information must be physically destroyed by cross-cut shredding, incineration or pulping.

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.

9.2.7. Removal of property

Control A9.2.7: Equipment, information or software should not be taken off-site without prior authorisation.

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.

The removal of any media (including tapes, disks, cassettes and printed reports)

POL00397117

containing CONFIDENTIAL or STRICTLY CONFIDENTIAL data from secure areas must be authorised by management (see §[REF _Ref204171366 \r \h * MERGEFORMAT]).

10. Communications and operations management

10.1. 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 Horizon / Horizon Online 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 the corresponding section of ISO/IEC 27002 for guidance on implementing the controls in this section, which is subject to the specific provisions, interpretations and highlights below.

10.1.1. Documented operating procedures

Control A10.1.1: Operating procedures must be documented, maintained, and made available to all users who need them.

The operating procedures identified by the security policy must be documented and maintained. Operating procedures must be treated as formal documents and changes authorised by management (see §[REF _Ref199240880 \r \h * MERGEFORMAT]).

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, key management, equipment maintenance, computer room and mail handling, management and safety.

10.1.2. Change Management

Control A10.1.2: Changes to information processing facilities and systems must be controlled.

Changes to Horizon and Horizon Online information processing facilities and systems must be controlled. Formal management responsibilities and procedures must be in place to ensure satisfactory control of all changes to equipment, software, configuration or procedures. In particular, it must not be possible to install any equipment,

POL00397117

application or operating system extension in Horizon Online except under the control of properly authorised and authenticated systems administrators carrying out authorised and audited changes [SEC-3299].

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 application change control procedures should be integrated (see also §[REF _Ref199240880 \r \h * MERGEFORMAT]). 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 were there is an impact on it;

d) communication of change details to all relevant persons;

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

10.1.3. Segregation of duties

Control A10.1.3: Duties and areas of responsibility must be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of assets.

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 §10.6.1.

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.

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.

10.1.4. Separation of development, test and operational facilities

Control A10.1.4: Development, test and operational facilities must be separated to reduce the risks of unauthorised access or changes to the operational system.

POL00397117

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 §[REF _Ref199225557 \r \h * MERGEFORMAT][REF _Ref199331680 \r \h * MERGEFORMAT]). Rules for the transfer of software from development to operational status must be defined and documented (also see §[REF _Ref199331704 \r \h * MERGEFORMAT]).

10.2. Third party service delivery management

Objective: To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.

10.2.1. Service management

Control A10.2.1: It must be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.

The risks should be identified in advance, and appropriate controls agreed with the domain operator and incorporated into the contract (see also §6.2 for the policy on third party contracts and outsourcing contracts involving access to Horizon / Horizon Online facilities).

Any risks associated with the interoperability of Horizon / Horizon Online 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, and

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

10.2.2. Monitoring and review of third party services

Control A10.2.2: The services, reports and records provided by the third party must be regularly monitored and reviewed, and audits shall be carried out regularly.

Domain suppliers who use third party services to deliver part of the Horizon Online service must monitor and review the services provided with the same rigour as internally provided services. Reviews must ensure that security controls are updated to reflect changing business, technology and regulatory risks and requirements. Audits of

POL00397117

third party services must be carried out as part of the domain suppliers internal audit program.

10.2.3. Managing changes to third party services

Control A10.2.3: Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, must be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.

Horizon and Horizon Online are considered critical systems to Post Office Limited. All changes impacting the service must be subject to change control procedures - see §[REF _Ref204167473 \r \h * MERGEFORMAT], which contains the policy on change control.

10.3. System planning and acceptance

Objective: To minimise the risk of systems failures.

10.3.1. Capacity management

Control A10.3.1: The use of resources must be monitored, tuned, and projections must be made of future capacity requirements to ensure the required system performance.

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/IEC 27002 for specific controls covering capacity planning.

10.3.2. System acceptance

Control A10.3.2: Acceptance criteria for new information systems, upgrades, and new versions must be established and suitable tests of the system(s) carried out during development and prior to acceptance.

Domains are referred to ISO/IEC 27002 for specific controls covering system acceptance.

The Royal Mail Group domain must comply with *the Security Design and Testing Policy (S18).*

10.4. Protection against malicious and mobile code

Objective: To protect the integrity of software and information.

POL00397117

10.4.1. Controls against malicious code

Control A10.4.1: Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures must be implemented.

All hosts and terminals carrying operational data must be protected against malware attacks. Such protection must be commensurate with the risk.

Domain suppliers are referred to the corresponding section of ISO/IEC 27002 for appropriate controls. Specifically:

a) Precautionary measures must prevent and detect the introduction of malicious software. It is essential that precautions be taken to detect and prevent computer viruses and other malware on personal computers and servers using related technology.

b) The use of software that has not been authorised for use in Horizon / Horizon Online 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) Malware detection and repair software must be installed on platforms where there is a significant risk of malware attack. It must be operated and regularly updated. Appropriate procedures and responsibilities must be in place to manage malware protection, training in its use, reporting and recovery from malware attacks.

e) Communications processes must be in place to verify all information relating to malware 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.

10.4.2. Controls against mobile code

Control A10.4.2: Where the use of mobile code is authorised, the configuration must ensure that the authorised mobile code operates according to a clearly defined security policy, and unauthorised mobile code must be prevented from executing.

In order to protect against the risks associated with mobile code:

a) Where Horizon or Horizon Online 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 Branch Terminal operating system allows their installation.

POL00397117

10.5. Back-up

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

10.5.1. Information back-up

Control A10.5.1: Back-up copies of information and software must be taken and tested regularly in accordance with an agreed backup policy.

Back-up copies of essential business information and software must be taken regularly and immediately prior to events such as maintenance or migration that put such information at risk of loss or corruption [SEC-3237].

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 §[REF _Ref204169468 \r \h * MERGEFORMAT]).

All media containing back-up material must be protected against loss and un-authorised access. Processes must exist which detect and report loss of, or unauthorised access to, backed-up material (see §[REF _Ref206229086 \r \h]). The security of the storage location must be reviewed regularly.

*See §[REF _Ref204169275 \r \h * MERGEFORMAT] for the policy on media in transit.*

Restoration following a failure must be in accordance with the change control procedures – see §[REF _Ref199240880 \r \h * MERGEFORMAT].

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. See §[REF _Ref204169435 \r \h * MERGEFORMAT] for the policy on data retention.

Domain suppliers are referred to the corresponding section of ISO/IEC 27002 for further guidance on interpretation.

10.6. Network security 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/IEC 27002 for guidance on interpretation, which is subject to the specific provisions, interpretations

POL00397117

and highlights below. Also see §[REF _Ref199242017 \r \h * MERGEFORMAT] of this document for the policy on network access control.

10.6.1. Network controls

Control A10.6.1: Networks must be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.

Operational responsibility for networks must be identified and documented. Network management must 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.

For Horizon Online, configuration standards must be documented for all network components (firewalls, routers etc) on which the security and segmentation of the network depends. The standards must establish, document and justify the protocols, services and ports necessary for the correct operation of Horizon Online. Protocols which are generally considered risky (e.g. FTP) must also document the security features implemented to mitigate the risks associated with the protocol. Operational controls must ensure that all such components are configured in accordance with the standards at all times (including after re-booting the component).

*See §[REF _Ref199234799 \r \h * MERGEFORMAT] for more network controls.*

10.7. Media handling and security

Objective: To prevent unauthorised disclosure, modification, removal or destruction of assets and interruptions to business activities.

Domain suppliers must implement the following ISO / IEC 27001 controls, which are subject to the specific provisions, interpretations and highlights below them.

Control A10.7.1: There must be procedures in place for the management of removable media.

Control A10.7.2: Media must be disposed of securely and safely when no longer required, using formal procedures.

*See also §[REF _Ref204172493 \r \h * MERGEFORMAT].*

Control A10.7.3: Procedures for the handling and storage of information must be established to protect this information from unauthorized disclosure or misuse.

POL00397117

Control A10.7.4: System documentation must be protected against unauthorised access.

All removable computer media, such as tapes, disks, cassettes and printed reports must be managed to ensure that essential information is not lost and sensitive information is not disclosed in an unauthorised manner (see also §[REF _Ref204171048 \r \h]). Controls must detect if sensitive information is lost or subject to unauthorised access. These should include maintaining an inventory (see §[REF _Ref204171775 \r \h]) which is periodically verified and tracking all movements of media that may contain sensitive information.

10.8. Exchanges of information

Objective: To maintain the security of information and software exchanged within an organisation and with any external entity.

Domain suppliers must implement the following ISO / IEC 27001 controls, which are subject to the specific provisions, interpretations and highlights below them.

Control A10.8.1: Formal exchange policies, procedures, and controls must be in place to protect the exchange of information through the use of all types of communication facilities.

Control A10.8.2: Agreements must be established for the exchange of information and, where relevant, software between domains and external parties.

Control A10.8.3: Media containing information must be protected against unauthorized access, misuse or corruption during transportation beyond a domain's physical boundaries.

Control A10.8.4: Information involved in electronic messaging must be appropriately protected.

Control A10.8.5: Policies and procedures must be developed and implemented to protect information associated with the interconnection of business information systems.

The following specific provisions and clarifications apply to the above controls:

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

POL00397117

is a negligible residual risk to Post Office Ltd after taking into account any other countermeasures or related business processes that are implemented.

b) Replay of encrypted PIN values must be prevented especially over the otherwise unprotected PIN Pad to Counter Terminal interface [SEC-3301].

c) Horizon[5] 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).

d) Any Sensitive Personal Data (as defined by the Data Protection Act 1998 – see §15.1.4) 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 §7.2) 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. See also §[REF _Ref199331960 \r \h * MERGEFORMAT].

e) Any Horizon / Horizon Online information exchanged with external parties, including Post Office clients, must be the subject formal specifications approved by Post Office Limited.

f) All Horizon / Horizon Online domains are likely to use electronic systems other than those directly concerned with Horizon / Horizon Online. 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 / Horizon Online and non-Horizon / Horizon Online systems.

g) All Horizon / Horizon Online 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 / Horizon Online data.

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

i) Any messaging application (e.g. e-mail) used to communicate with branch staff via Horizon / Horizon Online must be configured such that it cannot be used to attack the integrity or availability of any Horizon / Horizon Online system including those in the branches and the data centres. In the event that e-mail facilities are added to Horizon Online, additional security controls must be agreed with Post Office Information Security prior to implementation.

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

[5] This control is less critical in Horizon Online since the terminal does not store sensitive data nor is it capable of transacting business as a stand-alone terminal.

POL00397117

10.9. Electronic commerce services

Objective: To ensure the security of electronic commerce services, and their secure use.

Control A10.9.1: Information involved in electronic commerce passing over public networks must be protected from fraudulent activity, contract dispute, and unauthorised disclosure and modification.

See the specific provisions and clarifications relating to this control in §[REF _Ref199326362 \r \h * MERGEFORMAT].

Control A10.9.2: Information involved in on-line transactions must be protected to prevent incomplete transmission, mis-routing, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.

For transactions involving banking or payment cards, the Primary Account Number (PAN) must be masked when displayed or printed such that only the first 6 and the last 4 digits are readable unless there is an overriding business case for an authorised user to view the complete number.[6]

Also see specific provisions and clarifications relating this control in §[REF _Ref199326371 \r \h * MERGEFORMAT].

Control A10.9.3: The integrity of information being made available on a publicly available system must be protected to prevent unauthorised modification.

This control is not applicable to Horizon / Horizon Online since no Horizon / Horizon Online information is made available on a publically accessible system.

10.10. Monitoring

Objective: To detect unauthorized information processing activities.

10.10.1. Audit logging

Control A10.10.1: Audit logs recording user activities, exceptions, and information security events must be produced and kept for an agreed period to assist in future investigations and access control monitoring.

[6] Note that there are tighter rules set by the card schemes for the display of cardholder data on receipts produced at branch terminals.

POL00397117

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.

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 / Horizon Online boundary.

See §[REF _Ref204174088 \r \h * MERGEFORMAT] for the policy on recording events for inclusion in the audit trail.

The audit trail must be maintained securely for a period agreed contractually with Post Office Ltd (see also §[REF _Ref199325690 \r \h]). 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 §[REF _Ref204172755 \r \h * MERGEFORMAT] for the policy on destruction of data including audit data and any extracts thereof. See §[REF _Ref204172779 \r \h * MERGEFORMAT] for the policy on back-up of data including audit data.

10.10.2. Monitoring system use

Control 10.10.2: Procedures for monitoring use of information processing facilities must be established and the results of the monitoring activities reviewed regularly.

Network-based intrusion detection must be deployed to protect systems storing or processing CONFIDENTIAL or STRICTLY CONFIDENTIAL data in the Horizon Online Data Centre (see §[REF _Ref204170172 \r \h * MERGEFORMAT]). The intrusion detection system must alert operational staff to suspected compromise of such systems.

File integrity monitoring tools must be used to alert operational staff to unauthorised

POL00397117

modification of critical[7] system or content files in the Cardholder Data Environment at the data centres. File integrity tools must be used elsewhere where a risk assessment indicates they would be of benefit.

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 §[REF _Ref204172827 \r \h * MERGEFORMAT] and §[REF _Ref199325690 \r \h].

Automated logging must be implemented in order to ensure the following events can be reconstructed:

a) All individual access to Horizon / Horizon Online business data (including Cardholder Data),

b) All actions taken by any individual with root or administrative privileges,

c) Access to all audit trails and event logs,

d) Invalid logical access attempts,

e) Use of identification and authentication mechanisms,

f) Initialization of the audit and event logs, and

g) Creation and deletion of system-level objects.

For each of the above events, the minimum that must be recorded is:

a) User identification,

b) Type of event,

c) Date and time,

d) Success or failure indication,

e) Origination of event, and

f) Identity or name of affected data, system component, or resource

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

[7] For file integrity monitoring purposes, critical files are those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. File integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the domain provider.

POL00397117

Logs for all system components must be reviewed for potential security violations and incidents at least daily. Special attention must be paid to all system components that perform security functions like intrusion detection system (IDS) and RADIUS servers. Filtering and alerting tools should be used to minimise the risk of violations or incidents being missed.

Operator logs should be subject to regular, independent checks against operating procedures.

10.10.3. Protection of log information

Control A10.10.3: Audit logging facilities and information must be protected against tampering and unauthorised access.

All event logging data must be promptly retrieved to a centralised system where it is secured and analysed. Unauthorised changes to audit logging facilities and information must be detected and reported.

Domain suppliers are referred to the corresponding section of ISO/IEC 27002 for further guidance on interpretation.

10.10.4. Administrator and operator logs

Control A10.10.4: System administrator and system operator activities must be logged.

See §[REF _Ref204174241 \r \h] for further policies on this topic.

10.10.5. Fault logging

Control A10.10.5: Faults must be logged, analysed, and appropriate action taken.

There must be a process for reporting and handling faults and ensuring that appropriate 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.

10.10.6. Clock synchronisation

Control A10.10.6: The clocks of all relevant information processing systems within Horizon / Horizon Online must be synchronized with an accurate time source.

Relevant information processing systems must be interpreted as including any system component generating audit logging file entries for Horizon / Horizon Online (see §[REF _Ref204174297 \r \h * MERGEFORMAT]).

Domain suppliers are referred to corresponding section of ISO/IEC 27002 for further guidance on

POL00397117

interpretation.

11. Access control

Objective: To control access to Horizon / Horizon Online resources.

11.1. Business requirement for access control

Objective: To control access to information.

11.1.1. Access control policy

Control A11.1.1: An access control policy must be established, documented, and reviewed based on business and security requirements for access.

General Policy

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

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

The policy must take account of the following:

a) Security requirements of Horizon / Horizon Online applications,

b) Identification of all information related to Horizon / Horizon Online applications,

c) Policies for information dissemination and authorisation, e.g. the need to know principle, 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, and

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

Access must only be granted where there is an identified business need and must be denied unless specifically allowed.

Access to Horizon / Horizon Online must only be from systems approved by management.

POL00397117

Formal user access management processes must ensure that access control is kept up-to-date to reflect changes in users' employment and responsibilities – see §[REF _Ref205979241 \r \h].

UserIDs and passwords must not be shared[8], unless in very specific circumstances for which a specific exception would need to be agreed with Post Office Information Security.[9] 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.

On newly installed equipment and software (including replacements), default passwords and identification strings must be changed prior to setting the equipment / software live.

All passwords transmitted across any internal or external network must be encoded such that it is infeasible for an interceptor to deduce the password. Similarly, it must be infeasible to deduce password from the stored reference value against which entered passwords are verified.

Horizon Online users must not have any access to add, modify, delete or execute any operating system or application files (including databases) 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 [SEC-3228].

Horizon & Horizon Online Branch Terminal - Specific Policy

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 / Horizon Online 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 / Horizon Online 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.

11.2. User access management

Objective: To ensure authorised user access and to prevent unauthorised access to information systems.

8 In particular, the practice of allocating group or shared passwords is explicitly prohibited.

9 This requirement also means that userIDs and passwords used by applications must not be shared with individual users or other processes.

POL00397117

11.2.1. User registration

Control A11.2.1: There must be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.

The access control procedures for user registration and de-registration must include:

a) allocating unique user IDs to enable users to be linked to and held responsible for their actions;

b) checking that the user has appropriate management authorisation

c) checking that the level of access granted is appropriate to the business purpose (see §[REF _Ref204161912 \r \h]) and is consistent with security policy, e.g. it does not compromise segregation of duties (see §[REF _Ref204161940 \r \h]);

d) ensuring users are aware of their responsibilities in respect of access control procedures (see §[REF _Ref204163435 \r \h])

e) requiring users to sign statements indicating that they understand the conditions of access;

f) ensuring access is not granted until authorisation procedures are complete;

g) maintaining a formal record of all persons registered to use Horizon / Horizon Online systems;

h) immediately removing or blocking access rights of users who have changed roles or jobs or left the organization;

i) periodically checking for, and removing or blocking, redundant user IDs and accounts (see §[REF _Ref204162052 \r \h]);

j) ensuring that redundant user IDs are not issued to other users.

A role must be provided such that authorised 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 / Horizon Online.

11.2.2. Privilege management

Control A11.2.2: The allocation and use of privileges must be restricted and controlled.

Domain suppliers are referred to the corresponding section of ISO/IEC 27002 for guidance on interpretation.

11.2.3. User password management

Control A11.2.3: The allocation of passwords must be controlled through a formal management process.

POL00397117

a) Procedures must be established which verify the identity of a user prior to providing a new, replacement or temporary password.

b) Users allocated new or replacement passwords must be provided initially with a secure temporary password (see §[REF _Ref204159215 \r \h]), which they are forced to change immediately.

c) Temporary passwords must be given to users in a secure manner; the use of third parties or unprotected (clear text) electronic mail messages must be avoided.

d) Temporary passwords should be unique to an individual and must not be guessable;

e) Users should acknowledge receipt of passwords.

f) Passwords must never be stored on computer systems in an unprotected form.

g) Default vendor passwords must be altered following installation of systems or software.

11.2.4. Review of user access rights

Control A11.2.4: Management must ensure users' access rights are reviewed at regular intervals using a formal process.

In this context, regular intervals must not exceed 90 days.

Domain suppliers are referred to the corresponding section of ISO/IEC 27002 for further guidance on interpretation.

11.3. User responsibilities

Objective: To prevent unauthorised user access, and compromise or theft of information and information processing facilities.

11.3.1. Password use

Control A11.3.1: Users must be required to follow good security practices in the selection and use of passwords.

All domains must comply with the following 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 4 other passwords have been used.

d) Passwords must be a minimum of 7 characters long and must be alphanumeric (i.e. a mix of letters and numbers). There must not be more than two consecutive

POL00397117

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 for at least 30 minutes or until an administrator has replaced the password in accordance with §[REF _Ref204164269 \r \h].

11.3.2. Unattended user equipment

Control A11.3.2: Users must ensure that unattended equipment has appropriate protection.

Domain suppliers are referred to the corresponding section of ISO/IEC 27002 for guidance on interpretation.

11.3.3. Clear desk and clear screen policy

Control A11.3.3: A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities must be adopted where appropriate.

All domains must recognise the information security classifications of this policy. A clear desk and clear screen policy must be followed whenever handling information classified as CONFIDENTIAL or STRICTLY CONFIDENTIAL (see §[REF _Ref204163708 \r \h * MERGEFORMAT]).

Users of Branch Terminals must be encouraged to clear the screen on their terminal or logoff whenever it is left unattended (also see §[REF _Ref204163732 \r \h * MERGEFORMAT] and §[REF _Ref204163740 \r \h * MERGEFORMAT]).

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 Royal Mail Group *Clear Desk Policy* (s10), to reduce the risks of unauthorised access, loss of, and damage to, information during and outside normal working hours.

Individual domains are also referred to the corresponding section of ISO/IEC 27002 for further guidance on interpretation.

11.4. Network access control

Objective: To prevent unauthorized access to networked services.

*Also see §[REF _Ref199233886 \r \h * MERGEFORMAT] for the policy on Network Security Management.*

POL00397117

11.4.1. Policy on use of network services

Control A11.4.1: Users must only be provided with access to the services that they have been specifically authorised to use.

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

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

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

(c) Controls must protect against denial-of-service attacks originating from non-Horizon / Horizon Online systems including those listed in [REF _Ref199242230 \w \h * MERGEFORMAT] and [REF _Ref199242314 \w \h * MERGEFORMAT].

(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 / Horizon Online service.

(e) The Horizon Online system must not retrieve data from any external web service, including the Internet, unless additional security controls are documented and agreed with Post Office Information Security. The objective of such controls is to prevent the import of any mobile or malicious code (see §[REF _Ref199310581 \r \h * MERGEFORMAT] and §[REF _Ref199310617 \r \h * MERGEFORMAT]) and the unauthorised export of any Horizon Online business data.

(f) All Horizon Online systems must use private IP addresses (see RFC1918) which must not be exposed across the system boundary[10].

(g) For Horizon Online, a Cardholder Data Environment (see Definitions, §[REF _Ref199240475 \r \h * MERGEFORMAT]) must be defined, documented and agreed with Post Office Limited's PCI DSS auditors. The documentation must show all connections to Cardholder Data and must be maintained to reflect changes to the system. The Cardholder Data Environment must be segmented from other parts of the Horizon Online system in order to minimise the scope of the PCI DSS audit in so far as this is practical. Additional controls will exist in this environment to comply with PCI DSS.

[10] E.g. by the use of NAT (Network Address Translation).

POL00397117

(h) Network management staff within each domain must be alerted to any attempt to reach the Horizon / Horizon Online 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.

(i) Precautions must be taken to mitigate the risk of unauthorised devices being connected to any component of the Horizon Online system, with the exception of passive devices within the Branch.

(j) 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.

(k) 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. Also see the cryptographic policy, §12.3.

(l) 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.

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

(n) 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. Also see the policy on separation of live and test, §[REF _Ref199331482 \r \h].

(o) The use of wireless technologies within or associated with Horizon / Horizon Online 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.[11]

11.4.2. User authentication for external connections

Control A11.4.2: Appropriate authentication methods must be used to control access by remote users.

[11] The objective of this requirement is to ban Wi-Fi, Bluetooth and similar technologies whilst permitting, for example, the use of mobile phone carriers and satellite technologies to provide branch to data centre communications provided the traffic is secured appropriately for transit over a public network.

POL00397117

Users accessing Horizon Online facilities remotely (i.e. over any external connection) must be authenticated using a technique employing two factors: something the user has (e.g. a cryptographic token) and something the user knows (e.g. a password). For the sake of clarity, the connection between a branch and the data centre is not considered external for the purpose of this statement.

Domain suppliers are referred to the corresponding section of ISO/IEC 27002 for further guidance on interpretation.

11.4.3. Equipment identification in networks

Control A11.4.3: Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment.

Domain suppliers are referred to the corresponding section of ISO/IEC 27002 for guidance on interpretation.

11.4.4. Remote diagnostic and configuration port protection

Control A11.4.4: Physical and logical access to diagnostic and configuration ports must be controlled.

Ports, services, and similar facilities installed on an Horizon / Horizon Online computer or network facility, which are not specifically required for business functionality, must be disabled or removed.

Network access points used by third parties for remote diagnostic and/or configuration purposes must only be enabled for the duration necessary for the specific activity being undertaken. Enabling of the network access points must be under the control of the appropriate Horizon / Horizon Online support management. Third party staff and/or diagnostic systems accessing Horizon / Horizon Online systems must be identified and authenticated in accordance with this policy.

11.4.5. Segregation of networks

Control A11.4.5: Groups of information services, users, and information systems must be segregated on networks.

All RADIUS servers that authenticate network access must be secured and segregated into logical network segments by carrier access method and be externally visible to authorised domain users only.

The Cardholder Data Environment (see Definitions, §[REF _Ref199240475 \r \h * MERGEFORMAT]) must be secured and segmented to prevent unauthorised access to Cardholder Data and Sensitive Authentication Data.

All network interfaces between the Horizon / Horizon Online environment and

POL00397117

external networks must ensure that there are barriers (such as dynamic packet filtering firewalls and DMZs) that control access and communications flows between internal systems and the external connections. Such controls must ensure segregation between external networks as well as segregation between internal and external systems.[12]

*Domain suppliers are referred to the corresponding section of ISO/IEC 27002 for further guidance on interpretation. Also see the policy on the use of network services, §[REF _Ref199225557 \r \h * MERGEFORMAT] above.*

11.4.6. Network connection control

Control A11.4.6: For shared networks, especially those extending across a domain's boundaries, the capability of users to connect to the network must be restricted, in line with the access control policy and requirements of the business applications (see §[REF _Ref199320474 \r \h]).

*Domain suppliers are referred to the corresponding section of ISO/IEC 27002 for guidance on interpretation. Also see the policy on the use of network services, §[REF _Ref199225557 \r \h * MERGEFORMAT] above.*

11.4.7. Network routing control

Control A11.4.7: Routing controls must be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.

*Domain suppliers are referred to the corresponding section of ISO/IEC 27002 for additional guidance on interpretation. Also see the policy on the use of network services, §[REF _Ref199225557 \r \h * MERGEFORMAT] above.*

11.5. Operating system access control

Objective: To prevent unauthorized access to operating systems.

11.5.1. Secure log-on procedures

Control A11.5.1: Access to operating systems must be controlled by a secure log-on procedure.

Domain suppliers are referred to the corresponding section of ISO/IEC 27002 for guidance on implementing this control, which is subject to the specific provisions, interpretations and highlights below.

Branch staff must be prevented from accessing the operating system on Counter Terminals. They must only have access to authorised applications. For Horizon Online,

[12] Also see specific policy for mobile and personal computers in §[REF _Ref199321930 \r \h]

POL00397117

terminals must be bootable only from the primary mass storage device on the terminal.

Branch Terminals must include a single user action that, in between customer sessions, cleanly terminates the clerk session and presents a new clerk login screen. During a customer session, the clerk must first complete or cancel the session in accordance with business rules.

11.5.2. User identification and authentication

Control A11.5.2: All users must have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.

Domain suppliers are referred to the corresponding section of ISO/IEC 27002 for guidance on interpretation. See also §[REF _Ref204158711 \r \h] for additional authentication requirements over external connections.

11.5.3. Password management system

Control A11.5.3: Systems for managing passwords must be interactive and must ensure quality passwords.

Domain suppliers are referred to the corresponding section of ISO/IEC 27002 for guidance on interpretation. Also see the policy on password use, §[REF _Ref204159215 \r \h]

11.5.4. Use of system utilities

Control A11.5.4: The use of utility programs that might be capable of overriding system and application controls must be restricted and tightly controlled.

See also the Branch access control policy §11.1.1

11.5.5. Session time-out

Control A11.5.5: Inactive sessions must shut down after a defined period of inactivity.

Any inactive user session that has been idle for more than 15 minutes must be suspended or terminated until the user is re-authenticated.

Users of Horizon Online Branch Terminals must have access to a single user action that clears the screen, prevents further data entry and maintains the current session states, until such time as the operator is re-authenticated or until the Branch Terminal sessions are closed following an inactivity timeout; whichever is the sooner.

POL00397117

11.5.6. Limitation of connection time

Control A11.5.5: Restrictions on connection times must be used to provide additional security for high-risk applications.

Domain suppliers are referred to the corresponding section of ISO/IEC 27002 for guidance on interpretation.

11.6. Application and information access control

Objective: To prevent unauthorized access to information held in application systems.

11.6.1. Information access restriction

Control A11.6.1: Access to information and application system functions by users and support personnel must be restricted in accordance with the defined access control policy.

Application-level logon to Branch Terminals must provide equivalent security to that provided by logon via native operating systems. [SEC-3295]

Horizon Online Branch Terminals must have controls in place to prevent user bypass of the standard application [SEC-3298].

All access to any database containing CONFIDENTIAL or STRICTLY CONFIDENTIAL data as defined in §[REF _Ref204165333 \r \h * MERGEFORMAT] (including Cardholder Data as defined in §[REF _Ref199240475 \r \h * MERGEFORMAT]) must be authenticated. This includes access by applications, administrators, and all other users. Direct access to such databases by individuals is strongly deprecated and must be limited to authorised database administrators.

*Also see the access control policy, §[REF _Ref199320486 \r \h * MERGEFORMAT].*

11.6.2. Sensitive system isolation

Control A11.6.2: Sensitive systems must have a dedicated (isolated) computing environment.

Horizon and Horizon Online must be treated as sensitive systems in this context.

Domain suppliers are referred to the corresponding section of ISO/IEC 27002 for further guidance on interpretation.

POL00397117

11.7. Mobile computing and teleworking

Objective: To ensure information security when using mobile computing and teleworking facilities.

Domain suppliers must implement the following ISO / IEC 27001 controls, which are subject to the specific provisions, interpretations and highlights below them.

Control A11.7.1: A formal policy must be in place, and appropriate security measures must be adopted to protect against the risks of using mobile computing and communication facilities.

Control A11.7.2: A policy, operational plans and procedures must be developed and implemented for teleworking activities.

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.

When accessing Cardholder Data remotely via modem, it must not be stored onto local hard drives, floppy disks, or other external media. Cut-and-paste and print functions must not be used during such remote access.

Personal firewall software must be present and operational on any mobile and/or employee-owned computers (for example, laptops used by employees) which is used to access cardholder data and which also has direct connectivity to the Internet.

Domain suppliers are referred to the corresponding section of ISO/IEC 27002 for further guidance on interpretation of these controls.

12. Systems acquisition, development and maintenance

12.1. Security requirements of information systems

Objective: To ensure that security is an integral part of Information Systems

12.1.1. Security Requirements Analysis and specification

Control A12.1.1: Statements of business requirements for new information systems, or enhancements to existing information systems must specify the requirements for security controls.

All security requirements must be identified, justified, agreed and documented as part

POL00397117

of the overall business case.

The security controls must be specified within the statements of business requirements for Horizon, Horizon Online, 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
- Regulatory and contractual requirements

Security requirements and controls should be identified from risk assessment.

Within the Post Office domain:

- 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.

12.2. Correct processing in applications

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

Domain suppliers must implement the following ISO / IEC 27001 controls, which are subject to the specific provisions, interpretations and highlights below them.

Control A12.2.1: Data input to applications must be validated to ensure that this data is correct and appropriate.

In particular, applications must be protected against common application level attacks such as buffer overflows, SQL injection and cross-site scripting.

POL00397117

Control A12.2.2: Validation checks must be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.

Control A12.2.3: Requirements for ensuring authenticity and protecting message integrity in applications must be identified, and appropriate controls identified and implemented.

*See also §[REF _Ref199325178 \r \h * MERGEFORMAT]*

Control A12.2.4: Data output from an application must be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

In particular:

a) See the policy on Mobile Code, §[REF _Ref252542154 \r \h].

b) Applications requiring passwords must comply with the password policy in §11.3.1 unless otherwise approved by Post Office Ltd Information Security.

c) The security of data, especially business data, transaction data, sensitive data (see §[REF _Ref204163708 \r \h]) and audit data (see §[REF _Ref204174297 \r \h]), must be maintained in accordance with this policy during any migration from a live Horizon system or component to Horizon Online.

d) The secure file-store in configured Horizon terminals must be rendered unrecoverable on migration to Horizon Online. Any terminal which is not migrated (e.g. it is taken out of service instead) must have its file-store deleted in accordance with established Horizon procedures [SEC-3273].

12.3. Cryptographic Controls

Objective: To protect the confidentiality, authenticity and or integrity of information by cryptographic means.

12.3.1. Policy on the use of cryptographic controls

Control A12.3.1: A policy on the use of cryptographic controls for protection of information must be developed and implemented.

Horizon / Horizon Online 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

POL00397117

- 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 (see also §[REF _Ref199326016 \r \h * MERGEFORMAT]). 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 §[REF _Ref204163708 \r \h] 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 §[REF _Ref199225557 \r \h].

(f) Cardholder Data (see Definitions, §[REF _Ref199240475 \r \h * MERGEFORMAT]) must be rendered unreadable anywhere it is stored (including data on portable media, backup media, and in logs) by using any of the following approaches [SEC-3307]:

- One-way hashes (hashed indexes), such as SHA-1
- Truncation
- Index tokens and PADs, with the PADs being securely stored
- Strong cryptography, such as Triple-DES 128-bit or AES 256-bit with associated key management processes and procedures (see §[REF _Ref199327186 \r \h]).

(g) All Sensitive Authentication Data and Cardholder Data must be encrypted using approved algorithms and encryption protocols whilst in transit over any public network unless specifically agreed in writing by the Client. It must also be encrypted when sent by any end-user messaging technology (for example, e-mail, instant messaging, chat), whether internal or external to the domain. Approved algorithms are 128-bit 3DES (as per ANSI X9.52) and 256-bit AES (FIPS 197). Approved encryption protocols are SSL v3 / TLS, SSH, IPSec, and PPTP. [SEC-3310]

POL00397117

(h) 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.

(i) Subject to (h), 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). 256-bit AES is the preferred symmetric algorithm and key length.

(j) 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 / Horizon Online – See §[REF _Ref199224960 \r \h]. Selectively encrypted fields such as PINs, passwords and cryptographic key management fields are not considered such a threat.

(k) All non-console administrative access must be encrypted. Technologies such as SSH, VPN, or SSL/TLS must be used for web-based management and other non-console administrative access.

12.3.2. Key management

Control A12.3.2: Key management must be in place to support the use of cryptographic techniques.

See item 12.3.1(b), above for the policy on keys associated with cardholder PINs.

It must be possible to recover the system to a secure operating state from the compromise of any key that could directly or indirectly expose plain text PIN values [SEC-3226].

WAN encryption key management must be independent of network configuration such that the confidentiality of Post Office traffic is not compromised by a single configuration error of either the WAN or the encryption system [SEC-3168].

Key management processes and procedures must ensure that keys are generated such that it is impractical for an attacker to deduce the value of the key.

Keys must be protected in storage and transmission such that the integrity and (for secret / private keys) confidentiality of the key is maintained. Keys must also be protected against misuse and unauthorised substitution.

Secret / private keys distributed manually must be distributed and entered using split knowledge wherever a key is protecting against unauthorised internal disclosure. There must be dual control over the generation and installation of all such keys i.e. no one person may be able to generate, deduce or install such a key.

Key distribution must be restricted to the fewest possible people and places consistent

POL00397117

with maintaining system availability.

Keys must be changed periodically (at least annually if protecting Cardholder Data or Sensitive Authentication Data) and whenever it is known or suspected that they may have been compromised. Public key certificates must be revoked whenever it is known or suspected that the associated key set may have been compromised.

All key management procedures must be documented. Records must be maintained of key management activities. Those involved in key management processes protecting data classified as Confidential, Strictly Confidential, Cardholder Data, or Sensitive Authentication Data must be formally advised of their responsibilities and sign that they accept them.

12.4. Security of system files

Objective: To ensure the security of system files.

12.4.1. Control of Operational Software

Control A12.4.1: There must be procedures in place to control the installation of software on operational systems.

a) Operational Horizon Online systems must be "hardened" to an appropriate level of security in accordance with manufacturer's guidelines.

b) The updating of the operational software, applications, and program libraries must only be performed by trained staff upon appropriate management authorisation (see §[REF _Ref205973435 \r \h * MERGEFORMAT]).

c) Systems must only hold approved executable code, and not development code or compilers. All unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers must be removed.

d) Applications and operating system software must only be implemented after extensive and successful testing; the tests should include tests on usability, security, effects on other systems and user-friendliness, and must be carried out on separate systems (see also §[REF _Ref199331482 \r \h * MERGEFORMAT]); it should be ensured that all corresponding program source libraries have been updated.

e) A configuration control system must be used to keep control of all implemented software as well as the system documentation.

f) A rollback strategy should be in place before changes are implemented.

g) An audit log must be maintained of all updates to operational program libraries (also see §[REF _Ref204174088 \r \h * MERGEFORMAT]).

POL00397117

12.4.2. Protection of System Test Data

Control A12.4.2: Test data must be selected carefully, and protected and controlled.

Live Horizon / Horizon Online 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" such that no personal data is identifiable. Similarly, test data, test accounts, test passwords and test cryptographic keys must be removed from development and test systems (including all applications) before they migrate to live.

12.4.3. Access control to program source code

Control A12.4.3: Access to program source code must be restricted.

In particular:

a) Horizon / Horizon Online 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.

12.5. 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.

12.5.1. Change control procedures

Control A12.5.1: The implementation of changes must be controlled by the use of formal change control procedures.

In order to minimize the corruption of information systems, there must be strict control over the implementation of changes – see §[REF _Ref199309597 \r \h * MERGEFORMAT]. 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

POL00397117

In order to maximize the availability of the system there must be strict control over the maintenance of all operational Horizon / Horizon Online 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) Also see the policy on Technical Vulnerability Management, §[REF _Ref199331121 \r \h].

12.5.2. Further development & support policies

Domain suppliers must implement the following ISO/IEC 27001 controls.

Domain suppliers are referred to the corresponding section of ISO/IEC 27002 for guidance on interpretation.

Control A12.5.2: When operational systems are changed, business critical applications must be reviewed and tested to ensure there is no adverse impact on live operations or security.

Control A12.5.3: Modifications to off-the-shelf software packages must be discouraged, limited to necessary changes, and all changes must be strictly controlled.

Control A12.5.4: Opportunities for information leakage must be prevented.

Control A12.5.5: Outsourced software development must be supervised and monitored by the domain supplier.

*See also §[REF _Ref205721619 \r \h * MERGEFORMAT] & §[REF _Ref205721677 \r \h * MERGEFORMAT]*

Control: Custom application source code must be reviewed prior to operational use.

In accordance with Royal Mail policy S18, source code developed specifically for Horizon Online systems must be reviewed prior to operational use. The review must be independent of the developer producing the code and must check for compliance with §[REF _Ref199333408 \r \h]. Any deficiencies detected in the code must be corrected.

POL00397117

12.6. Technical Vulnerability Management

Objective: To reduce risks resulting from exploitation of published technical vulnerabilities.

12.6.1. Control of technical vulnerabilities

Control A12.6.1: Timely information about technical vulnerabilities of information systems being must be obtained, the exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

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 / Horizon Online and in accordance with the change control procedures.

13. Information Security Incident Management

13.1. Responding to security incidents and malfunctions

Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

13.1.1. Reporting security incidents

Control A13.1.1: Security incidents must be reported through appropriate management channels as quickly as possible.

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

See also §[REF _Ref205974803 \r \h] and §[REF _Ref205721677 \r \h].

13.1.2. Reporting security weaknesses

Control A13.1.2: All employees, contractors and third party users of information systems and services must be required to note and report any observed or suspected security weaknesses in systems or services.

Domain suppliers are referred to the corresponding section of ISO/IEC 27002 for guidance on

POL00397117

interpretation.

13.2. Management of information security incidents and improvements

Objective: To ensure a consistent and effective approach is applied to the management of information security incidents.

13.2.1. Responsibilities and procedures

Control A13.2.1: Management responsibilities and procedures must be established to ensure a quick, effective, and orderly response to information security incidents.

Each domain must take responsibility for reporting (see §[REF _Ref206240088 \r \h]), investigating and resolving security incidents within its own domains that present an actual or potential threat to the Horizon / Horizon Online environment or to any of the Horizon / Horizon Online participants. Domains must be able to identify and respond to potentially serious security incidents at any time during the contracted operating hours for the Horizon / Horizon Online service. Formal incident response plans must be established for any incident likely to affect business continuity (see §[REF _Ref204169468 \r \h]).

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

- Confidentiality, including compromise of Cardholder Data and other personal data,
- Integrity, including errors resulting from incomplete or inaccurate business data, and/or
- Availability, including information system failures, loss of service, and 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 or security alert (see §[REF _Ref204174088 \r \h]). 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 notified to relevant parties (via Post Office) and managed across the Horizon / Horizon Online community.

Security breaches and incidents must be reviewed regularly by the Information Security Management Forum (see §[REF _Ref206419393 \r \h]) to establish cross-community

POL00397117

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 / Horizon Online service. Serious incidents must be reported to Post Office Ltd. at the earliest opportunity. Where the timescales for reporting incidents are formally agreed between Post Office and its Clients, those timescales must be agreed with the relevant Domains in writing. A summary of other incidents must be reported to Post Office Ltd. as part of the regular service review.

See §8.2.3 for the policy on the Disciplinary Process that can be invoked as a result of an incident.

13.2.2. Learning from information security incidents

Control A13.2.2: There must be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.

Domain suppliers are referred to the corresponding section of ISO/IEC 27002 for guidance on interpretation.

13.2.3. Collection of evidence

Control A13.2.3: Where a follow-up action against a person or organisation after an information security incident involves legal action (either civil or criminal), evidence must be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

It is necessary to have adequate evidence to support an action against a person or organisation. Whenever this action is an internal disciplinary matter (see §[REF _Ref205717383 \r \h]) 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.

POL00397117

14. 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 and to ensure their timely resumption.

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

There must be a process in place, involving the Horizon / Horizon Online community, to develop and maintain business continuity of the end-to-end Horizon / Horizon Online 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 / Horizon Online 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[13] and updating of the plans and amended processes put in place where necessary.

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

Individual Horizon / Horizon Online 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.

Domain suppliers must implement the following ISO/IEC 27001 controls. Domain suppliers are referred to the corresponding section of ISO/IEC 27002 and to ISO/IEC 24762:2008 for guidance on interpretation.

[13] Plans that address compromise of Cardholder Data must be tested at least annually.

POL00397117

Control A14.1.1: A managed process must be developed and maintained for business continuity for each domain, which addresses the information security requirements needed for the Horizon / Horizon Online business continuity.

ControlA14.1.2: Events that can cause interruptions to Horizon / Horizon Online business processes must be identified, along with the probability and impact of such interruptions and their consequences for information security.

Note: compromise of the confidentiality personal data (including Cardholder Data) can cause an interruption to business processes, as systems may have to be closed down until the source of the compromise is identified, further compromise prevented and/or legal evidence is collected.

Control A14.1.3: Plans must be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.

Control A14.1.4: A single framework of business continuity plans must be maintained to ensure all plans are consistent, to address information security requirements consistently, and to identify priorities for testing and maintenance.

Control A14.1.5: Business continuity plans must be tested and updated regularly to ensure that they are up to date and effective.

15. Compliance

15.1. Compliance with legal requirements

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

15.1.1. Identification of applicable legislation

Control A15.1.1: All relevant statutory, regulatory and contractual requirements and the domain's approach to meet these requirements must be explicitly defined, documented, and kept up to date for Horizon / Horizon Online and the domain.

Horizon / Horizon Online must ensure compliance with all legislative requirements including the:

POL00397117

- 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 / Horizon Online 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. Should any domain become aware that a change to another domain's systems or procedures is required in order to meet legal requirements, it must inform the other domain.

15.1.2. Intellectual property rights (IPR)

Control A15.1.2: Appropriate procedures must be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.

Appropriate procedures must 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.

15.1.3. Protection of organizational records

Control A15.1.3: Important records must be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements.

Important records of each domain must be protected from loss, destruction and falsification.

POL00397117

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. Domains must issue guidelines on the retention, storage, handling, and disposal of records and information. A retention schedule must be drawn up identifying records and the period of time for which they should be retained. The schedule must also identify where there are requirements for the disposal of records at the end of their retention period. To comply with PCI DSS, the audit trail (see §[REF _Ref205722017 \r \h]) must be retained for at least one year with a minimum of three months available online (Royal Mail Group requirements are currently in excess of this).

Sensitive Authentication Data (see Definitions) must not be stored in any file or database including log, audit or diagnostic files after a transaction has been authorised even if the data is encrypted. Such data must also be deleted after use [SEC-3304].

See also §[REF _Ref204169342 \r \h] and §[REF _Ref204169468 \r \h] for policies on the protection from loss.

15.1.4. Data protection and privacy of personal information

Control A15.1.4: Data protection and privacy must be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.

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. 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 / Horizon Online 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 / Horizon Online. 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 / Horizon Online domains are a Data Processor as defined by the Act and must only process personal data for the purposes specified in the relevant Horizon / Horizon Online 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. The relevant Data Controller is responsible for identifying such data as Sensitive Personal Data and must inform those responsible for implementing the Horizon / Horizon Online system so that appropriate additional security measures can be taken – see §[REF _Ref199321405 \r \h]([REF _Ref205974982 \r \h].

POL00397117

Post Office Ltd. has developed a policy which covers 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.

15.1.5. Prevention of misuse of information processing facilities

Control A15.1.5: Users must be deterred from using information processing facilities for unauthorized purposes.

The Horizon / Horizon Online facilities are provided strictly for business purposes. Any use of these facilities for non-business or other purposes not associated with Horizon / Horizon Online, 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 §8.2.3). The security incident reporting procedures (see §13) must be used where one domain detects misuse by staff of another domain.

15.1.6. Regulation of cryptographic controls

Control A15.1.6: Cryptographic controls must be used in compliance with all relevant agreements, laws, and regulations.

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.

See §[REF _Ref204172827 \r \h] for the policy on the collection of evidence.

POL00397117

15.2. Reviews of security policy and technical compliance

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

15.2.1. Compliance with security policies and standards

Control A15.2.1: Managers in each domain must ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.

The security of information systems must be regularly reviewed. Such reviews must be performed against the Horizon / Horizon Online security policy and any other applicable security policies.

15.2.2. Technical compliance checking

Control A15.2.2: Information systems must be regularly checked for compliance with security implementation standards.

Technical platforms and information systems must be audited for compliance with security policy at planned intervals, and after any major change[14] and after any major security incident:

a) Firewall and router rule sets, especially those protecting the system boundary and the Cardholder Data Environment, must be reviewed at least quarterly.

b) Security controls, limitations, network connections, and restrictions must be tested at least annually to assure compliance with the access control policy (see §[REF _Ref199319275 \r \h]).

c) A scan of live data centres and operational support centres must be performed at least quarterly to demonstrate compliance with the policy in §[REF _Ref199225557 \r \h * MERGEFORMAT][REF _Ref199321772 \r \h * MERGEFORMAT] (policy prohibiting the use of wireless technologies). [SEC-3191]

d) Vulnerability scans of any internal IP port which provides access to the Cardholder Environment must be performed at least quarterly. Scans must be routinely scheduled and performed to confirm all ports are configured to support the network access control policy (see §[REF _Ref199225557 \r \h]).

e) Vulnerability scans must be performed at least quarterly by a scan vendor qualified by the payment card industry on any IP port which provides access to the Cardholder Environment from the Internet.

f) Penetration tests must be performed routinely to confirm Horizon Online is not

[14] Including after new system component installations, changes in network topology, firewall rule modifications, product upgrades, etc.

POL00397117

susceptible to known hacking exploits. Penetration tests of the Cardholder Environment must be performed at least annually at both network layer and at application layer. Tests of other elements of the system can be scheduled based on a risk assessment of the consequences and likelihood of a successful attack. All tests must be performed in accordance with Royal Mail Group Policy S7 - Security Health Check Policy.

g) File integrity checks (see §[REF _Ref204174088 \r \h]) must be performed at least weekly.

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

15.3. Information Systems Audit Considerations

Objective: To maximize the effectiveness of and to minimize interference to/from the information systems audit process.

Domain suppliers must implement the following ISO / IEC 27001 controls. Domain suppliers are referred to the corresponding section of ISO/IEC 27002 for guidance on interpretation.

Control A15.3.1: Audit requirements and activities involving checks on operational systems must be carefully planned and agreed to minimize the risk of disruptions to business processes.

Control A15.3.2: Access to information systems audit tools must be protected to prevent any possible misuse or compromise.

Post Office Ltd retains the right to review activity records of all Horizon / Horizon Online 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 / Horizon Online.

*See §[REF _Ref205722532 \r \h * MERGEFORMAT] for the policy on creating a transaction audit trail.*

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

POL00397117

Annex A – Mapping PCI DSS controls to ISO/IEC 27001 controls

This Appendix provides a cross-reference to the policy in this document which addresses the various PCI DSS controls. Reference to a heading number includes reference to all sub-headings under that heading number.

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

PCI DSS Requirements	Policy Ref.
1.1 Establish firewall configuration standards that include the following:	§[REF _Ref199224556 \r \h * MERGEFORMAT]
1.1.1 A formal process for approving and testing all external network connections and changes to the firewall configuration	§[REF _Ref199224618 \r \h * MERGEFORMAT], §[REF _Ref199309868 \r \h * MERGEFORMAT], §[REF _Ref199310383 \r \h * MERGEFORMAT], §[REF _Ref199225557 \r \h * MERGEFORMAT]
1.1.2 A current network diagram with all connections to cardholder data, including any wireless networks	§[REF _Ref199224556 \r \h * MERGEFORMAT], §[REF _Ref199225557 \r \h * MERGEFORMAT][REF _Ref199310662 \r \h * MERGEFORMAT]
1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	§[REF _Ref199225557 \r \h * MERGEFORMAT][REF _Ref199242230 \w \h * MERGEFORMAT], §[REF _Ref199315812 \r \h * MERGEFORMAT], §[REF _Ref205723895 \r \h], §[REF _Ref199319038 \r \h * MERGEFORMAT]
1.1.4 Description of groups, roles, and responsibilities for logical management of network components	§[REF _Ref199224556 \r \h * MERGEFORMAT], §[REF _Ref199319275 \r \h * MERGEFORMAT]
1.1.5 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure	§[REF _Ref199224556 \r \h * MERGEFORMAT], §[REF _Ref205723895 \r \h]

POL00397117

PCI DSS Requirements	Policy Ref.
1.1.6 Quarterly review of firewall and router rule sets	§[REF _Ref199319856 \r \h * MERGEFORMAT]
1.2 Build a firewall configuration that restricts connections between untrusted networks[15] and any system components in the cardholder data environment.	§[REF _Ref199319948 \r \h * MERGEFORMAT], §[REF _Ref199224556 \r \h * MERGEFORMAT], §[REF _Ref199320012 \r \h * MERGEFORMAT], §[REF _Ref205723895 \r \h]
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.	§[REF _Ref199319948 \r \h * MERGEFORMAT], §[REF _Ref199320012 \r \h * MERGEFORMAT], §[REF _Ref205723895 \r \h]
1.2.2 Secure and synchronize router configuration files.	§[REF _Ref199224556 \r \h], §[REF _Ref199321559 \r \h * MERGEFORMAT]
1.2.3 Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.	See §[REF _Ref199225557 \r \h * MERGEFORMAT][REF _Ref199321772 \r \h * MERGEFORMAT] prohibiting the use of wireless technology.
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment. **1.3.1** Implement a DMZ to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment.	*Note: Horizon Online should not contain publically accessible servers or wireless networks – see §[REF _Ref199320231 \r \h * MERGEFORMAT]*
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	§[REF _Ref199234799 \r \h * MERGEFORMAT]
1.3.3 Do not allow any direct routes inbound or outbound for traffic between the Internet and the cardholder data environment.	§[REF _Ref199234799 \r \h * MERGEFORMAT], §[REF _Ref199320873 \r \h * MERGEFORMAT]

[15] Note: An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.

POL00397117

PCI DSS Requirements	Policy Ref.
1.3.4 Do not allow internal addresses to pass from the Internet into the DMZ	§[REF _Ref199225557 \r \h * MERGEFORMAT]
1.3.5 Restrict outbound traffic from the cardholder data environment to the Internet such that outbound traffic can only access IP addresses within the DMZ.	§[REF _Ref199234799 \r \h * MERGEFORMAT], §[REF _Ref199320873 \r \h * MERGEFORMAT]
1.3.6 Implementing stateful inspection, also known as dynamic packet filtering (that is, only "established" connections are allowed into the network)	§[REF _Ref199321036 \r \h * MERGEFORMAT]
1.3.7 Placing the database in an internal network zone, segregated from the DMZ	§[REF _Ref199321405 \r \h * MERGEFORMAT]([REF _Ref199321431 \r \h * MERGEFORMAT], §[REF _Ref199321137 \r \h * MERGEFORMAT]
1.3.8 Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet. Use technologies that implement RFC 1918 address space, such as port address translation (PAT) or network address translation (NAT).	§[REF _Ref199225557 \r \h * MERGEFORMAT], §[REF _Ref205723895 \r \h]
1.4 Instal personal firewall software on any mobile and employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.	§[REF _Ref199321888 \r \h * MERGEFORMAT], §[REF _Ref205723895 \r \h], §[REF _Ref199321930 \r \h * MERGEFORMAT]

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

PCI DSS Requirements	Policy Ref.
2.1 Always change vendor-supplied defaults **before** installing a system on the network (for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts).	§[REF _Ref199322719 \r \h * MERGEFORMAT]
2.1.1 For wireless environments, connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.	§[REF _Ref199225557 \r \h * MERGEFORMAT][REF _Ref199321772 \r \h * MERGEFORMAT]

POL00397117

PCI DSS Requirements	Policy Ref.
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening.	§[REF _Ref199224556 \r \h * MERGEFORMAT],
2.2.1 Implement only one primary function per server	§[REF _Ref199321405 \r \h] Control A10.8.5 Item ([REF _Ref205726302 \r \h], §[REF _Ref199324218 \r \h * MERGEFORMAT]
2.2.2 Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function)	§[REF _Ref199225557 \r \h * MERGEFORMAT], §[REF _Ref199324570 \r \h * MERGEFORMAT], §[REF _Ref205974138 \r \h]
2.2.3 Configure system security parameters to prevent misuse	§[REF _Ref199225557 \r \h * MERGEFORMAT], §[REF _Ref205974138 \r \h]
2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	§[REF _Ref199324860 \r \h * MERGEFORMAT], §[REF _Ref205974138 \r \h]
2.3 Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.	§[REF _Ref199325579 \r \h * MERGEFORMAT]
2.4 Shared Hosting providers must protect each entity's hosted environment and data. These providers must meet specific requirements as detailed in Appendix A: "PCI DSS Applicability for Hosting Providers."	§[REF _Ref199225557 \r \h * MERGEFORMAT]

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

PCI DSS Requirements	Policy Ref.
3.1 Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.	§[REF _Ref199325690 \r \h * MERGEFORMAT], §[REF _Ref205974597 \r \h]

POL00397117

PCI DSS Requirements	Policy Ref.
3.2 Do not store sensitive authentication data subsequent to authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3*:*	§[REF _Ref199325756 \r \h * MERGEFORMAT], §[REF _Ref205974597 \r \h]
3.2.1 Do not store the full contents of any track from the magnetic stripe (that is on the back of a card, in a chip or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic stripe data *In the normal course of business, the following data elements from the magnetic stripe may need to be retained: the accountholder's name, primary account number (PAN), expiration date, and service code. To minimize risk, store only those data elements needed for business.* *Note: See "PCI DSS Glossary" for additional information.*	§[REF _Ref199325811 \r \h * MERGEFORMAT], §[REF _Ref199240475 \r \h * MERGEFORMAT], §[REF _Ref205974597 \r \h]
3.2.2 Do not store the card-verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions *Note: See "[PCI DSS] Glossary" for additional information.*	§[REF _Ref199325811 \r \h * MERGEFORMAT], §[REF _Ref199240475 \r \h * MERGEFORMAT], §[REF _Ref205974597 \r \h]
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block.	§[REF _Ref199325811 \r \h * MERGEFORMAT], §[REF _Ref199240475 \r \h * MERGEFORMAT], §[REF _Ref205974597 \r \h]
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed). *Note: This requirement does not apply to employees and other parties with a legitimate business need to see the full PAN; the requirement does not supersede stricter requirements in place for displays of cardholder data (for example, for point-of-sale [POS] receipts).*	§[REF _Ref199326704 \r \h * MERGEFORMAT], §[REF _Ref205974597 \r \h]
3.4 Render PAN, at minimum, unreadable anywhere it is stored (including data on portable digital media, backup media, in logs) by using any of the following approaches: • One-way hashes based on strong cryptography • Truncation • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key management processes and procedures The MINIMUM account information that must be rendered unreadable is the PAN. *If for some reason, a company is unable to encrypt cardholder data, refer to [PCI DSS] Appendix B: "Compensating Controls."* *Strong cryptography" is defined in the PCI DSS Glossary of Terms, Abbreviations, and Acronyms.*	§[REF _Ref199326772 \r \h * MERGEFORMAT][REF _Ref199326827 \r \h * MERGEFORMAT] , §[REF _Ref205974597 \r \h]

POL00397117

PCI DSS Requirements	Policy Ref.
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local system or Active Directory accounts). Decryption keys must not be tied to user accounts.	§[REF _Ref199327186 \r \h * MERGEFORMAT]
3.5 Protect encryption keys used for encryption of cardholder data against both disclosure and misuse:	§[REF _Ref199327199 \r \h * MERGEFORMAT]
3.5.1 Restrict access to keys to the fewest number of custodians necessary	§[REF _Ref199327975 \r \h * MERGEFORMAT]
3.5.2 Store keys securely in the fewest possible locations and forms	§[REF _Ref199327975 \r \h * MERGEFORMAT]
3.6 Fully document and implement all key management processes and procedures for keys used for encryption of cardholder data, including the following:	§[REF _Ref199327975 \r \h * MERGEFORMAT]
3.6.1 Generation of strong cryptographic keys	§[REF _Ref199327975 \r \h * MERGEFORMAT]
3.6.2 Secure cryptographic key distribution	§[REF _Ref199327975 \r \h * MERGEFORMAT]
3.6.3 Secure cryptographic key storage	§[REF _Ref199327975 \r \h * MERGEFORMAT]
3.6.4 Periodic cryptographic key changes • As deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically • At least annually	§[REF _Ref199327975 \r \h * MERGEFORMAT]
3.6.5 Retirement or replacement of old or suspected compromised cryptographic keys	§[REF _Ref199327975 \r \h * MERGEFORMAT]
3.6.6 Split knowledge and establishment of dual control of cryptographic keys	§[REF _Ref199327975 \r \h * MERGEFORMAT]
3.6.7 Prevention of unauthorized substitution of cryptographic keys	§[REF _Ref199327975 \r \h * MERGEFORMAT]
3.6.8 Requirement for key custodians to sign a form stating that they understand and accept their key-custodian responsibilities	§[REF _Ref199327975 \r \h * MERGEFORMAT]

Requirement 4: Encrypt transmission of cardholder data across open, public networks

PCI DSS Requirements	Policy Ref.

POL00397117

PCI DSS Requirements	Policy Ref.
4.1 Use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks. *Examples of open, public networks that are in scope of the PCI DSS are the Internet, Wireless technologies, Global System for Mobile communications (GSM), and General Packet Radio Service (GPRS).*	§[REF _Ref199330567 \r \h * MERGEFORMAT][REF _Ref199330599 \r \h * MERGEFORMAT]
4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission. • *For new wireless implementations, it is prohibited to implement WEP after March 31, 2009.* • *For current wireless implementations, it is prohibited to use WEP after June 30, 2010.*	§[REF _Ref199225557 \r \h * MERGEFORMAT][REF _Ref199321772 \r \h * MERGEFORMAT] (policy prohibiting the use of WiFi)
4.2 Never send unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat).	§[REF _Ref199330947 \r \h * MERGEFORMAT][REF _Ref205975627 \n \h] & [REF _Ref199330599 \r \h * MERGEFORMAT]

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software or programs

PCI DSS Requirements	Policy Ref.
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers)	§[REF _Ref199331003 \r \h * MERGEFORMAT]
5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against other forms of malicious software.	§[REF _Ref199224960 \r \h * MERGEFORMAT]
5.2 Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.	§[REF _Ref199224960 \r \h * MERGEFORMAT]

Requirement 6: Develop and maintain secure systems and applications

PCI DSS Requirements	Policy Ref.

POL00397117

PCI DSS Requirements	Policy Ref.
6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install critical security patches within one month of release. *Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*	§[REF _Ref199331121 \r \h * MERGEFORMAT]
6.2 Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update configuration standards as required by PCI DSS Requirement 2.2 to address new vulnerability issues.	§[REF _Ref199331121 \r \h * MERGEFORMAT]
6.3 Develop software applications in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices, and incorporate information security throughout the software development life cycle. These processes must include the following:	§[REF _Ref199331704 \n \h]
6.3.1 Testing of all security patches and system and software configuration changes before deployment, including but not limited to the following:	§[REF _Ref199310383 \r \h], §[REF _Ref199331332 \r \h * MERGEFORMAT], §[REF _Ref199333408 \r \h], §[REF _Ref205974138 \r \h]([REF _Ref252473651 \w \h]
6.3.1.1 Validation of all input (to prevent cross-site scripting, injection flaws, malicious file execution, etc.)	
6.3.1.2 Validation of proper error handling	
6.3.1.3 Validation of secure cryptographic storage	
6.3.1.4 Validation of secure communications	
6.3.1.5 Validation of proper role-based access control (RBAC)	
6.3.2 Separate development/test and production environments	§[REF _Ref199331482 \r \h * MERGEFORMAT]
6.3.3 Separation of duties between development/test and production environments	§[REF _Ref199331541 \r \h * MERGEFORMAT], §[REF _Ref199331582 \r \h * MERGEFORMAT]
6.3.4 Production data (live PANs) are not used for testing or development	§[REF _Ref252542915 \r \h]
6.3.5 Removal of test data and accounts before production systems become active	§[REF _Ref252542915 \r \h]
6.3.6 Removal of custom application accounts, User IDs, and passwords before applications become active or are released to customers	§[REF _Ref199319275 \r \h], §[REF _Ref252542915 \r \h]

POL00397117

PCI DSS Requirements	Policy Ref.
6.3.7 Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability. *Note: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle required by PCI DSS Requirement 6.3. Code reviews can be conducted by knowledgeable internal personnel or third parties. Web applications are also subject to additional controls, if they are public facing, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.*	§[REF _Ref199332221 \r \h * MERGEFORMAT], §[REF _Ref199332335 \r \h * MERGEFORMAT]
6.4 Follow change control procedures for all system and software configuration changes. The procedures must include the following:	§[REF _Ref199332589 \r \h * MERGEFORMAT], §[REF _Ref199240880 \r \h * MERGEFORMAT]
6.4.1 Documentation of impact	§[REF _Ref199332589 \r \h * MERGEFORMAT], §[REF _Ref199240880 \r \h * MERGEFORMAT]
6.4.2 Management sign-off by appropriate parties	§[REF _Ref199332589 \r \h * MERGEFORMAT], §[REF _Ref199240880 \r \h * MERGEFORMAT]
6.4.3 Testing of operational functionality	§[REF _Ref199332925 \r \h * MERGEFORMAT]
6.4.4 Back-out procedures	§[REF _Ref199332589 \r \h * MERGEFORMAT], §[REF _Ref205974138 \r \h]
6.5 Develop all web applications (internal and external, and including web administrative access to application) based on secure coding guidelines, such as the *Open Web Application Security Project Guidelines*. Review custom application code to identify coding vulnerabilities. Cover prevention of common coding vulnerabilities in software development processes, to include the following: *Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current in the OWASP guide when PCI DSS v1.2 was published. However, if and when the OWASP guide is updated, the current version must be used for these requirements.*	§[REF _Ref199333408 \r \h], §[REF _Ref199333103 \r \h * MERGEFORMAT]
6.5.1 Cross-site scripting (XSS)	§[REF _Ref199333103 \r \h * MERGEFORMAT], §[REF _Ref199333408 \r \h * MERGEFORMAT]
6.5.2 Injection flaws, particularly SQL injection. Also consider LDAP and Xpath injection flaws as well as other injection flaws.	
6.5.3 Malicious file execution	
6.5.4 Insecure direct object references	
6.5.5 Cross-site request forgery (CSRF)	

POL00397117

PCI DSS Requirements	Policy Ref.
6.5.6 Information leakage and improper error handling	
6.5.7 Broken authentication and session management	
6.5.8 Insecure cryptographic storage	
6.5.9 Insecure communications	
6.5.10 Failure to restrict URL access	
6.6 For public-facing web-facing applications address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes • Installing a web-application firewall in front of public-facing web applications	§[REF _Ref199333103 \r \h * MERGEFORMAT]

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know

PCI DSS Requirements	Policy Ref.
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following:	§[REF _Ref199320474 \r \h], §[REF _Ref205979241 \r \h]
7.1.1 Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities	
7.1.2 Assignment of privileges is based on individual personnel's job classification and function	
7.1.3 Requirement for an authorization form signed by management that specifies required privileges	
7.1.4 Implementation of an automated access control system	
7.2 Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:	§[REF _Ref199320474 \r \h], §[REF _Ref205979241 \r \h]
7.2.1 Coverage of all system components	
7.2.2 Assignment of privileges to individuals based on job classification and function	
7.2.3 Default "deny-all" setting	

POL00397117

Requirement 8: Assign a unique ID to each person with computer access.

PCI DSS Requirements	Policy Ref.
8.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	§[REF _Ref199334374 \r \h]([REF _Ref205979412 \n \h] & ([REF _Ref205979423 \n \h], §[REF _Ref199334509 \r \h * MERGEFORMAT]
8.2 In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users: • Password or passphrase • Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys)	§[REF _Ref199334509 \r \h * MERGEFORMAT], §[REF _Ref204157318 \n \h]
8.3 Implement two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.	§[REF _Ref204157318 \r \h]
8.4 Render all passwords unreadable during transmission and storage on all system components using strong cryptography (defined in PCI DSS Glossary of Terms, Abbreviations, and Acronyms).	§[REF _Ref204157704 \r \h]
8.5 Ensure proper user authentication and password management for non-consumer users and administrators on all system components as follows: **8.5.1** Control addition, deletion, and modification of user IDs, credentials, and other identifier objects	§[REF _Ref204158763 \r \h]
8.5.2 Verify user identity before performing password resets	§[REF _Ref204159525 \r \h]
8.5.3 Set first-time passwords to a unique value for each user and change immediately after the first use	§[REF _Ref204159541 \r \h], §[REF _Ref205979916 \n \h]
8.5.4 Immediately revoke access for any terminated users	§[REF _Ref204159680 \r \h], §[REF _Ref205979983 \r \h], §[REF _Ref204166900 \r \h]
8.5.5 Remove inactive user accounts at least every 90 days	§[REF _Ref204160179 \r \h] & §[REF _Ref204162222 \r \h]
8.5.6 Enable accounts used by vendors for remote maintenance only during the time period needed	§[REF _Ref204162563 \r \h]

POL00397117

PCI DSS Requirements	Policy Ref.
8.5.7 Communicate password procedures and policies to all users who have access to cardholder data	§[REF _Ref204163482 \r \h] & §[REF _Ref204163467 \r \h]
8.5.8 Do not use group, shared, or generic accounts and passwords	§[REF _Ref204163532 \r \h]
8.5.9 Change user passwords at least every 90 days	§[REF _Ref204163580 \r \h]
8.5.10 Require a minimum password length of at least seven characters	§[REF _Ref204163593 \r \h]
8.5.11 Use passwords containing both numeric and alphabetic characters	§[REF _Ref204163609 \r \h]
8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used	§[REF _Ref204163622 \r \h]
8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts	§[REF _Ref204163641 \r \h]
8.5.14 Set the lockout duration to thirty minutes or until administrator enables the user ID	§[REF _Ref204164317 \r \h]
8.5.15 If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal	§[REF _Ref204164587 \r \h]
8.5.16 Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users	§[REF _Ref199319275 \n \h], §[REF _Ref204165907 \r \h], §[REF _Ref199333408 \r \h]([REF _Ref205980235 \n \h],

Requirement 9: Restrict physical access to cardholder data.

PCI DSS Requirements	Policy Ref.
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems that store, process, or transmit cardholder data.	§[REF _Ref204166181 \r \h]
9.1.1 Use video cameras or other access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. *Note: "Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes the areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.*	§[REF _Ref204167180 \r \h]

POL00397117

PCI DSS Requirements	Policy Ref.
9.1.2 Restrict physical access to publicly accessible network jacks	§[REF _Ref204167965 \r \h]
9.1.3 Restrict physical access to wireless access points, gateways, and handheld devices	§[REF _Ref199225557 \r \h * MERGEFORMAT][REF _Ref199321772 \r \h * MERGEFORMAT] (policy prohibiting the use of wireless technologies)
9.2 Develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. *For the purposes of this requirement, "employee" refers to full-time and part-time employees, temporary employees and personnel, and consultants who are "resident" on the entity's site. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the facility for a short duration, usually not more than one day.*	§[REF _Ref204168168 \r \h]([REF _Ref204168197 \r \h]
9.3 Make sure all visitors are handled as follows: **9.3.1** Authorized before entering areas where cardholder data is processed or maintained	§[REF _Ref204168244 \r \h]
9.3.2 Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as non-employees	§[REF _Ref204168255 \r \h]
9.3.3 Asked to surrender the physical token before leaving the facility or at the date of expiration	§[REF _Ref204168626 \r \h]([REF _Ref204168628 \r \h], §[REF _Ref204170730 \r \h]
9.4 Use a visitor log to maintain a physical audit trail of visitor activity. Document the visitor's name, the firm represented, and the employee authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.	§[REF _Ref204168626 \r \h]([REF _Ref204168663 \r \h]
9.5 Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.	§[REF _Ref204169342 \r \h], §[REF _Ref204169269 \r \h]
9.6 Physically secure all paper and electronic media that contain cardholder data	§[REF _Ref204170129 \r \h], §[REF _Ref204169269 \r \h]
9.7 Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data: including the following **9.7.1** Classify the media so it can be identified as confidential	§[REF _Ref204170172 \r \h], §[REF _Ref204169269 \r \h]
9.7.2 Send the media by secured courier or other delivery method that can be accurately tracked	§[REF _Ref204170184 \r \h], §[REF _Ref204169269 \r \h]

POL00397117

PCI DSS Requirements	Policy Ref.
9.8 Ensure management approves any and all media that is moved from a secured area (especially when media is distributed to individuals).	§[REF _Ref204171645 \r \h], §[REF _Ref204169269 \r \h]
9.9 Maintain strict control over the storage and accessibility of media that contains cardholder data. **9.9.1** Properly maintain inventory logs of all media and conduct media inventories at least annually.	§[REF _Ref204171775 \r \h], §[REF _Ref204169269 \r \h]
9.10 Destroy media containing cardholder data when it is no longer needed for business or legal reasons as follows **9.10.1** Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed	§[REF _Ref204172318 \r \h]
9.10.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	§[REF _Ref204172327 \r \h]

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data.

PCI DSS Requirements	Policy Ref.
10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	§[REF _Ref204174785 \r \h]
10.2 Implement automated audit trails for all system components to reconstruct the following events: **10.2.1** All individual accesses to cardholder data	§[REF _Ref204174088 \r \h], §[REF _Ref205980674 \r \h]
10.2.2 All actions taken by any individual with root or administrative privileges	§[REF _Ref204174088 \r \h], §[REF _Ref205980674 \r \h]
10.2.3 Access to all audit trails	§[REF _Ref204174088 \r \h]
10.2.4 Invalid logical access attempts	§[REF _Ref204174088 \r \h]
10.2 5 Use of identification and authentication mechanisms	§[REF _Ref204174088 \r \h]
10.2.6 Initialization of the audit logs	§[REF _Ref204174088 \r \h]

POL00397117

PCI DSS Requirements	Policy Ref.
10.2.7 Creation and deletion of system-level objects	§[REF _Ref204174088 \r \h]
10.3 Record at least the following audit trail entries for all system components for each event: **10.3.1** User identification	§[REF _Ref204174088 \r \h]
10.3.2 Type of event	§[REF _Ref204174088 \r \h]
10.3.3 Date and time	§[REF _Ref204174088 \r \h]
10.3.4 Success or failure indication	§[REF _Ref204174088 \r \h]
10.3.5 Origination of event	§[REF _Ref204174088 \r \h]
10.3.6 Identity or name of affected data, system component, or resource	§[REF _Ref204174088 \r \h]
10.4 Synchronize all critical system clocks and times	§[REF _Ref204174142 \r \h]
10.5 Secure audit trails so they cannot be altered **10.5.1** Limit viewing of audit trails to those with a job-related need	§[REF _Ref204174393 \r \h]
10.5.2 Protect audit trail files from unauthorized modifications	§[REF _Ref204174324 \r \h]
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	§[REF _Ref204174589 \r \h]
10.5.4 Write logs for external-facing technologies[16] onto a log server on the internal LAN.	§[REF _Ref204174589 \r \h]
10.5.5 Use file integrity monitoring or change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)	§[REF _Ref204174324 \r \h]
10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS). *Note: Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6*	§[REF _Ref204174088 \r \h]
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).	§[REF _Ref199325690 \r \h]

[16] for example, wireless, firewalls, DNS, mail

POL00397117

Requirement 11: Regularly test security systems and processes.

PCI DSS Requirements	Policy Ref.
11.1 Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use.	§[REF _Ref199319856 \r \h]([REF _Ref206215645 \w \h]
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). *Note: Quarterly external vulnerability scans must be performed by a scan vendor qualified by the payment card industry. Scans conducted after network changes may be performed by the company's internal staff.*	§[REF _Ref199319856 \r \h] ([REF _Ref252298890 \r \h] & ([REF _Ref252298893 \r \h]
11.3 Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following **11.3.1** Network-layer penetration tests **11.3.2** Application-layer penetration tests	§[REF _Ref199319856 \n \h * MERGEFORMAT]([REF _Ref206419799 \n \h]
11.4 Use intrusion-detection systems and/or intrusion prevention systems to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up-to-date.	§[REF _Ref204174088 \r \h]
11.5 Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files; and configure the software to perform critical file comparisons at least weekly. *Note: For file integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. File integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is the merchant or service provider)*	§[REF _Ref204174088 \r \h], §[REF _Ref199319856 \r \h]([REF _Ref206220249 \n \h]

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for employees and contractors.

PCI DSS Requirements	Policy Ref.
12.1 Establish, publish, maintain, and disseminate a security policy that accomplishes the following:	

POL00397117

PCI DSS Requirements	Policy Ref.
12.1.1 Addresses all PCI DSS requirements	This document.
12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment	§[REF _Ref206220387 \n \h]
12.1.3 Includes a review at least once a year and updates when the environment changes	§[REF _Ref206419834 \n \h]
12.2 Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).	§[REF _Ref199224618 \n \h]
12.3 Develop usage policies for critical employee-facing technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), e-mail usage and Internet usage) to define proper use of these technologies for all employees and contractors. Ensure these usage policies require the following:	§[REF _Ref206223763 \n \h], §[REF _Ref206225198 \n \h] Also see §[REF _Ref199225557 \r \h * MERGEFORMAT][REF _Ref199321772 \r \h * MERGEFORMAT] prohibiting the use of wireless technology.
12.3.1 Explicit management approval	§[REF _Ref206228103 \n \h], §[REF _Ref199309597 \n \h]
12.3.2 Authentication for use of the technology	§[REF _Ref199319275 \n \h]
12.3.3 A list of all such devices and personnel with access	§[REF _Ref204171775 \n \h]
12.3.4 Labeling of devices with owner, contact information, and purpose	§[REF _Ref206229978 \n \h]
12.3.5 Acceptable uses of the technology	§[REF _Ref206229629 \n \h]
12.3.6 Acceptable network locations for the technologies	§[REF _Ref199315812 \n \h] Also see §[REF _Ref199225557 \r \h * MERGEFORMAT][REF _Ref199321772 \r \h * MERGEFORMAT] prohibiting the use of wireless technology.
12.3.7 List of company-approved products	§[REF _Ref199319275 \r \h]
12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity	§[REF _Ref204163732 \n \h], §[REF _Ref199324570 \n \h]

POL00397117

PCI DSS Requirements	Policy Ref.
12.3.9 Activation of remote-access technologies for vendors only when needed by vendors, with immediate deactivation after use	§[REF _Ref199324570 \n \h]
12.3.10 When accessing cardholder data remotely via remote access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media.	§[REF _Ref199321930 \n \h]
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all employees and contractors.	§[REF _Ref206230889 \n \h], §[REF _Ref206230947 \n \h]
12.5 Assign to an individual or team the following information security management responsibilities: **12.5.1** Establish, document, and distribute security policies and procedures	§[REF _Ref206231316 \n \h]
12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel	§[REF _Ref206234536 \n \h]([REF _Ref206234595 \n \h], §[REF _Ref206234652 \n \h]
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations	§[REF _Ref206234833 \r \h]
12.5.4 Administer user accounts, including additions, deletions, and modifications	§[REF _Ref206234868 \r \h]
12.5.5 Monitor and control all access to data	§[REF _Ref199319275 \r \h], §[REF _Ref204174088 \r \h], §[REF _Ref206235099 \r \h]
12.6 Implement a formal security awareness program to make all employees aware of the importance of cardholder data security:	§[REF _Ref206235228 \r \h], §[REF _Ref199224960 \r \h]([REF _Ref206235460 \n \h]
12.6.1 Educate employees upon hire and at least annually	§[REF _Ref206237655 \r \h]
12.6.2 Require employees to acknowledge at least annually that they have read and understood the company's security policy and procedures	§[REF _Ref206237603 \r \h]
12.7 Screen potential employees (see definition of "employee" at 9.2 above) prior to hire to minimize the risk of attacks from internal sources. *For those employees such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.*	§[REF _Ref206233738 \n \h]
12.8 If cardholder data is shared with service providers, then contractually the following is required: **12.8.1** Maintain a list of service providers.	§[REF _Ref205721677 \r \h]

POL00397117

PCI DSS Requirements	Policy Ref.
12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess.	
12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status.	
12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.	§[REF _Ref206240599 \r \h], §[REF _Ref206239687 \r \h]([REF _Ref206234595 \n \h],
12.9.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: • Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum • Specific incident response procedures • Business recovery and continuity procedures • Data back-up processes • Analysis of legal requirements for reporting compromises • Coverage and responses of all critical system components • Reference or inclusion of incident response procedures from the payment brands	§[REF _Ref206240599 \r \h], §[REF _Ref204169468 \r \h]
12.9.2 Test the plan at least annually	§[REF _Ref204169468 \r \h] – control A14.1.5.
12.9.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts	§[REF _Ref206242031 \r \h]
12.9.4 Provide appropriate training to staff with security breach response responsibilities	§[REF _Ref206242031 \r \h]
12.9.5 Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems	§[REF _Ref206242685 \r \h]
12.9.6 Develop process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments	§[REF _Ref206242326 \r \h], §[REF _Ref204169468 \r \h]

POL00397117

Appendix A: PCI DSS Applicability for Hosting Providers (with Testing Procedures)

Requirement A.1: Hosting providers protect cardholder data environment

Requirements	Policy Ref.
A.1 Protect each entity's (that is merchant, service provider, or other entity) hosted environment and data, as in A.1.1 through A.1.4: A hosting provider must fulfil these requirements as well as all other relevant sections of the PCI DSS. *Note: Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not guaranteed. Each entity* must *comply with the PCI DSS and validate compliance as applicable.*	
A.1.1 Ensure that each entity only only runs processes that have access to that entity's cardholder data environment	§[REF _Ref199225557 \n \h][REF _Ref199242314 \n \h]
A.1.2 Restrict each entity's access and privileges to own cardholder data environment only	§[REF _Ref199320474 \r \h]
A.1.3 Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10	§[REF _Ref204174088 \r \h], §[REF _Ref205722017 \r \h]
A.1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.	§[REF _Ref206243721 \n \h]

--- End of Policy ---