FUJ00002073



| | |
|---|---|
| **Document Title:** | RMGA Information Security Policy |
| **Document Reference:** | SVM/SEC/POL/0003 |
| **Document Type:** | Policy |
| **Release:** | APPROVED |
| **Abstract:** | The Information Security Policy for the Royal Mail Group Account. This policy replaces all other security policies on the Account. |
| **Document Status:** | FOR APPROVAL<br>This document contains sections that have been identified to POL as comprising evidence to support the assessment of named Acceptance Criteria by Document Review. These sections must not be changed without authority from the FS Acceptance Manager |
| **Author & Dept:** | Howard Pritchard |
| **External Distribution:** | Sue Lowther |

## Approval Authorities:

| Name | Role | Signature | Date |
|---|---|---|---|
| Wendy Warham | RMGA Operational Director | | |
| Sue Lowther | Head of Information Security POL Ltd | | |

*Note: See Royal Mail Group Account HNG-X Reviewers/Approvers Role Matrix (PGM/DCM/ION/0001) for guidance.*

FUJ00002073



# 0 Document Control

## 0.1 Table of Contents

FUJ00002073

FUJ00002073

FUJ00002073

FUJ00002073

FUJ00002073



## 0.2 Document History

| Version No. | Date | Summary of Changes and Reason for Issue | Associated Change - CP/PEAK/PPRR Reference |
|---|---|---|---|
| 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 RMGA 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.<br>This text must not be changed without authority from the FS Acceptance Manager.<br>This version will not require full review using the RMGA 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 | |

## 0.3 Review Details

| | |
|---|---|
| Review Comments by : | 28 Oct 2008 |
| Review Comments to : | Brian Pinder & Howard Pritchard & RMGADocumentManagement GRO |
| Mandatory Review | |
| Role | Name |

FUJ00002073



| | |
|---|---|
| Programme Assurance Manager | Jan Holmes |
| Commercial Manager | Hilary Forrest |
| Business Continuity Manager | Tony Wicks |
| HR Manager | Sarah Bampton |
| RMGA Quality Manager | Nigel Hatcher |
| Optional Review | |
| Role | Name |
| Chief Information Security Officer | Howard Pritchard |
| Information Governance Team | Brian Pinder |
| Operational Security Manager | Pete Sewell |
| Operations Director | Wendy Warham |
| Head of Information Security POL Ltd | Sue Lowther |
| Key Management | Peter Ambrose |
| Issued for Information – Please restrict this distribution list to a minimum | |
| Position/Role | Name |
| Acceptance Manager | David Cooke |
| | |

( * ) = Reviewers that returned comments

## 0.4 Acceptance by Document Review

The sections in this document that have been identified to POL as comprising evidence to support Acceptance by Document review (DR) are listed below for the relevant Requirements:

| POL NFR Acceptance Ref | Document Section Number | Document Section Heading |
|---|---|---|
| SEC-3110 | 11.4 | Network Access Control |
| SEC-3092 | 2 | Information Security Policy Development |
| SEC-3095 | 13 | Information Security |
| SEC-3102 | 6.2.3 | Addressing Security in Third Party Agreements |
| SEC-3104 | 6.2.3 | Addressing Security in Third Party Agreements |
| SEC-3166 | 10.6 | Network Security Management |
| SEC-3189 | 10.6.1 | Network Controls |
| SEC-3203 | 11 | Access Control |
| SEC-3241 | 6.2 | External Parties |
| SEC-3241 | 15.1 | Compliance with legal requirements |
| SEC-3255 | 8.1.2 | Screening |

FUJ00002073



## 0.5 Associated Documents (Internal & External)

| Reference | Version | Date | Title | Source |
|---|---|---|---|---|
| PGM/DCM/TEM/0001 (DO NOT REMOVE) | 2.0 | 16-Apr-07 | (Document Title) | Cafe Vik |
| BSO ISO IEC 27001 – 2005 | | | Information Technology Security Techniques – Information Security Management System requirements | Dimensions |
| RMPOL002 | 1.0 | 8-Jun-05 | Community Information Security Policy for Horizon | PVCS |
| CPM34 | | | Fujitsu Services Manage Information Security Policy | CafeVik |
| CPM20 | | | Fujitsu Services Security Master Policy | CafeVik |
| RSPOL02 | 12 | 5-Apr-07 | Fujitsu Services Horizon Security Policy | Dimensions |
| SVMSECSTD0006 | | | RMGA Information Security Risk Management Approach. | Dimensions |
| SVMSECMAN0001 | | | Statement of Applicability | Dimensions |
| SVMSECPLA0001 | | | Risk Treatment Plan | Dimensions |
| SVMSECSTD0027 | | | RMGA Information Security Management Review Board Terms of Reference | Dimensions |
| SVMSECSTD0026 | | | RMGA CISO Terms of Reference | Dimensions |
| CSRRD019 | | | RMGA Customer Service Operational Change Process | PVCS |
| ITS2 | | | Operational Use of IT & Communications Systems | CafeVik |
| ITS3 | | | Use of Email and Internet Systems | CafeVik |
| ITS8 | | | Classifications and Privacy Markings | CafeVik |
| HRS1 | | | Security Checking in HR Shared Services Processes | CafeVik |
| RSPRO002 | | | RMGA Security Vetting Process | Dimensions |
| SVMSECSTG0001 | | | Fujitsu Services RMGA Information Security Communications Strategy | Dimensions |
| CS2 | | | Identification Cards and Physical Access Control | CafeVik |

FUJ00002073



| | | | | |
|---|---|---|---|---|
| ISN/001377 | | | Fujitsu Services Data Centre Security Policies | |
| ARCSECARC0003 | | | HNG-x Technical Security Architecture | Dimensions |
| SDMSVNMAN0027 | | | Horizon Access Controls Guidelines Joint Working Document | Dimensions |
| TBC | | | HNG-x Access Controls Guidelines Joint Working Document | Dimensions |
| ITS2.1 | | | Minimum Password Security | CafeVik |
| ITS9 | | | Security of Portable Equipment | CafeVik |
| ARCSECARC0001 | 2.0 | 07/06/07 | Security Constraints | Dimensions |
| CSPRO018 | | | RMGA Customer Service Incident Management Process | Dimensions |
| CRFSP006 | | | Audit Trail Functional Specification | Dimensions |
| RSPOL010 | | | Vulnerability and Risk Management Policy | PVCS |
| RSPRO047 | | | OOH Password Changing Process | Dimensions |
| SVMSDMPLA0002 | | | HNG-X Services Business Continuity Plan | Dimensions |
| SVMSDMPLA0003 | | | HNG-X Support Services Business Continuity Plan | Dimensions |
| Schedule 4 of the Agreement | | | Handling PCI Sensitive Authentication Data and Card holder Data | Dimensions |
| SVMSDMSD0007 | | | Service Management Service Description | Dimensions |
| Schedule S3 | | | Post Office Ltd Document | |
| CSOLA05152 & 53 | | | RMGA Network Banking Key Management | PVCS |
| RSPRO013 | | | Horizon Security Pass Procedure | PVCS |
| COMMGTREP0001 | | | Transfer Asset Register | Dimensions |
| PGMPASPLA0014 | | | Intergrated Audit Schedule | Dimensions |

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

## 0.6 Abbreviations

FUJ00002073



| Abbreviation | Definition |
|---|---|
| CA | Certificate Authority |
| GSA | Government Specified Algorithm |
| CISO | Chief Information Security Officer |
| CISP | Community Information Security Policy |
| CPNI | Centre for the Protection of National Infrastructure |
| DMZ | In computer networking, De-Militarised Zone (DMZ) is a firewall configuration for securing Local Area Networks (LAN) |
| CHAP | Challenge Handshake Authentication Protocol |
| COTS | Commercial Off The Shelf |
| DSA | Digital Signature Algorithm |
| EPOSS | Electronic Point of Sale System |
| IA | Information Assurance |
| ISMS | Information Security Management System |
| ISMR | RMGA Information Security Management Review Board |
| KEK | Key Encryption Keys |
| LAN | Local Area Networks |
| NBS | Network Banking Service |
| NDA | Non-Disclosure Agreement |
| OBC | Order Book Control |
| OED | Oxford English Dictionary |
| OOH | Out of Hours |
| PIN | Personal Identification Number |
| POL | Post Office Limited |
| RMG | Royal Mail Group |
| RMGA | Fujitsu Services Royal Mail Group Account |
| RTP | Risk Treatment Plan |
| SMDB | Service Management Database |
| SOA | Statement of Applicability |
| VPN | Virtual Private Network |
| WAN | Wide Area Network |
| PCISS | Payment Card Industry Security Standard |
| PCIDSS | Payment Card Industry Data Security Standard |

## 0.7 Glossary

FUJ00002073



| Term | Definition |
|---|---|
| Sensitive Authentication Data | means security related information used to authenticate cardholders appearing in plain text or otherwise unprotected form. This information can be any of the following:<br>• Card Validation Code<br>• Card Validation Value<br>• Full Track<br>• PINs<br>• PIN blocks (including encrypted PIN blocks<br>For the latest and most up to date definition, please refer to schedule 1 of the Agreement. |
| Cardholder Data | means the PAN or the PAN plus any of the following:<br>- cardholder name<br>- expiration date<br>- Service Code<br>- start date<br>- issue number;<br>For the latest and most up to date definition, please refer to schedule 1 of the Agreement. |
| Personal Data | means all data which are defined as personal data in the Data Protection Act 1998 and processed by Fujitsu Services under this Agreement;<br>For the latest and most up to date definition, please refer to schedule 1 of the Agreement |
| Sensitive<br>(As used within this document) | on it's own for example as used in 'sensitive information' or 'potentially sensitive' means something which may be personal or private or contain personal or private information or information which may be confidential |
| Shall/Should/Will | OED defines shall as "expressing a strong assertion or command". In a usage note the OED states that traditionally will is used for the 1st person singular and plural and shall for 2nd and 3rd persons but that it is now fully acceptable to interchange these. Shall and will are used interchangeably and this is acceptable .For the most part should is used to form a conditional close, |
| Subcontractor | One (as an individual or business) that contracts to perform part or all of the obligations of another's primary contract |
| ISMS | Information Security Management System:<br>that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and |

FUJ00002073



| | |
|---|---|
| | improve information security<br>NOTE: The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources. |
| Third Parties | As described within this document and the ISMS, include those parties contracted by RMGA to help them deliver the Service to POL e.g. to assist with maintenance, provide equipment and software, provide services such as cleaning, site security and recruitment, |
| RMGA Information | : All POL information / data held /stored within the RMG Account. |

## 0.8 Changes Expected

| Changes |
|---|
| Audit trail Functional Specification. |
| Further amendments to Policy with regards agreed Medium and Low comments once Policy formally approved. |
| At least Annual Review of Policy with POL. |
| Review against POL CISP, Regulatory, ISO and PCI standards. |

## 0.9 Accuracy

Fujitsu Services endeavours to ensure that the information contained in this document is correct but, whilst every effort is made to ensure the accuracy of such information, it accepts no liability for any loss (however caused) sustained as a result of any error or omission in the same.

## 0.10 Copyright

FUJ00002073



# 1 Introduction

## 1.1 Context

This policy is applicable to the Fujitsu Services Royal Mail Group Account (RMGA). For the purpose of this document, the terms Fujitsu Services Royal Mail Group Account or Fujitsu Services Royal Mail Group Account Staff shall (unless indicated otherwise) include all employees and contractors engaged by Fujitsu Services and its subcontractors to the extent to which their activities are relevant to the delivery of Services.

Section 5 of this document sets out the Executive Information Security Policy Statement for the RMGA which, together with the Framework of Controls in sections 6 to 15 (collectively the Information Security Policy) satisfy the contractual requirement for an ISO/IEC27001:2005 based Information Security Policy.

This policy complies with Post Office Limited's (POL) Community Information Security Policy for Horizon (CISP) (Ref: RMPOL002CISP); Fujitsu Services Manage Information Security Policy (Ref: CPM34); and Fujitsu Services Security Master Policy (Ref: CPM20).

# 2 Information Security Policy Development

This information security policy has been developed and works in parallel with the Fujitsu Services Horizon Security Policy version 12 (ref: RSPOL02) and it has been updated to reflect the provision of the HNG-x Service as well as being structured in accordance with ISO/IEC27001:2005.

Although the organisational and management policy statements contained within this policy will apply to the whole of RMGA, the technology and operational control statements are based upon requirements for Services provided to POL. It is likely that this policy will be updated at its next review to include relevant statements for Services provided to Royal Mail Group (RMG).

## 2.1 Purpose

The policy applies to all RMGA Staff and is mandatory. Failure to comply with the policy will be regarded as a disciplinary issue and may result in disciplinary action.

This Information Security Policy sets out management direction and support for information security, along with minimum standards to be met by RMGA, consistent with ISO/IEC27001:2005, contractual commitments and relevant POL requirements as expressed in CISP (Ref No 16).

This Information Security Policy:

- Provides a statement of executive commitment and support for information security;
- Provides a framework of controls within which the Services will be developed, implemented and delivered by RMGA in all areas of its business;
- Identifies the information security awareness and education requirements for all RMGA Staff;
- Outlines the requirements for business continuity management as related to information security;

FUJ00002073



- Describes the compliance, audit and management arrangements over information security and the action that may be taken should this policy not be followed; and
- Allocates information security responsibilities.

## 2.2 Information Security

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

# 3 Scope

## 3.1 Statement of Scope

This Information Security Policy specifies mandatory information security requirements to be applied throughout RMGA in the provision of its Services to Post Office Limited. The scope of this policy includes Horizon and HNG-x. Internal Management Systems and Internal Support Systems are also covered by this policy.

This Information Security Policy covers all activities undertaken by RMGA in the provision of these Services including design, development, 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.

This Information Security Policy document describes the overall strategy for providing information security and is based best practice as defined by ISO/IEC27001:2005.

Information security risks within Post Office sites that are outside of the scope of the Services provided by RMGA are excluded from the scope of this Information Security Policy.

# 4 Information Security Risk Assessment

FUJ00002073



The objectives of effective information security risk management are:

- To facilitate the overall management of security risk for Information Systems and IT related equipment, networks and applications for RMGA;
- To generate and maintain an accurate and current Information Security Risk Register for information assets which support The Service;
- To create and maintain a Statement of Applicability; and
- To provide appropriate management information in relation to Information Security risk and ensure that this is co-ordinated with the RMGA Business Risk management process.

## 4.1 Information Security Risk Assessment Approach

Risk Assessment will form a key component of the RMGA Information Security Management System (ISMS).

A formal information security risk assessment methodology will be adopted that is suited to the RMGA ISMS, and the identified business information security, legal and regulatory requirements. The risk assessment methodology will be selected by the Fujitsu Services RMGA Chief Information Security Officer (CISO) and shall ensure that risk assessments produce comparable and reproducible results. Full details of the risk assessment methodology can be found in RMGA Information Security Risk Management Approach (Ref: SVM/SEC/STD/0006)

The RMGA CISO will establish criteria for the management of information security risk. In addition to security risk management and containment, there will be criteria for accepting risks and identifying the acceptable levels of risk and these will be maintained and reviewed at regular intervals. Security risk acceptance criteria will be developed in accordance with the RMGA Business Risk management process.

Risk Assessments will be conducted on a regular, at least annual, basis and additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks.

Information assets, within the scope of the ISMS, will be identified and recorded along with the owners of these assets. The asset 'owners' will participate in information security risk assessments conducted by, or on behalf of, the Chief Information Security Officer.

The RMGA CISO will establish and maintain an information security risk register and will produce a Statement of Applicability (Ref: SVM/SEC/MAN/0001) which will define the controls which must be implemented for all areas of the RMGA lifecycle management, in accordance with the Information Security Policy, and in compliance with ISO/IEC27001:2005.

Fujitsu Services will work with the customer, where appropriate, to agree appropriate countermeasures commensurate with the value and nature of the business risk. The risk acceptance criteria need to be agreed with Post Office Limited.

All identified information security risks will be recorded in the RMGA information security risk register and those which require further mitigation will be recorded in a Risk Treatment Plan (RTP) (Ref: SVMSECPLA0001) which will include planned mitigation actions and next review dates. Risk treatment criteria must be agreed by the RMGA Information Security Review Board, and documented in the risk treatment plan. It may also be appropriate for recorded information security risks to be incorporated into corporate, business or project risk registers. The risk treatment plan may be used by internal auditors or IA inspection and feeds into the Statement of Applicability (SOA) for ISO/IEC27001:2005 auditors.

Traceability, based on the outputs of the risk management process, is needed to ensure that RMGA can determine why a given risk management decision was taken, and the RTP should be able to demonstrate the following:

FUJ00002073



- The cost and effects of each countermeasure is justified by the severity of the risk it addresses;
- A proper risk management decision has been taken for each risk;
- Each risk selected to be mitigated is properly addressed by one or more countermeasures;
- Responsibility for implementing each countermeasure is properly allocated;
- Each operating procedure implements a countermeasure efficiently and effectively.

# 5 Information Security Policy

## 5.1 Executive Statement

### 5.1.1 Executive Information Security Policy Statement

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.

It is the policy of the Fujitsu Services RMG 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 its contracts, and for the implementation and operation of appropriate countermeasures to manage those risks down to an acceptable level as determined by specialists within the Fujitsu Services RMG Account, best practice and in line with POL contractual requirements

It is the policy of the Fujitsu Services RMG Account to carry out these obligations in a manner that aligns with customer measures put in place in respect of wider Information Security risks and to work collaboratively with the customer to address information security concerns. To facilitate this, the RMG Account Information Security Policy incorporates relevant requirements from the Community Information Security Policy.

The Fujitsu Services RMG Account will present to the customer a focal point for information security matters, with representation at senior levels and to provide a clear point of contact on all information security related matters. This named security representative will be responsible for the delivery of Fujitsu Services Manage Information Security process and for establishing an Information Security Management System (ISMS) in accordance with the standards defined in ISO/IEC27001:2005 and will be supported by experienced specialists and technical staff with specific expertise in the areas of IT security and risk management.

The Fujitsu Services RMG Account Director has ultimate responsibility for security. A commitment to information security will be communicated throughout the Fujitsu Services RMG Account and any sub-contractors, and will be evidenced by Senior Management Team approval of the Fujitsu Services RMG Account Information Security Policy.

All line managers are responsible for ensuring all employees, contractors, and any third parties, where they own relevant agreements, are aware of this policy.

FUJ00002073



All RMGA Staff are required to be aware of policy details and to comply with these at all times.

Local Site Managers have responsibility for physical security at all sites used by Royal Mail Group Account. Physical security will be subject to checks by the RMGA Operational Security Manager.

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

The Fujitsu Services RMG Account will address information security based upon a clear understanding of the customer's information security objectives, a comprehensive analysis of risks to information security and a suite of properly aligned and managed Countermeasures in the areas of:

- Organising information security;
- Asset management;
- Human resources;
- Physical and environmental security;
- Communications and operational management;
- Access controls;
- Information systems acquisition, development and maintenance;
- Information Security Incident Management
- Business Continuity Management
- Compliance

The controls and control objectives for each of the areas identified above must be documented and supported by specific, documented policies and procedures. This must include the reasons for their selection and the justification for any controls which are excluded.

The information security countermeasures and practices implemented and operated by the Fujitsu Services RMG Account will be subject to internal governance arrangements and enhanced though a continual improvement process, founded upon reappraisals of risk, reviews of emerging best practice and reviews of the effectiveness of information security countermeasures. Regular reports on the effectiveness of countermeasures will be produced. By providing appropriate levels of assurance, both within Fujitsu and to the customer, information security will become an enabler for effective information sharing.

The Fujitsu Services RMG Account will use proven tools and methodologies in the development of the information security countermeasures and will maintain appropriate records of the implementation of these countermeasures. In order to achieve this, the RMGA Account Director will ensure that appropriate resources are provided for the management of information security.

This Fujitsu Services RMG Account Information Security Policy has been reviewed by the management of the Fujitsu Services RMG Account and approved by the Fujitsu Services RMG Operational Director, published and communicated, as appropriate, to all members of the Fujitsu Services RMG Account and its key subcontractors.

FUJ00002073



### 5.1.2 Information Security Policy Implementation

All users of Fujitsu Services and RMGA systems, supporting networks and applications which provide The Service must be aware of these policy details and comply with these at all times.

Compliance at all levels of RMGA is mandatory and any breach arising through deliberate action or lack of an acceptable standard of care and attention may result in disciplinary action being taken.

### 5.1.3 Review of Information Security Policy

This policy is owned by the Fujitsu Services RMG Account Chief Information Security Officer (CISO) who is responsible for its maintenance and review. It is approved by the Fujitsu Services RMG Account Director.

This policy document will be formally reviewed at least annually, after major changes to the scope of services and after any significant security incident or occurrence of fraud. The policy will be updated whenever necessary to reflect the needs and obligations of the Fujitsu Services RMG Account and developments in relevant best practice. The annual review will include a review of effectiveness, impact of the policy on the business and the effect of technology changes on the policy.

# 6 Organising Information Security

## 6.1 RMGA Internal Information Security Organisation

A summary of management responsibilities is included in this document for clarity.

### 6.1.1 Management Commitment to Information Security

Information Security is seen as a core responsibility of the Fujitsu Services RMG Account and executive sponsorship ensures that:

- The RMGA allocates sufficient expert resource to address its Information Security obligations; and
- RMGA participates fully in customer meetings and workshops responsible for information exchange, the advancement of best practice definition and communication;

RMGA will take steps to ensure that all of its Services are delivered from a standpoint of compliance with this Policy, through endorsement by executive management and a culture of intolerance of non-adherence. This will be reinforced through a training and appraisal process for all RMGA staff

### 6.1.2 Information Security Co-ordination

#### 6.1.2.1 RMGA Information Security Management Review Board

There shall be an RMGA Information Security Management Review Board (ISMR) chaired by the RMGA Operations Director.

Members of the ISMR shall include all relevant areas of the Fujitsu Services RMG Account and will be detailed within the Terms of Reference (SVM/SEC/STD/0027).

FUJ00002073



The board shall meet at intervals not exceeding 6 months.

The Terms of Reference will be formally documented.

This ISMR will manage communication and reporting to the Customer Information Security Management Forum.

Whenever necessary, the ISMR can commission independent specialists to undertake studies, investigations or audits.

#### 6.1.2.2 Customer Information Security Management Forum

RMGA will send appropriate representation to the Customer Information Security Management Forum which shall operate in accordance with terms of reference agreed between both parties.

### 6.1.3 Allocation of Information Security Responsibilities

The Fujitsu Services RMG Account Director has ultimate responsibility for security. A commitment to information security will be communicated throughout RMGA and any sub-contractors, and will be evidenced by Senior Management Team approval of the Fujitsu Services RMGA Information Security Policy.

Senior management is supported by experienced specialists and technical staff with specific expertise in the areas of IT security and risk management.

All line managers are responsible for ensuring all employees, contractors, and any third parties, where they own relevant agreements, are aware of policies.

All RMGA Staff are required to be aware of policy details and to comply with these at all times.

Local Site Managers have responsibility for physical security at all sites used by RMGA. Physical security will be subject to checks by the RMGA Operational Security Manager.

At Post Office outlets, the Post Office Manager has particular responsibility for safeguarding the Royal Mail Group Account equipment installed

**The key Fujitsu Services RMG Account Security responsibilities are as follows:**

**RMG Account Director**

The information security-related responsibilities of the RMG Account Director include:

- Overall control and management of information security throughout RMGA;
- Provision of adequate resources for information security;
- Appointing an experienced security professional responsible for managing and coordinating security across the complete RMGA domain.
- Approval authority for the Fujitsu Services RMGA Information Security Policy;
- Establishing the information security interface with the customer; and
- Establishing the information security interface with all Fujitsu Services subcontractors

**RMGA Programme Director**

The information security-related responsibilities of the RMGA Programme Director include:

FUJ00002073



- Ensuring that responsibilities and procedures for the management and operation of all information processing facilities are established, documented and maintained;
- Ensuring that changes to information processing facilities and systems are controlled; and
- Overall control of risk management and audit functions, including deciding the criteria for accepting risks and the acceptable levels of risk;

**RMGA Quality Manager**

The information security-related responsibilities of the RMGA Audit Manager include:

- Co-ordinating all audit related activities;
- Providing a point of contact for external audit personnel;
- Planning and carrying out audits of Royal Mail Group Account's business functions,
- Maintaining an integrated audit plan / schedule

**RMGA Operations Director**

The information security-related responsibilities of the RMGA Operations Director include:

- Sponsorship of the Chief Information Security Officer; (CISO);
- Ownership and overall control and management of operational security throughout RMGA;
- Day to day management of security related risks;
- Chairing the RMGA Information Security Management Review Board; and
- Acting as the approval authority for RMGA Security Procedures,

**Chief Information Security Officer (CISO)**

The CISO is responsible for the overall design of the RMGA security control framework. The CISO will lead the engagement with customer stakeholders with an interest in governance, control and security matters. The CISO will ensure the responsibilities of the Information Governance and Operational Security Teams are met. Full details are contained within the RMGA CISO Terms of Reference (Ref SVM/SEC/STD/0026) and include

- Developing and publishing all security-related policies and guidelines applicable at RMGA level;
- Reviewing and approving information security policies and procedures owned and implemented at business level;
- Ensuring that security incidents are recorded and investigated,
- Providing a point of contact for POL Head of Information Security,
- Monitoring for compliance with RMGA Information Security Policy,
- Ensuring all RMGA Staff are screened in line with contractual requirements, FS Group Policy and this policy.
- Ensuring that security relevant events are recorded,
- Ensuring that system audit trails and logs are analysed on a regular basis,
- Defining the information security risk assessment approach of RMGA:
- Analysis and evaluation of information security risks and evaluating options for the treatment of risks:
- Co-ordinating the implementation and operation of the Information Security Management System.

FUJ00002073



- Liase with the Quality Manager to organise Security Audits

**Operational Security Manager**

- The management of security incidents.
- The provision of event auditing services.
- Impact assessment, authorisation and approval for all operational and system design changes to ensure the implementation of security controls in technology and processes.
- Ensuring the physical security of Fujitsu Services sites where the RMG Account is located.
- Co-ordinating the evaluation of all new security products proposed.
- Providing regular operational reporting on activities and status.

### 6.1.4 Authorisation Process for Information Processing Facilities

The installation of Information Processing facilities will be technically reviewed by competent personnel, and approved and authorised by appropriate staff as documented in the RMGA Operational Change Process. This process ensures that no changes can be made to hardware, software or documentation that could impact on information security without being correctly authorised. This process including all configuration requirements is managed by the RMGA Change Control Team.

### 6.1.5 Confidentiality Agreements

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

Terms of reference for Fujitsu Services staff including those on variable length assignments must include the requirement to comply with RMGA Information Security Policies.

### 6.1.6 Contact with Authorities

RMGA will co-operate with external organisations through established Fujitsu Services channels. This will require the CISO to maintain contact with the Fujitsu Services teams responsible:

- Contact with law enforcement authorities, government vetting agencies and CPNI will be maintained by Fujitsu Services Group Security.
- Contact with regulatory bodies and the Information Commissioner will be maintained by Fujitsu Services Group Legal.

### 6.1.7 Contact with Special Interest Groups

General contact with special interest groups, information service providers, telecommunications operators, user groups and best practice organisations will be maintained by Fujitsu Services RMGA Security Team.

FUJ00002073



### 6.1.8 Independent Review of Information Security

All areas of information security are subject to regular reviews, as arranged by the RMGA CISO, to ensure compliance with security policy control objectives, controls, policies, processes and procedures for information security.

Regular reviews of implementation will be conducted by the RMGA CISO as part of an integrated audit plan. Additional independent reviews will be conducted by Fujitsu Services Business Assurance team and by the Manage Information Security Process Champion.

RMGA will seek registration to ISO27001 for its Information Security Management System and this will provide an independent assurance, to the RMGA management team and the customer, that information security is effectively managed.

## 6.2 External Parties

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

### 6.2.1 Identification of Risks Relating to External Parties

The risks associated with access to RMGA information and information processing facilities by third parties will be assessed and appropriate security controls implemented. These controls must be agreed, documented and defined in agreements with any external parties.

Physical access to any RMGA processing facilities provided by Fujitsu Services shall not be provided to third parties until all security requirements have been satisfied and evidence recorded.

RMGA will create and maintain a register of external parties with connections to Services provided to POL.

### 6.2.2 Addressing Security when Dealing with Customers

Any customer access to RMGA information will be subject to the requirements of this Information Security Policy.

### 6.2.3 Addressing Security in Third Party Agreements

Suppliers of goods and services must be subject to formal agreements in support of this security policy. Individual agreements with suppliers of standard COTS components are not required provided that there is clear evidence the components meet all security regulatory and contractual requirements relevant to the component.

# 7 Asset Management

## 7.1 Responsibility for Assets

FUJ00002073



### 7.1.1 Inventory of Assets

Asset identification and recording is a key aspect of security management. Information assets form the basis of business impact assessment and security risk management. RMGA must record all important assets needed to perform the HNG-x Service.

The RMGA asset inventory or register (register ref COMMGTREP0001) must hold the following information as a minimum:-

- The asset name, location and high level description, including security classification
- The asset Owner

A consistent approach to asset valuation will be adopted for RMGA information assets depending on the class of asset and an impact assessment.

### 7.1.2 Ownership of Assets

All assets issued as part of the RMGA HNG-x programme will be assigned an owner, who will be responsible for the asset. The owner may be a team, rather than an individual. Details of ownership will be documented in the inventory of assets which will be reviewed on a regular basis to ensure its accuracy.

### 7.1.3 Acceptable Use of Assets

All personnel using Fujitsu Services corporate systems will be subject to the corporate acceptable use policies:

- Operational Use of IT & Communications Systems (Ref: ITS2)
- Use of Email and Internet Systems (Ref: ITS3)

## 7.2 Information Classification

### 7.2.1 Classification Guidelines

All information concerning Post Office Limited and its contracted services, that are not in the public domain, shall be considered potentially sensitive and by default treated as private to POL and its contractors.

Fujitsu Services has a formal approach to information classification and has a published policy on Classifications and Privacy Markings (Ref: ITS8).

Current Fujitsu Services approved classifications are:

- COMPANY SECRET
- COMPANY RESTRICTED
- COMMERCIAL IN CONFIDENCE
- Xx EYES ONLY
- UNCLASSIFIED

* Xx**... EYES ONLY** is prefixed by additional qualifiers, some of which may be business specific.

FUJ00002073



Current RMG and POL approved classifications are:

- PUBLIC
- INTERNAL
- CONFIDENTIAL
- STRICTLY CONFIDENTIAL

## 7.2.2 Information Labeling and Handling

Classifications and Privacy Markings (Ref: ITS8) contains detailed guidance on labelling and handling information. For ease of reference a table is supplied at Appendix A. If in any doubt advice should be sought from the RMGA CISO.

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

RMGA information, which supports delivery of the Service, that requires protection from unauthorised access (whilst not exhaustive) includes for example:

- The business data exchanged with Post Office Ltd. and its clients (e.g. reference data to support EPOSS and transaction data resulting from Post Office counter activities.)
  Business data is transferred between Post Office Ltd., Post Office Ltd. Clients and the RMGA Data Centres and between the Data Centres and the Post Office branches. It is stored at the main operation systems and also in archives. Some data is also available for management services via the SMDB. **RMGA Classification: Company Restricted. POL Classification: PO Confidential**
- RMGA business management data - financials, service level agreements etc. Confidentiality and integrity requirements exist for much of this data. The Management Information System collects this data from the operational systems. This is then forwarded as appropriate to RMGA sites, Post Office Ltd. and their Clients. **RMGA Classification: Commercial in Confidence. POL Classification: INTERNAL - the inclusion of any personal data(as defined by the Data Protection Act) in this category, escaulates the POL classification to Confidential**
- Information contained in documents exchanged between RMGA and POL in the course of normal business communications. **RMGA Classification: Commercial in Confidence. POL Classification: INTERNAL -** detailing security breaches or potential security breaches, escalates the POL classification to confidential.
- Other data supporting the business processes such as training data (special, non-sensitive, business style data used in training sessions) and on-line documentation (e.g. Post Office procedures.) **RMGA Classification: Fujitsu Eyes Only or Commercial in Confidence. POL Classification: Internal**
- Operational systems data such as the software, configuration information, Tivoli scripts, system management event logs etc. This information must be held in Dimensions Document Management and associated configuration management servers and is subject to change management access controls. **RMGA Classification: Company Restricted. POL Classification: PO Confidential**
- Security information about users, Sensitive personal data, details of security investigations, keys, security audit logs etc. **RMGA Classification: Company Secret. POL Classification: Strictly Confidential**

FUJ00002073



- **In addition, POL have specific requirements for the handling of Cardholder Data and Sensitive Authentication Data (see Glossary for definition):**
  - Sensitive Authentication Data shall 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 shall also be deleted after use. Exceptionally, any data element required to be submitted in the settlement or reconciliation files may be retained for a configurable number of days after the file is successfully submitted as defined in Schedules 1 and A4.
  - Cardholder Data shall be rendered unreadable anywhere it is stored (including data on portable media, backup media, and in logs) by using any of the following approaches: 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.
  - All Sensitive Authentication Data and Cardholder Data shall be encrypted using approved algorithms and encryption protocols whilst in transit over any public network. 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. In all other respects Sentive Authentication data and cardholder data must be treated as POL Confidential: **RMGA Company Restricted**
  - Any exceptions to these policy requirements will be specifically agreed in writing in the document entitled "Security Constraints" (ARC/SEC/ARC/0001).
  - All Post Office Limited documents are classified as INTERNAL unless otherwise marked.

# 8 Human Resources

The objectives of this policy section are to ensure that all RMGA employees, contractors and third party users understand their roles, responsibilities and obligations for security; that all RMGA Staff are suitably screened for the roles they occupy in order to reduce the risk of theft, fraud or misuse of RMGA computing facilities; to ensure that employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support RMGA security policy in the course of their normal work, and to reduce the risk of human error; to ensure that security matters are dealt with in an orderly manner for employees, contractors and third party users on exit or transfer out of RMGA.

All Fujitsu Services Staff are subject to the FS corporate human resources policies which are administered as a shared service function across Fujitsu Services including the addressing of policy requirements for the employment of contract and third party staff working for RMGA.

## 8.1 Prior to Employment

### 8.1.1 Roles and Responsibilities

Where RMGA Staff have specific information security responsibilities these will be defined in documented job descriptions. Generic security responsibilities for all staff will be included in all role descriptions or objectives for the appropriate professional community.

### 8.1.2 Screening

FUJ00002073



All applications for employment shall be screened in order to assess reliability. Applicants' identities and references are to be checked as stated in the Fujitsu Services Policy Security Checking in HR Shared Services Processes (Ref: HRS1). Equivalent checks will be applied to all subcontractor staff, as appropriate.

Requirements for further pre-employment checks for RMGA Staff are outlined below. It is the responsibility of the hiring manager to ensure that employees have the appropriate level of security for their role.

- Additional security checks, in accordance with POL vetting procedures, must be performed for all RMGA engineer staff who require access to Post Office branches in order to undertake development, support or maintenance activities. Full details can be found in RMGA Horizon Security Pass Procedure (Ref: RSPRO013).
- Satisfactory Credit Reference Bureau checks will be required for all RMGA Staff who have access to financial information contained within Post Office systems.
- Criminal Record Checks will be carried out on RMGA staff where legally permitted
- UK Security Clearance may be required for individuals who have access to POL information classified as Strictly Confidential. Advice should be sought from the Chief Information Security Officer who will confirm the requirement with POL on a case by case basis.

### 8.1.3 Terms and Conditions of Employment

As part of their contractual obligation, employees, contractors and third party users must agree the terms and conditions of their employment contract, which must state their and RMGA responsibilities for information security.

## 8.2 During Employment

### 8.2.1 Management Responsibilities

All Managers must ensure that RMGA Staff apply security in accordance with agreed POL & FS policies and procedures. They must ensure that RMGA Staff are properly briefed and comply with the terms and conditions of their employment and this Information Security Policy.

### 8.2.2 Information Security Education and Training

All Fujitsu Services RMG Account employees and, where relevant, third party users, will receive appropriate training and regular updates in organisational policies and procedures. The security awareness, education, and training activities will be suitable and relevant to the person's role, responsibilities and skills, and will include information on known threats, security requirements, legal responsibilities and business controls, who to contact for further security advice and the proper channels for reporting information security incidents. This will also include the requirement for all staff when sent various policies or briefings to acknowledge that they have read and understood them.

The Information Security Policy will be refreshed, at least, annually and changes cascaded to all RMGA Staff.

FUJ00002073



The Fujitsu Services RMGA Information Security Communications Strategy (Ref: SVMSECSTG0001) will promote information security awareness and explain the importance and use of information security controls. This includes information security training as part of Fujitsu Services RMGA induction courses for new

Policy documents must be readily available to all staff; this may be achieved by publishing through the RMGA community portal.

### 8.2.3 Disciplinary Process

Any member of RMGA Staff (Fujitsu Services and Subcontractors) failing to adhere to this Information Security Policy, associated Procedures and instructions may render themselves liable to disciplinary action in accordance with the disciplinary code of the organisation responsible for their conduct

Detailed guidance, and support, on the application of these processes can be obtained from the RMGA HR Manager.

## 8.3 Termination Responsibilities

### 8.3.1 Termination Responsibilities

When a member of RMGA Staff exits or transfers from the programme it is the line manager's responsibility to ensure that all assets, both information assets and software and hardware assets are reviewed and returned and that access rights are reviewed and where applicable revoked or adjusted upon change.

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

### 8.3.2 Return of Assets

All RMGA Staff must return all of RMGA Assets in their possession upon termination of their employment, contract or agreement.

When an RMGA Staff member leaves or is reassigned Line managers must follow formal HR procedures to ensure the return of all RMGA property where applicable. This will include return of all RMGA equipment and software licences. The line manager must ensure that any RMGA data which is held on personally allocated computers is removed

### 8.3.3 Removal of Access Rights

The access rights of all RMGA Staff to information and information processing facilities must be removed upon termination of their employment contract or agreement or adjusted upon change of assignment or role, including revoking their rights to the system and escorting them from RMGA premises.

Where RMGA Staff move within the RMGA, computer access must be modified or terminated as appropriate to their change of role.

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

FUJ00002073



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

# 9 Physical and Environmental Security

The objectives of this policy section are to ensure that all RMGA Staff, contractors and third party users understand their roles, responsibilities and obligations for physical and environmental security and to prevent unauthorised access damage and interference to critical or sensitive business information processing facilities.

## 9.1 Secure Areas

### 9.1.1 Physical Security Perimeter

All physical perimeters of Fujitsu Services RMG Account sites will be clearly defined. Site security personnel at Fujitsu Services RMG Account sites will maintain an appropriate level of control over the physical security perimeter of each site deploying security barriers, entry controls, CCTV, security fences, special lighting etc. as necessary. This is being backed by regular visits by Fujitsu Corporate, working with Fujitsu Services RMGA sites to maintain the appropriate levels of physical security ensuring no gaps or weaknesses are introduced. Datacentres providing processing facilities for Post Office data will have much higher levels of physical security than general offices not withstanding the need to protect sensitive information that may be stored at these offices.

CCTV footage will be stored on appropriate Digital media for a period of no less than 3 months on a rolling basis. Thereafter stored offline in a secure location.

RMGA CISO is responsible for ensuring that appropriate physical and environmental controls are in place, based on risk assessment, to protect assets from unauthorised access, damage and interference.

Consideration must be given also to any security threats presented by neighbouring premises.

Intrusion detection alarm systems must be used for installations which are left unattended. Intrusion alarms may be connected to a security company or the Police. Alarm systems must be tested regularly and maintained to manufacturers' requirements.

### 9.1.2 Physical Entry Controls

Full details of Fujitsu Corporate Policy can be found in Identification Cards and Physical Access Control (Ref: CS2).

Site security personnel shall control access to all Fujitsu Services RMG Account sites. All Account staff, whether permanent or contract, will be required to produce a valid security pass for that site before being allowed access to the site. Access rights must be removed immediately when the holder leaves the employ of RMGA, whether through leaving permanent employment of Fujitsu Services or due to re-assignment to other tasks.

Visitors to RMGA premises must have a RMGA sponsor, who must be responsible for that visitor whilst they are within a RMGA facility. All visitors to Fujitsu Services RMG Account sites are to be issued with a "visitor's badge".

RMGA visitors to Post Office Branches must be subject to RMGA vetting procedures and approval by Post Office Ltd.

FUJ00002073



## 9.1.3 Securing Offices, Rooms and Facilities

RMGA employs a best practice approach to securing offices, rooms and facilities across all sites, including a clear desk policy. In practice this means:

- Access to all secure areas is strictly controlled by the use of security facilities;
- All papers, discs and portable media that contain RMGA ( POL) Information are to be stored in an appropriately secured place when not in use
- PCs and workstations are to be protected by passwords and, either locked or a password-protected screen-saver invoked when not in use. Screens are to be timed-out whenever left inactive for a specified period based on formal risk assessment as defined in the Operational Use of IT & Communications Systems (Ref: ITS2)
- Support functions and equipment e.g. photocopiers, fax machines must be sited appropriately within the secure area to avoid demands for access which could compromise information;
- Doors and windows must be locked when unattended and external protection must be considered for windows particularly at ground level; and
- Directories and internal telephone books identifying locations of sensitive processing facilities must not be readily accessible by the public.
- Physical access to network jacks, wireless access points, gateways and handheld devices is restricted.
- The use of portable wireless devices, including 3G phones, is forbidden in areas where sensitive data is stored, processed or transmitted.

## 9.1.4 Protecting Against External and Environmental Threats

Detailed policy for Physical and Environmental security of Data Centre environments (ISN/001377) is included in Fujitsu Services Data Centre Security Policies.

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

Hazardous or combustible materials must be stored securely at a safe distance from a secure area. Bulk supply such as stationery must not be stored within a secure area until required. Fallback equipment and backup media must be sited at a safe distance to avoid damage from a disaster at the main site.

## 9.1.5 Working in Secure Areas

Information processing facilities for Post Office Limited data must be housed in secure areas. Information processing facilities managed by RMGA must be physically separated from those managed by third parties. Physical and logical segregation of RMGA Assets from other Fujitsu contracts must be maintained, however shared use of data centres, server rooms and environmental facilities is permitted. Security measures associated with installed equipment must take these factors into consideration to reduce RMGA's risks to an acceptable level.

Similar considerations apply to RMGA Assets at other non-RMGA sites (e.g. AP Client sites).

FUJ00002073



Managers responsible for secure areas must ensure that access rights to secure areas are regularly reviewed and updated at least monthly.

Unoccupied secure areas must be physically locked and subject to at least daily periodic checks, and there must be physical protection and guidelines for those staff working in secure areas.

Access to sensitive information and information processing facilities must be controlled and restricted to authorised persons only. Authentication controls (e.g. swipe card plus PIN) must be used to authorise and validate all access. An audit trail of all access must be maintained securely.

### 9.1.6 Public Access, Delivery and Loading Areas

Public access to RMGA sites will be through main entrances.

Where RMGA sites have isolated delivery and loading areas, these will be monitored when in use by the site security staff either directly or via the site CCTV. Direct access to the site will not normally be granted to staff via the loading bay or delivery area. The loading bay and delivery area doors are to be kept locked when not in use.

## 9.2 Equipment Security

### 9.2.1 Equipment Siting and Protection

Information processing equipment located on Fujitsu Services RMGA premises shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access. Where necessary equipment will be physically located in secure areas, protected by appropriate entry controls.

### 9.2.2 Supporting Utilities

Equipment shall be protected from power failures and other electrical anomalies as appropriate according to the potential risks identified by formal risk assessment. Where deemed necessary alternative power arrangements, e.g. backup generators, UPS, dual supplies etc. will be deployed.

All supporting utilities such as water, electricity air conditioning must be adequate for the systems they support and shall be regularly tested and inspected to reduce the risk of malfunction and ensure their availability and integrity.

### 9.2.3 Cabling Security

It is the responsibility of the Facilities Manager to ensure that all equipment and cabling is secured to the relevant ISO 27001 standards against interception, for example encryption and physical security and well maintained and protected against environmental hazards, including fire and water damage.

### 9.2.4 Equipment maintenance

Owners of equipment must ensure that it is correctly maintained to enable its continued availability and integrity. All equipment shall be maintained in accordance with the manufacturers' instructions by qualified and authorised maintenance personnel. A record is to be kept by owners of all maintenance work carried out.

FUJ00002073



All faults are to be recorded via a documented Fault Reporting System. This system shall also record the work carried out to fix the fault.

### 9.2.5 Security of Equipment Off-Premises

Off site equipment must be stored securely and adequately protected.

Equipment movements must be controlled and subject to appropriate authorization.

Regardless of ownership, any use of RMGA IT equipment outside RMGA premises must be authorised by the Line Manager who is responsible for ensuring that the user is aware of the security requirements and the access controls requirements.

### 9.2.6 Secure Disposal or Re-use

If equipment is to be disposed of or re-allocated then any RMGA data, software or information must be irreversibly removed as described in line with Para 7.2.2 and Appendix A of this document .

All equipment containing storage media (for magnetic media see para 10.7.2) which may have been used to store RMGA sensitive information must be checked to ensure that all sensitive information and licensable software has been removed or securely overwritten prior to disposal or re-allocation .

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

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

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

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

Portable memory devices such as USB sticks, portable hard-drives, PDAs and all the other gadgets capable of transporting data must be degaussed, cross-shredded, incinerated or pulped.

All mobiles phones must not be used for the purpose of storing RMG sensitive/confidential information.

### 9.2.7 Removal of Property

The removal from site of any equipment which may have been used for storage of sensitive RMGA data; RMGA or POL information; or any software must be authorised in advance by the RMGA CISO.

FUJ00002073



All decommissioning must take account of the removal of any sensitive or confidential information stored on any hardware or electronic media including backups and must ensure that any equipment that is not required is securely stored and documented or disposed of in a secure manner (including network equipment). This includes all equipment used to provide the RMGA service. Individual units are expected to produce their own procedures to comply with this

# 10 Communications and Operations Management

The objective of this section is to ensure that RMGA Information systems and networks are managed effectively to ensure their integrity, availability and confidentiality, and to prevent their accidental or deliberate misuse.

## 10.1 Operational Procedures and Responsibilities

### 10.1.1 Documented Operating Procedures

Responsibilities and procedures for the management and operation of all computers and networks must be established and supported by appropriate instructions and guidelines to ensure their correct and secure operation. ISO27001 requires this information to be made available to all who need it

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

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

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

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

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

### 10.1.2 Change Management

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

FUJ00002073



Change controls procedures must exist which permit the controlled correction of live systems in order to meet operational requirements and emergencies, e.g. patching of system vulnerabilities. All such changes must be reviewed and approved by the appropriate line management as soon as possible.

All Operational and emergency changes must be reviewed following implementation and either removed from the live environment or consolidated via the normal change control and build procedures.

There must be strict control over the implementation of changes to the software or hardware of any RMGA system, application or network. Such change control procedures must ensure that any changes do not compromise any security or control procedure.. Change control procedures must ensure:

- The identification of all components affected by the change.
- The authorisation of all changes and their approval on completion.
- The control of software versions at each stage.
- Quality and content control.
- The maintenance of a full record of all changes (audit trail)
- The deletion of any temporary User IDs/passwords, data and linkages when the system becomes live.
- Changes only carry out their required function and nothing more.
- Only those changes that have been tested are implemented on the live system.
- Changes meet operational requirements.

### 10.1.3 Segregation of Duties

Accountability of individuals is essential and segregation of duties will be enforced where appropriate.

Within the RMGA Service provision, duties and areas of responsibility shall be segregated in order to reduce opportunities for unauthorised modification or misuse of information or services. Specific requirements for banking keys are described within CS/OLA/051/052 and 053 for RMGA Network Banking Key Management."

### 10.1.4 Separation of Development, Test and Operational Facilities

Development, test, and operational facilities must be separated to reduce the risks of unauthorised access, or changes, to operational systems.

## 10.2 Third Party Service Delivery Management

### 10.2.1 Service Delivery

It is anticipated that all operational services for the Horizon or HNG-x Services will be hosted directly in Fujitsu Services operated environments, i.e. Fujitsu Services Datacentres. Should Fujitsu Services deem it necessary to use external facilities management services to host these Services, RMGA will carry out a formal risk assessment to identify areas of risk and appropriate

FUJ00002073



controls to mitigate these risks. As a minimum, controls no less stringent than those described in this policy document will be included in the agreement with any third party.

### 10.2.2 Monitoring and Review of Third Party Services

All third-parties, providing services to RMGA as part of the HNG-x Service will be subject to monitoring and review to ensure compliance with this policy.

Evidence of the adequacy of suppliers' security procedures must be sought where externally supplied goods or services are used to process critical and/or sensitive information.

### 10.2.3 Managing Changes to Third Party Services

All changes to third party contracts will be managed in accordance with RMGA change control procedures.

## 10.3 System Planning and Acceptance

### 10.3.1 Capacity Planning

RMGA provides a Capacity Management Service as described in Annex B of the CCD entitled "Service Management Service : Service Description (SVM/SDM/SD/0007)

### 10.3.2 System Acceptance

Acceptance criteria for new information systems, upgrades and new versions shall be established and suitable tests of the system, including any security requirements, carried out prior to acceptance.

The following items must be considered:

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

The purpose of the hardening process is to remove unnecessary services and applications thereby reducing the vulnerability of the system. This is covered in ARC/SEC/ARC/0003.

FUJ00002073



# 10.4 Protection against Malicious and Mobile Code

## 10.4.1 Controls against Malicious Software

RMGA will analyse threats associated with malicious software and, where appropriate, implement effective preventative controls as defined in RS/POL/010 Vulnerability and Risk Management Policy. These controls include:

- Virus prevention;
- Virus detection;
- Procedures for recovering from virus attacks, including; and
- Appropriate user awareness procedures.

Any anti-virus software in use will be updated on a regular basis.

The deliberate introduction of malicious code is a disciplinary offence.

## 10.4.2 Controls against Mobile Code

RMGA Services provided to POL do not currently use mobile code. However, should mobile code become used in Services, controls will be in place to ensure that authorised mobile code operates according to the provisions within this information security policy and unauthorised mobile code shall be prevented from executing.

# 10.5 Backup

## 10.5.1 Information Backup

A regular backup copy of data in POL Services will be taken at predetermined times without impacting the live service. Backups will be stored securely at each of the data centres.

Back-up copies of information must also be taken as part of data migration processes.

Back-ups will not normally be made to removable media but in the event that this is necessary:

- A log will be maintained of any backup media removed from site.
- Any backup media containing information transported off-site will be encrypted, protected from physical damage, sealed in tamper-evident packaging and transported by an authorised courier
- Back-ups must be tested and checked periodically to detect accidental or deliberate loss or corruption.

All RMGA supporting information, including system and support documentation, and project documentation will be backed up on a regular basis. These backup media will be stored securely and protected from environmental damage. The backup and restoration procedures will be documented and a log of all backups maintained.

# 10.6 Network Security Management

FUJ00002073



### 10.6.1 Network Controls

Networks will be adequately managed and controlled, in order to be protected from threats, and to maintain security for the Services using the network, including information in transit.

Sensitive information will be protected during transmission across Wide Area Networks. Controls to protect such data in transit may include:

- Encryption of user identification and authentication information;
- Information to be encrypted before transmission; and
- Appropriate cryptographic techniques and solutions used to protect the information.

Network configurations for Services provided to POL must permit traffic to flow between clearly defined security boundaries only as specifically required for the provision of Service and associated management.

Denial-of-service attacks and unauthorised access from other systems and networks must be prevented, including unauthorised access from:

- any public networks used;
- networks connecting to Third Parties;
- networks connecting Horizon or HNG-x to POL and/or RMG;
- other systems operated by Fujitsu on behalf of itself or other clients; and
- the Branch LAN.

Intrusion detection systems will notify network staff of attempted unauthorised access to POL Services. Individual attempts will be recorded and treated as a minor security incident. A concerted attempt or a successful breach will be treated as a major incident in accordance with the RMGA Customer Service Incident Management Process (SVM/SDM/PRO/018).

Back-up network facilities will be provided to protect against any single network communications, equipment, or configuration failure which would have a significant impact on the Service. Any backup or alternate network must be secured to the same level as the primary network.

The use of wireless technology within the Service is specifically prohibited, with the exception of public telecommunications services provided by UK licensed public telecommunications operators agreed in writing by Post Office Ltd.

### 10.6.2 Security of Network Services

All RMGA network services used in the provision of the HNG-x Service shall be clearly identified and their security attributes documented, monitored and tested.

## 10.7 Media Handling

### 10.7.1 Management of Removable Media

All removable computer media such as tapes, discs, cassettes, portable memory etc must be managed to ensure that essential information is not lost or disclosed in an unauthorised manner. Removable media must be protected against theft, damage or deterioration. Data centres must

FUJ00002073



have a secure media library with procedures to control the movement of media in and out. In other locations, magnetic media must be stored in lockable containers, cabinets, fire safes etc.

All removable media and documentation must be labelled with a classification appropriate to the contents. Any unmarked material should be investigated as far as reasonably practical to determine its appropriate classification and as a minimum is to be treated as Fujitsu Eyes Only.

Documents and other hard-copy information must be handled, distributed, stored and destroyed in accordance with the information labelling and handling guidelines.

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

As defined by ISO27001 removable media includes paper documents.

### 10.7.2 Disposal of Media

Computer media shall be disposed of securely according to its classification when no longer required. Sensitive information must not be made available to third parties via inappropriate disposal of computer media.

.

### 10.7.3 Information Handling Procedures

Procedures for the handling and storage of information will be established and maintained in order to protect such information from unauthorised disclosure or misuse, consistent with its classification level.

### 10.7.4 Security of System Documentation

System documentation can contain information where unauthorised disclosure could have significant impact, such as application procedures, data structures, access controls etc. and as such must be classified as **Company Restricted** and protected accordingly.

## 10.8 Exchange of Information

### 10.8.1 Information Exchange Policies and Procedures

All forms of information exchange including email, telephone conversations, meeting notes and minutes, relevant to the scope of this policy, are subject to the policy statements set out in this policy document.

### 10.8.2 Exchange Agreements

The exchange of information with external organisations will be subject to formally agreed controls appropriate to the classification of the information.

### 10.8.3 Physical Media in Transit

FUJ00002073



Security measures in RMGA IT systems will ensure appropriate confidentiality, integrity and availability of services, software components and data, whether in storage or in transit. This is also stated in 10.5.1 and 7.2.2.

### 10.8.4 Electronic Messaging

All personnel using the Fujitsu Services e-mail system will be subject to the corporate employee e-mail usage policy of Fujitsu Services, Use of Email and Internet Systems (Ref: ITS3).

Information classified in Fujitsu as Company Restricted or in POL as Confidential, or above, must not be sent unencrypted over all public networks and all networks that could be externally accessed (e.g. networks with unprotected access points and wireless networks)..

### 10.8.5 Business Information Systems

Unless otherwise stated, the policy statements set out in this policy document apply to all electronic office systems used by RMGA.

## 10.9 Electronic Commerce Services

### 10.9.1 Electronic Commerce Security

Electronic commerce will be protected by the use of encryption techniques and other controls, as appropriate, as defined by a risk assessment & relevant documentation to prevent fraudulent activity, contract dispute and unauthorised disclosure or modification of information. On-Line Transactions

Information involved in on-line transactions shall be protected to prevent incomplete and inaccurate transmission of information, unauthorised modification or alteration and disclosure, duplication or replay.

### 10.9.2 Publicly Available Information

All personnel using the Fujitsu Services corporate IT infrastructure to access publicly available systems, i.e. the Internet, will be subject to the corporate employee internet usage policy of Fujitsu Services, Use of Email and Internet Systems (Ref: ITS3).

There is no public access to the Horizon or HNG-x Services provided to POL.

The integrity of information that is published electronically via web based systems, e.g. management information, will be protected by the provisions of this policy document.

## 10.10 Monitoring

### 10.10.1 Audit Logging

Audit logs recording exceptions and other security relevant events will be produced, maintained, stored and disposed of securely.

Audit logs may be used for the detection and prevention of system misuse; to assist in future investigations; to support disciplinary and/or legal proceedings and for the monitoring of access. All security critical events will be time stamped.

FUJ00002073



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. Such logs must be protected so that the contents cannot be changed nor data deleted.

Auditable events will be carefully selected to minimise overheads but will include a record of all significant system changes.

Audit logs will be kept for an agreed period, in accordance with POL policy.

Effective audit analysis tools will be used.

The Audit Trail Specification defines the *operational* and *commercial* audit trails. These are, respectively, the audit trail associated with the operation of the services which make up the HNG-X solution and the audit trail associated with that part of RMGA internal commercial records to which Post Office Ltd's Internal Auditors or Agents may have access as set out in Schedule D5 of the HNG-X contract.

### 10.1.2 Monitoring System Use

Security alerts, suspicious activity or unusual occurrences shall be reported and investigated as security incidents. The provision of a real-time alert facility to a specific terminal shall be considered and the security incident handling process must be used as referenced in Section 13 of this document.

### 10.1.3 Protection of Log Information

Access to Audit Logs will be strictly controlled and will be protected from deletion, disablement, modification or fabrication. Wherever possible, there will be a segregation of duties between overall system security and Audit Logs security. Audit Logs will be analysed and administered only by appropriately trained staff.

### 10.1.4 Administrator and Operator Logs

Operational activity will be subject to monitoring, through physical supervision and the regular review of system log and console reports.

### 10.1.5 Fault Logging

All faults are to be recorded and analysed on the Service Desk system, as defined by Service Management. This system shall also record the work carried out to fix the fault.

### 10.1.6 Clock Synchronisation

Time clocks within the HNG-x Service will be synchronised with a reliable time source.

Audit trails will accurately record system time to ensure events can be correlated.

# 11 Access Control

FUJ00002073



The objective of this section is to prevent unauthorised access to RMGA facilities, computers, information and network Assets.

# 11.1 Business Requirement for Access Control

## 11.1.1 Access Control Policy

Access to all information assets must be controlled on the basis of business and security requirements. The purpose of this section is to define the access control policy for Royal Mail Group Account.

This Access Control Policy defines how access to information system resources is controlled in the RMGA and the delivery of The Service. It covers the Services provided by RMGA to POL, including Data Centre systems; RMGA managed systems such as interface systems at POL Branches and closely related RMGA systems. Access may be the result of direct user action, or automatically initiated activities.

Procedures for the implementation of the principles of this access control policy, which include lower level detailed access rules, can be found in the associated access controls joint working documents [Ref: SDM/SVN/MAN/0027 for Horizon and Ref: TBC for HNGx]

**The main principles of this access control policy are:**

- Physical and logical access to the IT systems must be controlled, with access granted selectively, and permitted only where there is a specific need.
- The principle of “least privilege” must apply to restrict the access rights of users whether human or non-human.
- Information must be appropriately separated in filestore, database tables etc. Each data set must be accessible only to those with a need for that access.
- All access to RMGA systems will be specified in terms of roles.
- Any exceptions to the policy require specific permissions
- Individuals in specified roles will be permitted to carry out defined functions and access specified data.
- Some users may be permitted to carry out more than one major function, so are permitted to take more than one “role”. This is not permitted in cases where security may be undermined.
- Access controls associated with resources must define the “role” of the user, not the individual user’s identity.
- Access controls associated with resources must provide access to the resources as in the role definitions guideline document.
- Access controls must take account of legal and contractual obligations regarding access to data and services (see Section 15).
- Access controls must take account of policies on information classification (see 7.2) and separation of duties (see 10.1.3)
- Access controls must take account of distributed and networked environments including all types of connection to each asset.
- Access to RMGA information processing facilities by third parties" must only be for the time needed
- Accountability of individuals is essential and segregation of duties must be enforced.
- There must be segregation of access control roles, e.g. access request, access authorization, and access to assets.
- Users are individually identified so that they can be made accountable for their actions.
- Multiple individuals will not share access credentials, or be required to share access credentials due to deployed technical solutions.

FUJ00002073



- All users and applications must be authenticated to IT systems. This authentication must identify them as individuals.
- Help Desks must maintain the information required to authenticate the callers and their Branches/offices as required for the type of call. If the call needs to be passed onto another internal RMGA help desk, the call must be forwarded only after the initial authentication has been carried out.
- Wherever authorisation is given orally, normally over a telephone link, additional verification methods must be used.
- Where possible RMGA operations will be automated to reduce the need for human intervention and the potential accidental and malicious security breaches that could result from human activity.
- System management tasks must be automated where practical. This includes taking remedial action where the results of monitoring the system show this is needed. Only where action cannot be taken automatically, or human verification of an action is needed, must human intervention be required.
- Facilities must be used to restrict access to computer and network resources on a need-to-know basis.
- Initial default accounts must be renamed where possible.
- Initial default passwords must always be replaced by secure passwords.
- All access to RMGA systems will be monitored.
- Access to RMGA information processing facilities by third parties must be controlled.
- There must be a demonstrable need for third party access.
- A risk assessment must be carried out to determine the security implications and control requirements for any forms of physical and electronic access by third parties.
- Any third party access to transaction data must be “read-only” and must not breach the confidentiality requirements of this policy.
- On-site third parties must be identified and documented.
- 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.
- The safety and security, including confidentiality, of access credentials is the responsibility of the each individual issued with the credentials and of those issuing the credentials.

## 11.2 User Access Management

### 11.2.1 User Registration

There must be clear user access processes which include:

- identity management;
- formal authorisation of access requests;
- periodic review of access;
- removal of access rights

Records of all persons registered to use RMGA systems must be kept, though the way this is done may be role or service dependent.

### 11.2.2 Privilege Management

The allocation and use of privileges shall be restricted and controlled.

FUJ00002073



The principle of Least Privilege shall be used to limit permanent access, and to use minimum default access permissions.

The system will maintain the clearances and authorisations granted to users, and access to information will be consistent with users' clearances and privileges.

Access to System Administration accounts will be strictly controlled. Knowledge of the passwords and authentication for system administrator accounts will be restricted to the authorised system administrators.

System administrators will be allocated and use a unique identifier, and the passwords will be subject to more frequent refresh than normal user account standards.

The use of system administration accounts will be kept to a minimum.

Segregation of responsibilities will ensure that no privileged user can cover up unauthorised actions, and a continuous record of all system administration commands, and the use of powerful system utilities, will be maintained securely.

### 11.2.3 User Password Management

There shall be a documented process for the issue and reset of user passwords. This process is to ensure that passwords remain private to the user.

Passwords will be stored in a one-way encrypted form and must be protected against substitution or dictionary attack.

Passwords shall be chosen to conform to the following criteria:

- 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.
- Passwords must expire in 30 days.
- 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.
- 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 identical characters. The password must not be the same as the username.
- After 3 consecutive unsuccessful attempts to log-on, the user must be locked out for at least 30 minutes or until reset by an administrator
- In general, system users must be subject to the controls specified above. The following exceptions are permitted:
- The username and password used to automate the login may be held in 'clear' i.e. readable format or unencrypted, if it is only accessible to authorised operational management staff for that system and the potential damage from misuse of that username is minimised.
- The password may expire less frequently than the 30 days for human users where suitably obscure passwords are used, e.g. strong passwords consisting of upper case, lower case characters, numbers and symbols and the risk of external access to such accounts is very low. (This is also referenced in 11.5.3).

### 11.2.4 Review of User Access Rights

RMGA will conduct a formal review process at regular intervals to review user access rights. These reviews shall be carried out at least annually, and include revalidation of user access

FUJ00002073



rights and privileges granted to users. In environments with sensitive information, a process must be in place to remove accounts that have been inactive for more than 90 days

## 11.3 User Responsibilities

### 11.3.1 Password Use

To compliment corporate policy as referenced at ITS 2.1 and in line with good practise all Users are;

- To keep passwords confidential to themselves.

- Passwords must not be shared with anyone else or stored in any way (unless Fujitsu approved processes for securely storing say infrequently used passwords).

- To change passwords if they believe they might have been compromised.

- To select passwords that comply with the policy in 11.2.3 and which are easy for the holder to remember but difficult for someone else to guess.

- Not to use the same value of password on any other system (unless there is assurance that it will be adequately protected on that system).

System Administrators, service desk personnel and any other individuals capable of resetting passwords and shall not reveal passwords unless the information owners or authorised users have first provided definitive evidence substantiating their identity.

Additionally, resetting procedures shall ensure that users comply with the following:

- Change Passwords that are subject to any possible compromise or suspected security breach;
- Change Passwords regularly to be within their life span before reaching their expiry; and
- Change Passwords temporarily assigned by the helpdesk immediately on first use.

### 11.3.2 Unattended User Equipment

All Fujitsu PCs, workstations and where possible mobile devices e.g. PDAs, will be configured to automatically lock after a preconfigured period of time to prevent unauthorised use. The system shall require that the Identification and Authentication process is repeated to unlock the device before work can be continued.

RMGA Staff will manually lock their PC, workstation (and where possible mobile device) or log-off before leaving it unattended for extended periods.

A warning screen, which is displayed prior to log-on at PCs and workstations, will warn the reader that unauthorised access to systems may result in disciplinary or legal action being taken.

For Services provided to POL after a period of inactivity at a Post Office counter, the session will time out but can be resumed on entry of the password. After a longer period of inactivity, the user is forcibly logged out.

### 11.3.3 Clear Desk and Clear Screen Policy

FUJ00002073



RMGA employs a clear desk and clear screen policy across all sites. Employees are required to ensure that whenever they leave their desk unattended during normal working hours all sensitive information is protected from unauthorised access by others.

All PCs and workstations will be configured to lock after a preconfigured period of time and will require a password to unlock. All employees are required to clear their desk of all materials and property when leaving the office

## 11.4 Network Access Control

### 11.4.1 Policy on Use of Network Services

To protect networked services, access to internal and external networked services shall be controlled by:

- Appropriate inter-network interfaces such as firewalls;
- Appropriate authentication mechanisms for users and equipment;
- Access control lists on routers;
- Controls on use of ports;
- Control of user access to network information systems;
- The use of Virtual Private Networks (VPN) to provide authentication and encryption for business and system management traffic to/from the Post Office branches
- The use of VPN protection for authentication and encryption for all Fujitsu Services Core Services links.
- The use of dial-up/dial-in for Out of Hours (OOH) access is limited to authorised Users and is described in OOH Password Changing Process- RSPRO047.

### 11.4.2 User Authentication for External Connections

Authentication, whereby a user's claimed identity is verified, is essential before any access is granted to any RMGA system. Authentication mechanisms are required to ensure that trust relationships can be established between communicating components within, and external to, RMGA Services.

All HNG-x Service connections with remote computer systems will be authenticated. The User or application that initiates a transfer shall be authenticated by both the destination and the source node. Authentication must be successful before any transfer is executed.

### 11.4.3 Equipment Identification in Networks

Automatic equipment identification will be considered as a means to authenticate connections from specific locations and equipment.

### 11.4.4 Remote Diagnostic and Configuration Port Protection

Access to diagnostic ports must be securely controlled to ensure they are only available to approved persons at approved times.

### 11.4.5 Segregation in Networks

FUJ00002073



Controls must segregate HNG-X from systems run for other clients by Fujitsu Services.

Controls must also reduce the possibility of interference between HNG-X systems by separating independent parts of the overall system, particularly those which have different security requirements. (This may be by a combination of network set-up, router controls, controls at ports of specific systems and Microsoft domain structure.) For example,

- RMGA management sites must separate their main networks from both the Fujitsu Corporate network and from those more secure Local Area Networks (LAN) used to access the Data Centre e.g. via a DMZ
- Systems concerned with Outlet Business Change must be separate from those used for operational running.
- Security services, e.g. the Key Management Service (KMS), must be protected from unauthorised access from other systems.
- Traffic originating within the RMGA Data Centres is generally initiated by controlled applications. These applications (and the way they are configured in the system) must restrict traffic between systems to the minimum necessary

## 11.4.6 Network Connection Control

Local users must only have access to specific LANs that provide access to local services and (via controlled connections) to the Fujitsu Corporate network.

The only permitted connections from the RMGA management site network must be:

- To the Fujitsu Corporate network via a controlled router, suitably firewalled and which restricts traffic to specifically authorised traffic only;
- To Order Book Control (OBC) users at regional offices and OBC suppliers at their sites via a controlled router and firewalls.
- To the secure LANs via a firewall which restricts data to that permitted (e.g. software from the Configuration Management system).

The only permitted connections from the secure LANs must be:

- To the Data Centres via encrypted links.
- To other secure LANs via an encrypted link (i.e. between the RMGA management sites).

All users with any interactive access to the Data Centres must do so via secure LANs

- Separate secure LANs must be used for separate user groups/activities where Company Secret/Strictly Confidential data is being handled at RMGA management sites. For example, Security Management and Audit users must be on a separate high security LAN from other users.
- Servers at the RMGA management sites that Company Restricted/Confidential data or are used to update the Data Centre require stronger security and must therefore be on a secure LAN.

## 11.4.7 Network Routing Control

All access in and out of the RMGA Data Centres must be restricted to the required traffic from/to the authorised sources/destinations for business and system traffic using routers and firewalls. Such traffic must be routed only to the ports at systems which require that traffic. The following controls will apply:

FUJ00002073



- All management and support users will access the Data Centres (and other managed systems) from controlled workstation environments.
- All RMGA Corporate management, system management and support sites with access to the main operational systems must have fixed links to the Data Centres.
- External support users with access to any of the RMGA systems containing sensitive or protectively marked information must access the systems via controlled workstations and environments as for RMGA support staff, but subject to extra controls. (Support of routers is an exception – see below).
- All fixed links must be protected by the use of hardware encryption devices.
- Firewalls and Routers must be configured to deny access to external users, (including support or maintenance users) until this access has been agreed. When permitted, the appropriate router must be configured to restrict access to the Data Centre to the particular system(s) needing support.

## 11.5 Operating System Access Control

### 11.5.1 Secure Log-on Procedures

Access to operating systems will be controlled by procedures that request the user to log-on using approved, valid credentials. Where access is granted to Horizon or HNG-x Service applications, this will be supported by two-factor authentication. Should authentication fail the system will not indicate which attribute of the authentication process caused the failure. All access to operating systems for HNG-x shall be subject to monitoring and audit. Passwords must not be transmitted in clear text over any network

### 11.5.2 User Identification and Authentication

All users will be uniquely and securely identified and such identity authenticated, prior to access being granted.

### 11.5.3 Password Management System

RMGA password management systems will provide effective, interactive facilities that ensure quality passwords that comply with section 11.2.3 of this policy for Services provided to POL and for Fujitsu Services systems Minimum Password Security (Ref: ITS2.1).

### 11.5.4 Use of System Utilities

RMGA will ensure that access to system utility programs will be restricted. Only members of specific administrator groups will be permitted access. System logging will be enabled to provide audit of all attempts to gain access to these utilities.

### 11.5.5 Session Time-out

All Horizon and HNG-x user terminals will be configured to automatically lock after a preconfigured period of 15 minutes to prevent unauthorised use. The system shall require that the Identification and Authentication process is repeated to unlock the device.

FUJ00002073



### 11.5.6 Limitation of Connection Time

All Horizon and HNG-x user terminals will be configured to automatically disconnect if there is no user activity in a preconfigured period of time following session time-out.

## 11.6 Application and Information Access Control

### 11.1.1 Information Access Restriction

Access to applications hosted and managed by RMGA will be restricted in accordance with the access control policies set out in this policy document.

RMGA service support-users will not normally have access to financial information contained in Horizon or HNG-x Services.

### 11.1.2 Sensitive System Isolation

Horizon and HNG-X systems hosted by RMGA must operate on logically separated networks segregated by appropriate boundary devices. Platforms hosting the above systems must be housed in secure zones within data centre locations.

Support Systems located outside RMGA data centres must incorporate high level controls to ensure that physical and logical separation from all other systems at their site are in place. In all cases security controls on staff using these systems must be in place.

All such systems must be regularly monitored and audited.

### 11.1.3 Mobile Computing and Communications

Fujitsu Services policy Security of Portable Equipment (Ref: ITS/9) outlines the controls required to ensure that care is taken to avoid loss of company equipment or data.
Where remote access is required to RMGA systems remote users will only connect through an approved remote access facility. As a minimum, this facility will:

- Provide a secure means of authentication of users in addition to identification and password; and
- Strongly encrypt any data passing across public networks.

Where access involves connection through a third party network, users must be provided with a personal firewall. Users must also be provided with a facility to enable them to update anti-virus software to the latest version before receiving any e-mails.

### 11.1.4 Teleworking

RMGA Staff will only use teleworking facilities with the prior approval of RMGA management. The teleworking facilities will be secured to a level no less than other RMGA office environments as governed by this policy document.

# 12 Information Systems Acquisition, Development and Maintenance

FUJ00002073



The objective of this section is to reduce the risk of accidental changes or unauthorised access to operational systems or data and to ensure that security requirements are fully implemented within the acquisitions, development and subsequent maintenance of any RMGA delivered system or service.

# 12.1 Security Requirements of Information Systems

## 12.1.1 Security Requirements Analysis and Specification

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

Statements of business requirements for new information systems, or enhancements to existing information systems must specify the requirements for security controls and must include the Fujitsu Services relevant security requirements from the Community Information Security Policy (RMPOL002) and this Security Policy.

Security requirements and controls will reflect the business value of the information assets involved and the potential business damage, which might result from a failure or absence of security.

Specifications for the requirements for controls must consider security of the automated controls to be incorporated in the information system, and the need for supporting manual controls. Similar considerations shall be applied when evaluating software packages, developed or purchased, for business applications.

System requirements for information security and processes for implementing security will be integrated in the early stages of information system projects.

If products are bought in, a formal evaluation and procurement process must be followed. Contracts with suppliers must address the security requirements.

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

# 12.2 Correct Processing in Applications

## 12.2.1 Input Data Validation

Checks must be applied to the input of business transactions, standing data, and parameter tables.

## 12.2.2 Control of Internal Processing

Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts. The design and implementation of applications will ensure that the risks of processing failures leading to a loss of integrity are minimized.

## 12.2.3 Message Integrity

An assessment of security risks shall be carried out to determine if message integrity is required and to identify the most appropriate method of implementation.

FUJ00002073



### 12.2.4 Output Data Validation

Output validation must be applied which checks for:

- plausibility;
- reconciliation - control counts to ensure complete processing of all data;
- sufficient information is provided to determine the accuracy, completeness, precision, and classification of the information;

A log will be created which audits activities in the data output validation process.

## 12.3 Cryptographic Controls

### 12.3.1 Policy on the Use of Cryptographic Controls

Services will comply with Post Office Cryptographic standards, contractual and relevant regulatory requirements for the handing of cryptographic key material.

RMGA communications services will be secured using standard algorithms and key strengths in line with Industry Good practice and Post Office Cryptographic Standards:

- All cryptographic key lengths shall be at least 128 bits for symmetric keys and at least 1024 bits for asymmetric keys where the associated cryptographic control protects the integrity or confidentiality of HNG-X Business Data, Reference Data or Application Software.

- PCI requirements state that for PCI Card holder data all Keys shall be AES 256 or TDES 168 in length

Approved keys must be protected in line with Government Specified Algorithms requirements as directed by POL Ltd.

Digital signatures provide a means of protecting the authenticity and integrity of electronic documents. All keys used for signing data must be afforded levels of protection equal to or greater than the highest levels of data signed.

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.

All cryptographic keys must be protected against unauthorised use, modification, loss, and destruction. In addition, secret and private keys need protection against unauthorized disclosure.

Equipment used to generate, store and archive keys must be physically protected.

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.

### 12.3.2 Key Management

A structured approach to Key Management will be implemented across all Services provided to POL. This must ensure that Keys are held securely and that unauthorised Users or systems must

FUJ00002073



not be able to deduce or use the key material. The following controls will be implemented to protect cryptographic keys.:

- Key material (symmetric keys, private keys and entropy) must be held in clear only when in physically secure environments.
- Public keys (except for the Certificate Authority's (CA) public key) must be held in certificates signed by the Certification Authority.
- Symmetric keys must only be stored where necessary, and be held securely.
- PIN encipherment keys must not be used for any other cryptographic purpose.
- Keys (or part keys) held in filestore must be in a separate filestore accessible only to authorised key custodians via authorised applications.
- Keys used for protecting data must not be resident in filestore in clear.
- Replay of encrypted PIN values will be prevented.
- Keys must be changed periodically according to Government Specified Algorithm policy or, where commercial algorithms are employed, in accordance with industry recognised timescales. Different periods may apply to Symmetric Keys used for encrypting data, Key Encryption Keys (KEKs) used to encrypt other keys and Certification Authority keys.
- New KEKs must not be distributed solely under the protection of existing KEKs.
- Key material in transit electronically must be encrypted (except for CHAP keys between the routers within the RMGA Data Centre LAN).
- Cryptographic keys are either installed locally at the machine where they are to be used, or are distributed electronically using an approved protocol which protects these keys in transit.
- Where a key is delivered in two parts, e.g. a red key and a black key, the parts must be delivered by different routes.
- The key (or part key) to be handled manually must be held in a locked safe when not in use. Access to this must be authorised and recorded in conformance with RMGA procedures.
- The creation, handling, transmission and storage of keys must be undertaken in accordance with ISO11568 Parts 1 to 3. (ISO 11568-1:2005 specifies the principles for the management of keys used in cryptosystems implemented within the retail-banking environment). Key generation must be undertaken on standalone workstations or other hardware units within a physically secure environment.
- Any new PIN processing devices at Data Centres must also comply with FIPS 140-2 Level 3. (FIPS is the Federal Information Processing Standards publication and 140 -2 references the Security requirements for Cryptographic Modules)

In addition, the following policies also apply to the management of the Network Banking Service (NBS) and HNG-x related keys:

- Key generation and management must comply with ISO11568 Parts 1 to 3.
- All keys that may directly or indirectly reveal a plain text PIN must be generated, handled, transcribed and stored in a way which ensures that no one individual has access to all key parts.
- PINs and any cryptographic key that may directly or indirectly reveal them must never appear in plain text outside a tamper detecting hardware security device complying with

FUJ00002073



the relevant section of ISO9564. (ISO 9564 specifies the basic principles and techniques which provide the minimum security measures required for effective international PIN management). Modules handling PINs or keys associated with multiple PIN Pads must conform to FIPS 140-2 level 3.

- Devices used to generate keys associated with PIN encryption and PIN Pad loading must be physically secure and conform to agreed standards.

## 12.4 Security of System Files

### 12.4.1 Control of Operational Software

Where RMGA uses proprietary software it must be within the terms of the licence conditions. Unauthorised copying of software and documentation is prohibited.

RMGA's configuration management system will maintain an inventory of all proprietary software used by all services.

The RMGA Operational and Change Management Processes will be utilised at all times to ensure that no changes are made to operational software or documentation without appropriate authorisation and regression facility.

For all systems that process or store Cardholder Data, File Integrity Monitoring must be used at least once per week to detect unauthorised changes to critical system, application and configuration files. The exclusion of files in this environment from the File Integrity Monitoring process must be formally documented and justified.

### 12.4.2 Protection of System Test Data

All test data and test cases for RMGA Services will be stored in a change control mechanism and will be protected and controlled, including the use of access controls.

Operational databases or live Horizon or HNG-x data must not be used for testing purposes. Where live information needs to be used, for testing realism the data will be sanitised before being used in the test environment.

Authorisation in writing from POL will be obtained each time operational information is to be copied to a test application platform and the copying and use of operational information will be logged to provide an audit trail.

Operational information will be securely erased from test application systems immediately after the testing is complete.

### 12.4.3 Access Control to Program Source Code

The source code for existing systems and newly developed applications will be kept in a configuration control system, which controls access to source code.

Access control policies set out in this policy document will apply to source code control systems.

## 12.5 Security in Development and Support Processes

FUJ00002073



### 12.5.1 Change Control Procedures

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

There must be strict control over the implementation of changes to the software or hardware of any RMGA system, application or network. The operational change process must ensure that changes do not compromise any security or control procedure.

All changes to the system, operating system, and programs must be subject to the RMGA formal operational change process and must be approved before commencement.

All proposed changes to RMGA systems must consider information security as part of the impact assessment. Where changes are significant then formal risk assessment must take place. RMGA Security must be consulted on all aspects of information security and risk assessment.

The operational change process must ensure that existing 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.

### 12.5.2 Technical Review of Applications after Operating System Changes

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

When operating systems are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

### 12.5.3 Restrictions on Changes to Software Packages

If changes must be applied by RMGA, then the original software shall be retained and the changes applied to a clearly identified copy and fully documented, so that they can be re-applied if necessary to future software upgrades.

### 12.5.4 Information Leakage

The purchase, development, use, maintenance and modification of software by RMGA will be appropriately controlled in order to protect against covert channels, Trojan code, worms, viruses and equivalent items.

### 12.5.5 Outsourced Software Development

Software development is not currently outsourced. Should this position change, the provisions of this Information Security Policy document, in particular the requirements set out in Section 6.2, shall apply.

## 12.6 Technical Vulnerability Management

### 12.6.1 Control of Technical Vulnerabilities

FUJ00002073



RMGA will ensure that all technical vulnerabilities are recorded upon identification. The impact of the technical vulnerability will be assessed and methods for mitigating the risk proposed. In accordance with the risk management approach as defined in the Vulnerability and Risk Management Policy RS/POL/010, mitigations will be implemented as appropriate in order to ensure that the vulnerability has been controlled.

# 13 Information Security Incident Management

Fujitsu Services must:

- Ensure information security events and weaknesses associated with RMGA information systems are communicated in a manner allowing timely corrective action to be taken and as referenced in CS/PRO/018 (RMGA Customer Service Incident Management Process).
- Ensure a consistent and effective approach is applied to the management of information security incidents.

An information security Incident is: "an adverse event or series of events that compromises the confidentiality, integrity or availability of RMGA information or information technology assets, having an adverse impact on Fujitsu Services reputation, brand, performance or ability to meet its regulatory or legal obligations." This will also extend to include assets entrusted to Fujitsu including data belonging to Post Office Ltd, its clients and its customers.

## 13.1 Reporting Information Security Events and Weaknesses

### 13.1.1 Reporting Information Security Events

Information security events must be reported through the RMGA Service Desk as quickly as possible.

A formal information security event reporting procedure must be established, in line with the incident management process which includes an incident response and escalation procedure, setting out the action to be taken on receipt of a report of an information security event.

Incidents that threaten Cardholder Data and Sensitive Authentication Data must be acted upon as outlined in the incident management process under PCI Incidence Response.

All security incidents reported to the Service Desk must be logged and given a reference and handled in accordance with the incident management process.

All RMGA Staff will be made aware of their responsibility to report any information security events and suspected breaches as quickly as possible.

### 13.1.2 Reporting Security Weaknesses

RMGA has established effective procedures for reporting, acting upon and escalating all security incidents/ breaches that could affect security. It is the responsibility of all users of the RMGA services and RMGA personnel to use these procedures. [Ref: CS/PRO/018]

All security weaknesses must be recorded with a unique reference number, investigated and resolved in accordance with these procedures. Where appropriate the Operational Security

FUJ00002073



Manager or CISO will liaise with Post Office Security staff to review relevant incidents and actions.

If RMGA Staff identify or suspect that a security weakness exists anywhere in the RMGA system then they must report these matters to the RMGA Service Desk, or direct to the Operational Security Manager, as quickly as possible in order to prevent information security Incidents.

All RMGA staff must be aware that they should not, in any circumstances, attempt to prove a suspected weakness themselves. If such a course of action resulted in a security Incident then it may be treated as a disciplinary issue.

## 13.2 Management of Information Security Incidents and Improvements

### 13.2.1 Responsibilities and Procedures

In addition to reporting of information security events and weaknesses, the monitoring of systems, alerts, and vulnerabilities shall be used to detect information security Incidents.

Procedures for reporting, acting upon and escalating all security incidents/ breaches are fully described in CS/PRO/018 and include:

- timely response
- analysis and identification of the cause and seriousness of the Incident;
- continuity of evidence
- ensuring only authorised access for all investigative purposes
- containment;
- co-ordination management, incident log recording, planning and implementation of corrective action to prevent recurrence, if necessary;
- communication with those affected by or involved with recovery from the Incident;
- reporting the action to the appropriate authority;
- documenting in detail all emergency actions
- ensuring that the integrity of business systems and controls is restored with minimal delay.
- incorporating security industry developments and changes
- modification to documentation in light of lessons learnt
- recording lessons learnt

### 13.2.2 Learning from Information Security Incidents

FUJ00002073



The information gained from the evaluation of information security Incidents shall be used to identify recurring or high impact Incidents.

The RMGA Operational Security Manager must carry out a check of all security Incidents investigations on a regular basis and create a summary report highlighting all security incidents. The report must also highlight any trends or weaknesses which may need to be raised at future Security Forums.

### 13.2.3 Collection of Evidence

Where a follow-up action against a person or organization after an information security incident involves or may involve legal action (either civil or criminal), evidence will be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s). Legal action may also be initiated by 3rd parties e.g. by regulatory bodies or controllers of potentially compromised sensitive information.

Should it be considered necessary the incident might be passed to an external investigator or forensics team, who will ensure that any data required for evidential purposes is captured and investigated using a systematic approach which ensures that an auditable record of evidence is maintained and can be retrieved

Incident investigation procedures provide that evidence is collected such that it is admissible and of sufficient weight by keeping original documents, copies of information held on hard discs, removable media and log files.

# 14 BUSINESS CONTINUITY MANAGEMENT

The objective of this policy section is to counteract interruptions to RMGA business activities and to protect critical business operations from the effects of major failures of information systems or disasters and to ensure their timely resumption.

## 14.1 Information security aspects of business continuity

### 14.1.1 Including information security in the business continuity management process

A managed process must be developed and maintained for business continuity throughout RMGA.

The RMGA Business Continuity Manager is responsible for ensuring that a process is implemented to minimize the impact on the RMGA and delivery of The Services and recover from loss of information assets. This process will identify the critical business processes and integrate the information security management requirements of RMGA business operations with other continuity requirements.

The RMGA Chief Information Security Officer will be involved in the development and maintenance of the process, and any continuity plans, to ensure that information security requirements are adequately addressed.

### 14.1.2 Business continuity and risk assessment

Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and any consequences for information security.

FUJ00002073



The consequences of disasters, security failures, loss of service, and service availability must be subject to a business impact analysis.

Business continuity management will include controls to identify and reduce risks, in addition to the general risks assessment process, limit the consequences of damaging incidents, and ensure that information required for business processes is readily available.

### 14.1.3 Developing and implementing continuity plans including information security

A Business Continuity Plan must be developed and implemented to ensure timely resumption of essential operations. Information security will be an integral part of the overall business continuity process.

RMGA Business Continuity Manager must ensure that an effective business continuity plan is agreed with RMGA Security staff and implemented to reduce the risks from deliberate or accidental threats to deny access to vital services or information including deliberate loss of confidentiality and integrity of RMGA assets.

Plans must be established, and maintained, to enable internal operations and business services to be maintained following failure or damage to vital services, facilities or information.

All relevant security provisions must be maintained, even if degraded conditions are in effect. If alternative temporary locations are used, the level of implemented security controls at these locations should be equivalent to the main site(s).

In order to minimise any disruption to the Services managed by RMGA, continuity plans will encompass:

- Handling emergency situations;
- Operating in fall-back mode;
- Recovery (or Business Resumption) to full operational status
- The escalation plan and the conditions for its activation; and
- Responsibilities for executing each component of the plan.

Business continuity plans will address RMGA vulnerabilities and therefore may contain sensitive information that needs to be appropriately protected. BC Plans must be stored off-site in secure conditions but readily available in the event of the need to activate them.

### 14.1.4 Business continuity planning framework

The Fujitsu Services RMG Account will maintain a framework of business continuity plans, integrated with Fujitsu Services Corporate plans and, where appropriate, with the plans of the customer ensuring that all plans are consistent, and to identifying priorities for testing and maintenance.

### 14.1.5 Testing, maintaining and re-assessing business continuity plans

FUJ00002073



The RMGA Business Continuity Manager is responsible for ensuring that the BC Plan is regularly reviewed.

The identification of changes in business arrangements not yet reflected in the business continuity plans will be followed by an appropriate update of the plan. This formal change control process will ensure that the updated plans are distributed and reinforced by regular reviews of the complete plan.

Business continuity plans must be tested under representative operational conditions and updated regularly to ensure that they are up to date and effective. The test schedule for business continuity plan will indicate how and when each element of the plan will be tested. External suppliers of key services must be included in tests to ensure that risks are minimised, wherever RMGA is dependent upon subcontractors (or third parties), for essential services or supplies.

Tests of business continuity plan will ensure that all members of the recovery team and other relevant RMGA Staff are aware of the plans and their responsibility for business continuity and information security and know their role when a plan is invoked.

The RMGA Business Continuity Manager and Chief Information Security Officer must be satisfied that continuity arrangements of external suppliers of key facilities and services are sufficient to ensure that RMGA will meet its contracted commitment for information security to the customer.

# 15 COMPLIANCE

RMGA is required to comply with legislative requirements and commercial standards. The controls defined in ISO27001 are designed to provide a sound baseline for commercial organisations of many types.

Through the implementation of this policy, RMGA will apply ISO27001 to provide a baseline definition for information security encompassing the eleven categories of controls in the context of the RMGA Service.

The RMGA Information Security Policy will encompass and comply with all security aspects of customer requirements as defined in relevant Contract Schedules and the Community Information Security Policy, where appropriate. Being a high level policy, in many cases one policy statement may cover a number of the detailed requirements as laid down in these schedules.

## 15.1 Compliance with legal requirements

Fujitsu Services is required to comply with legislative requirements and technical and commercial standards in its own right as a business organisation. In addition RMGA provides a managed service for POL; in this case POL may have additional legal and regulatory requirements imposed upon them. These legal and regulatory obligations are passed down to RMGA within the contractual agreement as specific implementation requirements and as such are not specifically covered in this document. Relevant POL requirements as expressed in the CISP have already been included within the specific policies, which are mandatory.

### 15.1.1 Identification of applicable legislation

It is the customer responsibility to explicitly define, document, and keep up to date all relevant statutory, regulatory, and contractual requirements for each information system and provision of facilities to enable the customer to discharge its own legal and regulatory obligations must be explicitly provided through requirements statements in the normal way.

FUJ00002073



RMGA will document its approach to meet these requirements.

Implementation advice on Fujitsu's legal responsibilities is provided by Fujitsu Group Legal department.

### 15.1.2 Intellectual property rights (IPR)

The Copyright, Designs and Patents Act 1988 states "The owner of the copyright has the exclusive right to copy the work." It is illegal to copy software without the copyright owner's permission.

Proprietary software must be used within the terms of the licence conditions. Unauthorised copying of software and documentation is prohibited.

Where practicable vendor-supplied software packages shall be used without modification. If changes are deemed necessary, these should first be requested under change control to the original supplier and implemented as an upgrade from the supplier.

RMGA will not permit any modified or non-standard software components to be incorporated.

An inventory of all proprietary software used by the Services will be maintained.

### 15.1.3 Data Retention and Protection of organisational records

Records stored electronically and hard copy retained for the contractual period will be accessible throughout the required retention period and will be safeguarded against loss due to future technology change as referenced in the Audit Trail Specification CR/FSP/006.

Data will be retrievable to meet legal requirements as requested by a court of law, e.g. records required can be retrieved in an acceptable timeframe and in an acceptable format.

### 15.1.4 Data protection and privacy of personal information

It is Fujitsu Services' clearly stated policy to comply with all laws and regulations relating to the protection of personal information in all countries in which it transacts business and to maintain a high standard of compliance in all its worldwide operations.

All applications handling personal data on individuals must comply with data protection legislation and principles. RMGA shall process personal information only in accordance with the instructions of each Data Controller as set out in the Agreement and applicable provisions of the Service Description CCDs dealing with such processing.

### 15.1.5 Prevention of misuse of information processing facilities

Users shall be deterred from using information processing facilities for unauthorized purposes.

Under the Computer Misuse Act, it is an offence to access or modify material without proper authority, or to access material with intent to commit further offences. Warning notices to this effect must be displayed to potential users prior to system log-on.

### 15.1.6 Regulation of cryptographic controls

RMGA will only use cryptographic techniques within the Services that are compliant with POL cryptographic policies and standards as referenced in CISP.

FUJ00002073



## 15.2 Compliance with security policies and standards and technical compliance

### 15.2.1 Compliance with security policies and standards

Compliance with the requirements defined in the RMGA Information Security Policy is mandatory. The policy is to be applied throughout RMGA for the secure management and operation of all systems and Services designed, built, implemented, operated, used, supplied or managed by the Fujitsu Services RMG Account.

Regular audits are carried out under the direction of RMGA CISO and/or RMGA Programme Assurance Manager, to verify that RMGA is operating in accordance with its security policy and procedures.

Security Audits can also be initiated by Post Office Limited, its clients or regulators either in response to a specific incident or on a regular basis.

These audits will form part of an overall assurance programme and will be scheduled, co-ordinated, reported and corrective action plans acted on as part of an integrated audit schedule (IAS) PGM/PAS/PLA/0014 which is maintained by the RMGA Quality Manager.

Where relevant, RMGA will comply with customer security requirements as expressed in the Community Information Security Policy. They do not need to comply with requirements in the CISP addressed specifically to other parties.

### 15.2.2 Technical compliance checking

RMGA Information systems must be regularly checked for compliance with security implementation standards and regulatory requirements. Technical compliance checking involves the examination of operational systems to ensure that hardware and software controls have been correctly implemented. An external auditor will annually audit the card holder environment to ensure compliance. This type of compliance checking requires specialist technical assistance. It shall be performed manually (supported by appropriate software tools, if necessary) by an experienced system engineer, or by an automated software package which generates a technical report for subsequent interpretation by a technical specialist.

Compliance checking also covers, for example, penetration testing, which might be carried out by independent experts specifically contracted for this purpose. Caution should be exercised in case success of a penetration test could lead to a compromise of the security of the system and inadvertently exploit other vulnerabilities.

Any technical compliance check shall only be carried out by, or under the supervision of, competent, persons authorised by the RMGA CISO.

Technical compliance checking will form part of an overall assurance programme and will be scheduled and co-ordinated as part of an integrated audit programme.

## 15.3 Information systems audit considerations

### 15.3.1 Information system audit controls

RMGA Services will be developed to ensure that customer requirements for audit controls are met.

FUJ00002073



RMGA systems used to support the Services will consider the following when implementing audit controls:

- All security critical events are time stamped and recorded;
- Auditable events are carefully selected to minimise overheads;
- Audit trail information is protected from modification;
- Audit trails include a record of all significant system changes;
- Effective audit analysis reduction and analysis tools are used;
- All observed system irregularities are investigated; and
- Audit trails are archived and stored for an agreed duration.

### 15.3.2 Protection of information system audit tools

System audit tools (programs and log files) will only be available to authorised personnel and will be protected to prevent any possible misuse or compromise.

.

FUJ00002073

FUJ00002073



# A Information Labelling and Handling Guidelines

The declassifying policy must not be applied to Post Office data entrusted to Fujitsu unless specifically agreed in writing.

| Classification | Marking | Email | Phone | Fax<br>**NB** Telex should not be used | **De-Classifying** |
|---|---|---|---|---|---|
| **Commercial in Confidence**<br>**Eyes Only** | Documents - Marking must be at the top and bottom of each page and on the front and back covers in letters at least 7 mm high or where produced on a printer which does not accommodate scaleable fonts, in upper case bold. Where a document contains pages of differing classifications the highest classification must be marked on the covers. | May be transmitted by electronic mail within the Company and where the recipient is an employee or a contractor where receipt is in the company's interest. It should only be transmitted outside the company if the recipient is a trusted party with sound business reason for receipt - approved encryption methods must be used. | Matters should only be discussed when necessary and in a guarded manner. | Information should only be transmitted when a person-to-person link has been established (the sender being responsible). | Can only be downgraded to Unclassified by the owner. |
| **Company Restricted** | HTML - Marking must appear at the top of each page in font size of at least 14pt. It is recommended that where scrolling is likely a procedure is implemented to continue to display the marking at all times. | May be transmitted unencrypted by electronic mail within the Company, providing such mail is flagged as sensitive (e.g. 'Confidential' if sent by Outlook). Where transmissions are outside of the company secure approved encryption methods must be used. | Should not be used | Information should only be transmitted within the company when a person-to-person link has been established. Use of approved devices supporting and using encryption must be used for transmissions outside the company. | Should, unless otherwise stated, be downgraded to Fujitsu Eyes Only after two years. |
| **Company Secret** | **Documents** - Marking must be at the top and bottom of each page and on the front and back covers in letters at least 7 mm high or where produced on a printer which does not accommodate scaleable fonts, in upper case bold.<br>Where a document contains pages of differing classifications the highest classification must be marked on the covers.<br>All pages must be consecutively numbered to reflect the total number of pages e.g. 1 of 6, 2 of 6 etc. | Secure approved encryption will be used between transmitting devices for transmission of all data marked COMPANY SECRET. | | Can be used providing secure approved encryption is used between transmitting devices and remote facsimile devices are known to be supervised by a trusted individual. | Must, unless otherwise stated, be downgraded to FUJITSU EYES ONLY after two years. |

FUJ00002073



| | | | | | |
|---|---|---|---|---|---|
| | Copies must be numbered in the same manner i.e. 1 of 6 copies etc.<br><br>A distribution list must be attached showing the copy number of copies sent to each recipient.<br><br>**HTML** - Marking must appear at the top of each page in font size of at least 14pt. It is recommended that where scrolling is likely a procedure is implemented to continue to display the marking at all times. | | | | |
| **Classification** | **Storage**<br><br>When sensitive information is not in use it must still be protected against compromise. | **Copying** | **Destruction**<br><br>Classified waste must be kept separate from other waste and appropriately protected until its destruction by pulping, burning or shredding. | **Despatch**<br><br>**NB** On receipt to be opened by the addressee, or by a specifically authorised deputy | |
| **Commercial in Confidence**<br><br>**Eyes Only** | **Hard Copy -** Must be stored in container, cabinet, cupboard or safe with secure lock.<br><br>**Disks or tapes** used to stock back-up copies must be marked and protected in the same manner as hard copies.<br><br>**IT Systems –** Information may only be held in the machine's memory if the integrity of the information is assured.<br><br>**Cafe VIK/ ProjectWeb -** Commercial in Confidence or Fujitsu Eyes Only may be held in the public area of Cafe VIK. Commercial in Confidence and other 'EYES ONLY' material can be held in private areas of communities or ProjectWeb. | May be copied on the authority of a manager but further distribution must be kept to the essential minimum. | Must be destroyed by the holder when no longer required. | **Enveloping -** Must be enclosed in a fully opaque windowless envelope, with the classification clearly marked.<br><br>**External Transmission -** Can be sent by post or commercial courier. The above envelope should be inserted into an outer envelope, bearing only the addressee's details.<br><br>**Internal Transmission**<br><br>Can be sent internally in a sealed envelope. | |
| **Company Restricted** | **Hard Copy -** Must be stored in container, cabinet, cupboard or safe with secure lock.<br><br>Computer Media<br><br>**Disks or tapes** used to stock back-up copies must be marked and protected in the same manner as hard copies.<br><br>**IT Systems -** Information may only be held in the machine's memory if the integrity of the information is assured.<br><br>**Cafe VIK/ ProjectWeb -** Information may only be held in the private area of a Community or a project in ProjectWeb of which all members are authorised to receive copies of the | Should be carried out or supervised by trusted individuals or trusted partners. Extra or spoilt copies should be destroyed. | Must be destroyed by the holder, if in bulk, under the direct supervision of a security officer or other nominated responsible person. | **Enveloping -** Must be enclosed in a fully opaque windowless envelope with the classification clearly marked. Must be double-enveloped also using a fully opaque windowless envelope. The outer envelope should only bear the addressee's details.<br><br>**External Transmission -** Post Office Recorded Delivery is to be used. | |

FUJ00002073



| | | | | |
|---|---|---|---|---|
| **Company Secret** | document. | Must not be copied, or the information further disseminated without the agreement of the originator. Copying can only be carried out by trusted individuals. | Must not be disposed of under bulk waste arrangements, its destruction must be carried out or witnessed by the holder or an appropriate delegate.<br><br>**Hard disks** should be overwritten using a secure approved utility. **Removable media** should be degaussed or destroyed as for paper. Media, which cannot be over written or is damaged, should be destroyed by an approved company. Ensure all image, archive and backup copies are destroyed or protected as appropriate. | **Internal Transmission - M**ay be sent by internal mail, if it is to be carried by an outside courier/messenger it must be done so against receipt. |