POL00395097

Information Security Management Policy Set -
Security Incident Management

Unclassified

NB: This document is one of a set of policies which will eventually replace the Horizon Security Policy and other security documentation prior to HNG X going live and is not intended to be active until the full set of policies are completed and approved as a set

Document Title:	RMGA ISMS Policy Set **Security Incident Management**
Document Type:	Policy (POL)
Release:	Release Independent
Abstract:	This is a subordinate security policy of the RMGA policy and addresses the policy security Incident management.
Document Status:	DRAFT
Author & Dept:	Mike Jenkins – Principal Consultant (Security)
Internal Distribution:	Graham Chatten; Ian Terblanche; Richard Brunskill; Jan Holmes, Martyn Hughes, Naomi Elliott, Hilary Forrest, Colin Lenton-Smith, Ian Cooley, Dave Tanner, Jerry Acton, Sheila Bamber, Graham Welsh, Pete Thompson, Mik Peach. Dave Wilcox, John Burton, Chris Bridgeland
External Distribution:	Sue Lowther – Post Office Limited.

Approval Authorities:

Name	Role	Signature	Date
Ian Terblanche	Account Director RMGA		
Colin Lenton-Smith	Commercial Director RMGA		
Martyn Hughes	Programme Director RMGA		
Naomi Elliott	Service Director RMGA		
Brian Pinder	Security Manager RMGA		
Sue Lowther	Head of Information Security Post Office Limited		
Jan Holmes	Programme Assurance Manager		

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

POL00395097

0 Document Control

0.1 Table of Contents

POL00395097

0.2 Document History

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
0.1	03/09/2007	ISMS Policy Document set first draft	

0.3 Review Details

Review Comments by :	Friday, 14th September 2007
Review Comments to :	Mike.jenkins GRO & RMGADocumentManagement GRO

Mandatory Review	
Role	**Name**
Royal Mail Group Account Security Forum	Brian Pinder
Service Director RMGA	Naomi Elliott
Programme Director RMGA	Martyn Hughes
Director Commercial RMGA	Colin Lenton-Smith
Programme Assurance Manager, RMGA	Jan Holmes
IT Security Manager RMGA	Brian Pinder
Head of Information Security POL	Sue Lowther after 1st Internal Review ie NOT this time
Commercial & Contracts Manager RMGA	Hilary Forrest

Optional Review	
Role	**Name**
Customer Services RMGA	Richard Brunskill
Service Support Manager	Peter Thompson
Head of Service Transition & Change	Graham Welsh
Head of Service Management	Steve Denham
Royal Mail Group Account Application Team Manager	Tom Northcott
Managing Solution Architect	Giacomo Piccinelli
HNGX Security Architect	Jim Sweeting
RMGA Security Operations	Bill Membery
RMGA Applications Test	Nigel Taylor

Issued for Information – Please restrict this distribution list to a minimum	
Position/Role	Name

POL00395097

(*) = Reviewers that returned comments

0.4 Associated Documents (Internal & External)

	Reference	Ver	Date	Title	Source
1.	PGM/DCM/TEM/0001		13/6/06	Fujitsu Services RMGA HNG-X Document Template	Dimensions
2.	BS ISO/IEC 17799: 2005		16 June 05	Information technology Security techniques Code of practice for information security management	British Standard
3.	ISO27001		Nov 2006	Information Security Management System Requirements.	British Standard
4.	RS/PRO/002		28/04/06	RMGA Security Vetting Process	PVCS
5.	RS/PRO/013		4/01/06	Horizon Security Pass Procedure	PVCS
6.	RS/POL/003		14/04/05	RMGA Access Control Policy	PVCS
7.	RS/POL/04			Computer Virus Policy	PVCS
8.	RS/POL/010		29/03/07	Vulnerability & Risk Management Policy	PVCS
9.	RS/FSP/001		01/02/06	Security Functional Specification	PVCS
0.	CS/SER/016		06/03/06	Service Description for the Security Management Service	PVCS
1.	SVM/SDM/PRO/0018			Incident Management Process	Dimensions
2.	CS / 3		29 Jan 03	Stop and Search	Intranet Site
3.	ITS / 8		1 Aug 04	FS Corporate Classification and Privacy markings	Intranet Site
4.	ITS / 19		4 April 06	FS Corporate Facility Security	Intranet Site
5.	PCI		Jan 2005	Payment Card Industry Data Security Standard	PCI
6.	CISP			Community Information Security Policy	Post Office Document
7.	ARC/SEC/ARC/SEC/003			HNGX Security Architecture	Dimensions
8.	SVM/SDM/POL/0023	0.0	May 2007	ISMS Security Policy Master Set	Dimensions
9.	SVM/SDM/POL/0025	0.0		Security Organisation and Management Policy	Dimensions
0.	SVM/SDM/POL/0024	0.0		Asset Management Policy	Dimensions
1.	SVM/SDM/POL/0030	0.0		Human Resources Policy (Security matters)	Dimensions
2.	SVM/SDM/POL/0028	0.0		Physical and Environmental Security Policy	Dimensions
3.	SVM/SDM/POL/0029	0.0		Operations and Communications Management	Dimensions
4.	SVM/SDM/POL/0027	0.0		Access Controls	Dimensions
5.	SVM/SDM/POL/0033	0.0		Systems Acquisition, Development & Maintenance	Dimensions
6.	SVM/SDM/POL/0031	0.0		Incident Management	Dimensions
7.	SVM/SDM/POL/0032	0.0		Business Continuity	Dimensions
8.	SVM/SDM/POL/0034	0.0		Compliance	Dimensions

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

POL00395097

0.5 Abbreviations

Abbreviation	Definition
CISP	Community Information Security Policy (for Post Office)
FS	Fujitsu Services
IA	Information Assurance
ISMS	Information Security Management System
ISO	International Standards Organisation
PCI	Payment Card Industry (Security Standard)
PIN	Personal Identification Number
POL	Post Office Limited
RMGA	Royal Mail Group Account (Fujitsu Services' organisational entity)

0.6 Glossary

Term	Definition
Asset	Any information asset which contributes to RMGA business and delivery of the Service. Will include hardware and networks; applications and data; people and premises; Intellectual Property and licences.
Asset Owner	The term 'owner' identifies an individual, role or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. The term 'owner' does not mean that the person actually has any property rights to the asset,, these may be Fujitsu Services
The Service	The counter automation services delivered to Post Office Ltd
RMGA Staff	Includes all staff directly employed by RMGA; those Fujitsu Services staff on assignment to the RMGA project; all Fujitsu Services persons; all 3rd party contractors and sub-contractors, involved in the delivery of The Service
Information Security Incident	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

0.7 Changes Expected

Changes
This is the first draft for consultation and comments. Changes are expected in light of comments received.

0.8 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.

POL00395097

0.9 Copyright

POL00395097

1 Purpose and Scope

The purpose of this document is to define the security incident management policy for Royal Mail Group Account consistent with IS27001, contractual commitments and relevant POL requirements as expressed in CISP. [Ref 16]

The scope of this policy includes all security domains and business operations of the Post Office counter automation system (The Service), related processes and procedures.

This policy is a derivative policy and supports the RMGA Information Security Master Policy which is in turn subordinate to Fujitsu Services corporate Information Services policy where they are applied to operational areas provided from FS Core.

1.1 Objectives

The objectives of this policy are:

- To ensure information security events and weaknesses associated with RMGA information systems are communicated in a manner allowing timely corrective action to be taken.
- To ensure a consistent and effective approach is applied to the management of information security incidents.

2 Policy Statement.

1. Information security events should be reported through appropriate management channels as quickly as possible.

2. All employees, contractors and third party users of information systems and services should be required to note and report any observed or suspected security weaknesses in systems or services.

3. Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to information security Incidents.

4. There should be mechanisms in place to enable the types, volumes, and costs of information security Incidents to be quantified and monitored.

5. Where a follow-up action against a person or organization after an information security Incident involves legal action (either civil or criminal), evidence should be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

POL00395097

3 RMGA Incident Management

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.

Incidents can be categorised in many ways, they can occur alone or in combination with other Incident categories and can vary significantly in severity and impact. It is important that all Incidents are recognised and acted upon.

For the purpose of illustrating the impact of Incidents two levels of severity have been defined (Note: in practice the assessment may be less straightforward):

A **MINOR** Incident will normally have limited and localised impact and be confined to one domain, resulting in one or more of the following:

- Loss or unauthorised disclosure of internal or sensitive material leading to minor exposure, or minor damage of reputation
- Loss of integrity within the system application or data, leading minimal damage of reputation; minimal loss of customer / supplier / stakeholder confidence; negligible cost of recovery
- Loss of service availability within the domain, leading to reduced ability to conduct business as usual; negligible loss of revenue; minimal loss of customer / supplier / stakeholder confidence; negligible cost of recovery

A **MAJOR** Incident will have a significant impact on The Service resulting in one of more of the following:

- Loss or unauthorised disclosure of confidential or strictly confidential material, leading to brand or reputation damage; legal action by employees, clients, customers, partners or other external parties
- Loss of integrity of the applications or data, leading to brand or reputation damage; loss of customer / supplier / client confidence; cost of recovery
- Loss of service availability for applications or communications networks, leading to an inability to conduct business as usual; loss of revenue; loss of customer / supplier / client confidence; cost of recovery

3.1 Reporting information security events

A formal information security event reporting procedure must be established, 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. This will normally result in a call to the RMGA Service Desk.

All Incidents reported to the Service Desk will be logged and given a reference and, even if classified as minor, must be forwarded to the RMGA Security Manager to determine if there is a security Impact.

All RMGA Staff should be made aware of their responsibility to report any information security events as quickly as possible to their line manager and onwards to the RMGA Security Manager. They should also be aware of the procedure for reporting information security events and the point of contact.

3.2 Reporting security weaknesses

If RMGA Staff identify or suspect that a security weakness exists anywhere in the RMGA system then they must report these matters either to their line manager or directly to RMGA Business Security Manager as quickly as possible in order to prevent information security Incidents.

POL00395097

The reporting mechanism should be as easy, accessible, and available as possible.

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 would be treated as a disciplinary issue.

3.3 Management of information security Incidents and improvements

Whenever an Incident is identified which presents a serious threat to conduct normal business it should be contained and isolated as quickly as possible. This will mean Platforms that appear to have suffered virus attack or other malicious code attack need to be quarantined immediately to prevent further spread. It may also be necessary to isolate network connections that appear to be the source for Denial of Service threats or where they have been subjected to suspected hacking attack.

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

Procedures must be established to handle different types of information security Incident, including:

- information system failures and loss of service;
- malicious code;
- denial of service;
- errors resulting from incomplete or inaccurate business data;
- breaches of confidentiality and integrity;
- misuse of information systems;

The procedures must also cover:

- analysis and identification of the cause of the Incident;
- containment;
- 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;

Audit trails and similar evidence must be collected and secured, as appropriate, for:

- internal problem analysis;
- use as forensic evidence in relation to a potential breach of contract or regulatory requirement or in the event of civil or criminal proceedings, e.g. under computer misuse or data protection legislation;
- negotiating for compensation from software and service suppliers;

Any action to recover from security breaches and correct system failures should be carefully and formally controlled; the procedures should ensure that:

- only clearly identified and authorized personnel are allowed access to live systems and data in line with the access controls policy and access guidelines [Ref:SVM/SVM/POL/0027];
- all emergency actions taken are documented in detail;
- emergency action is reported to operational management and reviewed in an orderly manner;
- the integrity of business systems and controls is restored with minimal delay.

The objectives for information security Incident management must be agreed by the RMGA Business Security Manager and the priority criteria for Incident management defined. Line mangers must ensure

POL00395097

that those responsible for information security Incident management understand the RMGA's priorities for handling information security Incidents.

3.4 Learning from information security Incidents

There must be mechanisms in place to enable the types, volumes, and costs of information security Incidents to be quantified and monitored.

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

The RMGA Security Team must carry out a check of all security Incidents investigations at at least six monthly intervals and create a summary report highlighting all Incidents to the POL Head of Information Security. The report must also highlight any trends or weaknesses which may need to be raised at future Security Forums.

3.5 Collection of evidence

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

Before undertaking security Incident investigation and computer forensics it is essential that investigators, whether internal or external, have a thorough understanding of the Rules of Evidence. The submission of evidence in any type of legal proceedings generally amounts to a significant challenge, but when computers are involved the problems are intensified. Special knowledge is needed to locate and collect evidence, and special care is required to preserve and transport evidence. Evidence in computer crime cases may differ from traditional forms of evidence in as much as most computer related evidence is intangible and is in the form of electronic pulse or magnetic charge.

In general, the rules for evidence cover:

a) Admissibility of evidence: whether or not the evidence can be used in court;

b) Weight of evidence: the quality and completeness of the evidence.

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

The weight of evidence provided should comply with any applicable requirements. To achieve weight of evidence, the quality and completeness of the controls used to correctly and consistently protect the evidence (i.e. process control evidence) throughout the period that the evidence to be recovered was stored and processed should be demonstrated by a strong evidence trail.

Incident investigation procedures must be developed which ensure 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.

POL00395097

4 Applicability

This policy applies to all of the RMGA and is mandatory for all RMGA Staff, contractors and 3rd parties who have access to RMGA facilities and systems.

4.1 Policy Review

Once approved, this policy document must be formally reviewed annually.

4.2 Compliance with this and related policies

All users of Fujitsu Services which support The Service and RMGA systems must be aware of policy details and to 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 could result in disciplinary action being taken.

4.3 Compliance with ISO27001

Fujitsu Services aims to follow internationally accepted good practice in the area of Information Security, and complies with ISO27001, the international Standard for Information Security Management.

4.3.1 RMGA Policy Controls

This Policy explicitly complies with the following controls in ISO27001:

ISO27001 control	Control Number
13.1 **Objective**: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.	
Information security events shall be reported through appropriate management channels as quickly as possible	13.1.1
All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.	13.1.2
13.2 **Objective**: To ensure a consistent and effective approach is applied to the management of information security incidents.	
Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.	13.2.1
There shall be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.	13.2.2
Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or	13.2.3

POL00395097

criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).	

Where associated policies comply with ISO27001 controls, these are indicated in the policy description.

4.4 Exemptions

These apply to both this policy and associated detailed policies:

- Activities where compliance would represent a breach of national law

Otherwise, any deviations from this policy must be approved by the Head of Information Security (where information security is involved) or the Corporate Security Manager in all other cases.

4.5 Related Policies and Documents

The following Policies support this policy and are mandatory:

Description	Document Ref;
RMGA ISMS Information Security Policy Set	SVM/SDM/POL/0023
Risk Assessment and Management Policy	SVM/SDM/POL/0026
Security Organisation and Management Policy	SVM/SDM/POL/0025
Asset Management Policy	SVM/SDM/POL/0024
Human Resources Policy (Security matters)	SVM/SDM/POL/0030
Physical and Environmental Security Policy	SVM/SDM/POL/0028
Operations and Communications Management	SVM/SDM/POL/0029
Access Controls	SVM/SDM/POL/0027
Systems Acquisition, Development & Maintenance	SVM/SDM/POL/0033
Incident Management	SVM/SDM/POL/0031
Business Continuity	SVM/SDM/POL/0032
Compliance	SVM/SDM/POL/0034

4.6 Fujitsu Services Corporate Security Policies.

Note: these policies apply to all Fujitsu Services staff and resources and must be complied with in the absence of any specific RMGA Security Policy statement. These policies may be found on Cafevik

CS1_Security and Reporting of Incidents.doc

CS2_IDENTIFICATION CARDS.doc

HRS1_SharedService.doc

ITS01_Security Organisation.doc

ITS02_Operational Use Of IT.doc

ITS03_Use_Of_Email_and_Internet_ Applications.doc

ITS04_Monitoring Of IT AND Communications.doc

ITS05_3rd Party Connectivity Policy.doc

POL00395097

ITS06_Internet Connection Policy.doc

ITS07_disposal_of_classified_data.doc

ITS08_Classifications And Privacy Markings.doc

ITS09_Security Of Portable Equipment.doc

ITS12_Server Management.doc

ITS13_Avmanagement.doc

ITS15_Application Management.doc

ITS17_Systems Audit.doc

ITS18 - Remote Access.doc

ITS19_Facility Security.doc

ITS20_Wireless Lans.doc

4.7 Policy Owner

Brian Pinder, - RMGA Business Security Manager