FUJ00002566

Post Office HNG-X Account Information Security Policy

FUJITSU RESTRICTED (COMMERCIAL IN CONFIDENCE)

Document Title	Post Office HNG-X Account Information Security Policy
Document Reference	SVM/SEC/POL/0003
Document Type	Policy
Release	Release Independent
Abstract	A definition and the fundamental principles of Information Security, Senior Management commitment with an Executive Statement as well as what it is expected of individuals Information Security on the Post Office HNG-X Account.
Document Status	APPROVED
Author	Kumudu Amaratunga (POA Security Operations) (Chris Cole)
Owner	Tom Lillywhite (POA CISO)
External Distribution	POL via the ISMF and all 3rd Parties for information

Approval Authorities:

Name	Role	See Dimensions for record
Peter Thompson	Fujitsu Services Delivery Executive	
Julie George	Post Office Ltd Head of Information Security	

FUJ00002566

0 Document Control

0.1 Table of Contents

FUJ00002566

0.2 Document Control

Version No.	Date	Summary of Changes and Reason for Issue	Related Change
0.1	17/01/08	Initial draft	
0.2	14/02/08	Updated to incorporate changes from CCN 1202 in Section 7.2	
0.3	28/02/08	Updated following review comments received to date This document has been revised by POA Document Management on behalf of the Acceptance Manager to contain notes which have been identified to POL as comprising evidence to support the assessment of named Acceptance Criteria by Document Review. This text must not be changed without authority from the FS Acceptance Manager. This version will not require full review using the POA Document Control Process, as agreed between Acceptance Manager and Programme Management.	
0.4	28/02/08	Updated following review comments received to date	
0.5	29/05/08	Updated following final comments from POL and to address further comments from Acceptance Team	
2.1	09/09/08	For Approval by POL	
2.2	12/09/08	Comments under review	
2.3	15/09/08	Updated following review comments from POL	
2.4	16/09/08	Updated following telephone call with POL	
2.5	16/09/08	Updated following email with POL	
2.6	23/09/08	For further review by POL	
3.0	20/10/08	For Approval by POL	
3.1	11/12/08	For Review by POL Ref Med /Low comments	
3.2	12/12/08	Revised table in section 0.4	
3.3	26/Jan/09	Updated following review by POL	
4.0	12/02/09	For Approval	
4.1	31/Aug/09	For Review	
5.0	15/Sep/09	For Approval	
5.1	3/06/2010	Annual Review	
5.2	08/09/11	Annual Review and changes in Fujitsu Protective Marking	
5.3	15-May-2012	Annual review	
5.3.1	28-Jun-2013	Interim Addendum to be issued until major re-write of ISMS document and issue of High Level Information Security Policy. Addresses PCI-DSS requirement 12 issues raised by QSA during audit.	
5.4	05-Nov-2013	Major revision for review. Change in approach of Information Security Policy and ISMS Manual.	CP1090

FUJ00002566

		Information Security Policy now only captures a definition and the fundamental principles of Information Security, Senior Management commitment with an Executive Statement as well as what it is expected of individuals. How the Account complies with the ISO/IEC 27001:2005 Controls are to be captured in the ISMS Manual.	
5.5	05-NOV-2013	Revised following review comments.	
6.0	23-Jan-2014	Approval version	

0.3 Review Details

Review Comments by :	
Review Comments to :	CISO, Information Security Risk and Assurance Manager and Post Office Account Document Management
Mandatory Review	
Fujitsu Services Delivery Executive	James Davidson (now Pete Thompson)
Fujitsu Services Client Managing Director	Haydn Jones
Fujitsu Services CISO	Tom Lillywhite
Fujitsu Services Operations Security Manager	Kumudu Amaratunga
Fujitsu Services Security Architect	Dave Haywood
Fujitsu Services Quality and Compliance Manager	Bill Membery
Fujitsu Services Commercial Manager	Sarah Guest
Post Office Ltd Head of Information Security	Julie George
Post Office Ltd Senior Commercial Manager	Liz Tuddenham
Optional Review	
Fujitsu Services Client Executive	Gavin Bell
Fujitsu Services Senior Operations Manager	Alex Kemp
Fujitsu Services Business Continuity Manager	Sathish Ramalingam
Fujitsu Services Lead SDM & Risk Manager	Yannis Symvoulidis
Fujitsu Services Commercial Manager	Adrian McMahon Stone
Post Office Ltd Commercial Manager	Sue Stewart
Issued for Information – Please restrict this distribution list to a minimum	

0.4 Associated Documents (Internal & External)

Reference	Version	Date	Title	Source
ISO/IEC 27001:2005	1.0	Oct 2005	Information Technology Techniques – Security Techniques – Information Security Management Systems – Requirements	BSI ISO/IEC
SVM/SEC/MAN/0003			POA Account ISMS Manual	Dimensions

FUJ00002566

N/A			(Fujitsu) Conduct Guidelines	Café Vik
CPM6			Legal Compliance	Café Vik
CPM20			Fujitsu Security Master Policy	Café Vik
CPM21			Intellectual Property	Café Vik
CPM27			Risk Policy	Café Vik
CPM36			Data Protection	Café Vik

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

0.5 Abbreviations

Abbreviation	Definition
BMS	Business Management System
CISO	Chief Information Security Officer
ISMF	Information Security Management Forum
ISMS	Information Security Management System
POA	(Fujitsu) Post Office Account
POL	Post Office Limited

0.6 Glossary

Term	Definition
Fujitsu UK & I	Fujitsu United Kingdom and Ireland

0.7 Changes Expected

Changes
This is the initial draft of the new POA Information Security Policy. Changes are expected after review.

FUJ00002566

1 Introduction

1.1 Information Security Definition

Information is an asset which, like other important business assets, has value to an organisation and consequently needs to be suitably protected. Information security protects information from a wide range of threats in order to safeguard customers and staff, ensure business continuity, minimise business damage and maximise operational efficiency.

Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Whatever forms the information takes, or means by which it is shared or stored, it should always be appropriately protected and is subject to the provisions of this policy document.

Information security is characterised here as the preservation of:

- ***Confidentiality***: ensuring that information is accessible only to those authorised to have access;
- ***Integrity*****:** safeguarding the accuracy and completeness of information and processing methods;
- ***Availability*****:** ensuring that authorised users have access to information and associated assets when required.

Information security is achieved by implementing a suitable set of countermeasures, including policies, practices, procedures, organisational structures and technical measures. Therefore by using an Information Security Management System (ISMS), this provides a systematic approach to managing sensitive company information so that it remains secure. It also encompasses people, processes and IT systems

1.2 Information Security Purpose

The purpose of Information Security Management is to provide an appropriate level of protection for information assets from relevant threats, whether internal or external, deliberate or accidental.

The implementation of this policy is important to maintain our integrity as a supplier of services to stakeholders and to support Post Office Ltd's (POL) Legal and Regulatory obligations with the parameters of Fujitsu's Contractual obligations.

1.3 Information Security Scope

This Information Security Policy specifies mandatory information security requirements to be applied throughout the Post Office Account (POA) in delivery of its contracted HNG-X Services to POL.

This Information Security Policy covers all activities undertaken by the POA in the provision of these services including design, development, integration, deployment, operation and support of services, as well as the programme management, stakeholder management, governance and administrative procedures applied by executive management to oversee those services.

1.3.1 Excluded from Scope

Information Security risks within POL sites that are outside of the scope of the Services provided by the POA are excluded from the scope of this Information Security Policy.

FUJ00002566

2 Information Security Approach

2.1 Implementation of Information Security

The POA implements and manages Information Security based upon security best practice as defined by Contractual obligations, including adherence to POL Information Security policies where stated in Contract, Fujitsu Corporate Policies and ISO/IEC27001:2005.

2.2 Fundamental Principles

It is the Policy of the Account to ensure that:

- Confidentiality of information will be maintained by protection against unauthorised access
- Integrity of information is assured through protection against unauthorised modification
- Information is available to authorised users when needed
- Regulatory and Legislative requirements will be met
- Information Security Risk Management will be implemented in accordance with Fujitsu Services Business Management System (BMS) Manage Risk Process and agreed Post Office processes.
- Information Security Training and Awareness will be provided to all staff

2.3 Senior Management Commitment to Information Security

POA Senior Management commitment to Information Security is demonstrated by:

- Approval of this POA Information Security Policy.
- Provision of resources and approval of roles and responsibilities for Information Security, including ensuring adequate skills and competencies.
- Support of Security communications and awareness activity.
- Provision of a senior level board, meeting quarterly, within the Account Governance structure to provide oversight of Information Security, including Information Security Risk Management escalations and approvals, internal audits and the sponsorship of management reviews.

2.4 Post Office Account Information Security Delivery Team

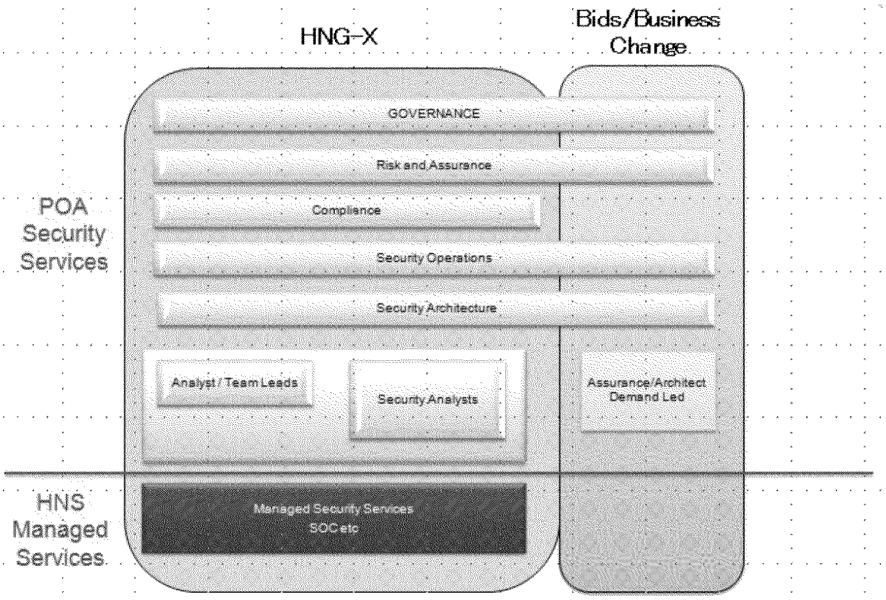
The POA Information Security Delivery Team is made up of a number of appropriately skilled and trained staff with responsibilities for the following functional security services:

- Governance
- Information Security Risk Management and Assurance
- Security Architecture
- Security Operations / PCI Compliance
- Security Analytical , Auditing and Operational services

FUJ00002566

These are further supported by Fujitsu managed security services provided by Security Services Business e.g. Security Operations Center (SOC).

The Security Services Operating Model is shown below:



Up to date Account Security contacts can be found on Page 16 within the current Account Organisation Chart.

3 Information Security Policy Statement

3.1 Executive Information Security Policy Statement

The Fujitsu Post Office Account will address Information Security based upon a clear understanding of Fujitsu Corporate Information Security Policies, Contractual Obligations and the Post Office Ltd's Information Security Policies and objectives.

The relevant Delivery Executives in each area of the account have ultimate responsibility for delivery of Information Security. They demonstrate commitment to Information Security through appointment of a senior accountable security lead and the required security resources, and through their approval of this Information Security Policy.

The Account will appoint a Chief Information Security Officer (CISO) as the focal point for Information Security, who has representation into the Post Office Account Senior Management Team as part of the Extended Leadership Teams, to provide a clear point of contact on all Information Security related matters. This CISO will be accountable for the delivery of Information Security (within the Information Security Scope) and will be supported by experienced Information Security specialists and technical staff.

It is the policy of the Account to take responsibility for the identification of Risks to Information Security arising through the activities it undertakes and the Services it provides within the scope defined within the applicable contracts.

The Account Information Security Team will work collaboratively with its customers to address Information Security concerns and appropriate controls will be implemented to manage

FUJ00002566

Information Security risks down to an acceptable level as determined through our Risk Management activities t in line with contractual obligations.

The Information Security controls and processes implemented and operated by the Account will be subject to Governance, Assurance and regular audit. It will be enhanced though a Continual Security Improvement Process founded upon reappraisals of risk and reviews of the effectiveness of the Information Security controls.

The Account will use proven methodologies in the development of the Information Security controls and will maintain appropriate records of the implementation of these using appropriate tools. In order to achieve this, the Account will ensure that necessary resources are provided for the management of Information Security.

3.2 Your Information Security Responsibilities

All Managers are responsible for ensuring employees, contractors, and any third parties, where they own relevant agreements, are aware of this Information Security Policy, adhere to the policies, and processes and follow appropriate guidance provided.

Key Contractual References and Information Security Policies to be aware of are:-

- Schedule A4 of the Contract
    - Paragraph 2.3, Data Protection Act
    - Paragraph 2.6, Security and Disclosure of Personal Data
    - Paragraph 4.1, Security Policy
    - Paragraph 7.1, Legal and Regulatory Controls
    - Paragraph 7.3, Security Organisation and Management
- POL Community Information Security Policy for Horizon and Horizon Online (Ref:- POL/HNG/CIS/001)
- Fujitsu Security Master Policy (Ref:- CPM 20)
- Fujitsu Legal Compliance (Ref:- CPM 6)
- Fujitsu Intellectual Property (Ref – CPM 21)
- Fujitsu Risk Policy (CPM 27)
- Fujitsu Data Protection (CPM 36)
- POA ISMS Manual (Ref:- SVM/SEC/MAN/0003)
- Fujitsu Conduct Guidelines (Ref:- NSN)

Every individual working in relation to the Account is required to be aware and understand these policies, processes, and guidance and to comply with them at all times.

All actual, suspected or potential information security incidents, breaches or other concerns and issues should be notified immediately to the relevant security managers. It is every individual's responsibility to ensure that Incident Management reporting obligations are fully complied with.

It is every individuals' responsibility to familiarise themselves with the relevant Information Security Management System (ISMS) manuals and supporting processes and guidance as necessary to conduct their own role and duties.

Individuals must actively support the Account Information Security Delivery Team in discharging all contractual and corporate obligations e.g. audit etc where requested.

FUJ00002566

3.3 Information Security Policy Compliance

Any individual failing to adhere to Fujitsu and Account Security Policies and associated security processes may be liable to disciplinary action in accordance with Fujitsu Conduct Guidelines.

This policy will be reviewed and re-issued on an annual basis at a minimum or whenever there is a material change to the organisation or delivery of security services.