FUJ00235010

Document Title:	RMGA User Management Procedure
Document Reference:	SVM/SEC/PRO/0012
Document Type:	Process (PRO)
Release:	N/A
Abstract:	This document establishes the controls that RMGA has to meet to manage user access to its assets based on its contractual requirements.
Document Status:	FOR REVIEW
Author & Dept:	Bill Membery, Kirsty Gallacher
External Distribution:	N/A
Security Risk Assessment Confirmed	YES

Approval Authorities:

Name	Role	Signature	Date
Steve Denham	RMGA Head of Service Management	See Dimensions for record	
Howard Pritchard	RMGA CISO	See Dimensions for record	

See HNG-X Reviewers/Approvers Matrix (PGM/DCM/ION/0001) for guidance on who should approve.

FUJ00235010

0 Document Control

0.1 Table of Contents

FUJ00235010

0.2 Document History

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
0.1	12/12/08	Initial Draft version	N/A
0.2	27/07/09	Amended following full review	N/A

0.3 Review Details

*See HNG-X Reviewers/Approvers Matrix (PGM/DCM/ION/0001) for guidance on completing the lists below. You may include additional reviewers if necessary, but you should generally **not exclude** any of the mandatory reviewers shown in the matrix for the document type you are authoring.*

Review Comments by :	20 July 2009
Review Comments to :	Kirsty.Gallacher GRO

Mandatory Review	
Role	Name
Kirsty Gallacher	Service Support Manager
Howard Pritchard	CISO
Nigel Hatcher*	RMGA Quality Manager
Andy Dunks	RMA Security Operations
Ellie Sims	RMGA HR Representative
Optional Review	
Role	Name
Leighton Machin	Branch Services SDM
Ian Venables*	OBC/DMN Manager
Janet Reynolds	Operations Support
David Wilcox*	Reference Data Manager
Sarah Bull	Branch Services & Release Management SDM
Mik Peach*	SSC Manager
Ian Mills	Networks SDM
Mike Stewart	Online Services & SAP SDM
Claire Drake	Data centres SDM
Sandie Bothick	HSD SDM
Jim Sweeting	Security Architect
Damian McClintock	Principal Solution Architect
Issued for Information – Please restrict this distribution list to a minimum	

FUJ00235010

Position/Role	Name
Dave Jackson	Practice Head - Northern Implementations
Adrienne Thompson	Team Manager SoP Northern Ireland
Catherine Irvine	Service Manager, Network Security Support, Infrastructure Svces
Martin Mcnally	Data Centre Manager
Pete Thompson	Operations Transition Manager
Vince Cochrane	Implementation Delivery Manager -- HNG-x Programme Infrastructure Deployment

(*) = Reviewers that returned comments

0.4 Associated Documents (Internal & External)

Reference	Version	Date	Title	Source
PGM/DCM/TEM/0001 (DO NOT REMOVE)	4.0	21-Nov-2008	RMGA HNG-X Generic Document Template	Dimensions
SVM/SEC/PRO/0006	0.1		Application For Access To The Live Network	Dimensions
ARC/SEC/ARC/0003			HNG-X Technical Security Architecture	Dimensions
DES/GEN/TEM/0004			HNG-X LIVE Physical Platform Design Template	Dimensions
DES/PPS/HLD/0006			HNG-X NAMING STANDARD	Dimension
DES/PPS/HLD/0003			Active Directory HLD	Dimension
DES/SEC/HLD/0001			HNG-X Authentication HLD	Dimensions
DES/SEC/HLD/0003	1.3	05/11/2007	HNG-X Key Management High Level Design	Dimensions
DES/SEC/HLD/0004			HNG-X Authorization High Level Design	Dimensions
DES/SEC/HLD/0009			Windows server Security Settings	Dimension
DES/SYM/HLD/0020			Secure Console Access High Level Design	Dimension
DEV/APP/LLD/0028			Active Directory LLD	Dimension
DEV/GEN/SPG/0012			Active Directory Support Guide	Dimensions
DEV/INF/LLD/0059	0.1	18/01/2008	HNGX Cygwin/SSH LLD	Dimensions
PA/PRO/001			Change Management Process	Dimensions
SVM/SDM/POL/0027			Access Control Policy	Dimensions
SVM/SDM/SD/0017			Security Management Service: Service Description	Dimensions
SVM/SDM/OLA/0014			Fujitsu Standard Data Centre OLA	Dimensions
SVM/SDM/OLA/0015			OLA for Core Division Wintel & NT, Nearshore	Dimensions
SVM/SEC/PLA/0007			RMGA Security Risk Register	Dimensions

FUJ00235010

Reference	Version	Date	Title	Source
SVM/SEC/POL/0003			RMGA Information Security Policy	Dimensions
BS ISO/IEC 27001:2005			Information technology — Security techniques — Information security management systems — Requirements	External
BSI ISO/IEC 27002:2005			Information technology — Security techniques — Code of practice for information security management	External
BS/ISO IEC 20002			Contact RMGA Security for details	External
CISP			Post Office Ltd Community Information Security Policy	External

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

0.5 Abbreviations

Abbreviation	Definition
CCD	Contract Controlled Document
CISO	Chief Information Security Officer
HR	Human Resources
FS	Fujitsu Services
POL	Post Office Limited
RMGA	Royal Mail Group Account

0.6 Glossary

Term	Definition
Accountability	A Security principle that requires individuals must be identifiable.
Authenticity	Indentifying or verifying, the eligibility of a piece of hardware, software , network equipment, or individual to access specific categories of information.
Availability	The property of being accessible and usable upon demand
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals
Corrective Controls	Corrective controls involve physical, administrative, and technical measures designed to react to detection of an incident in order to reduce or eliminate the opportunity for the unwanted event to recur.
Detective controls	These use practices, processes and tools that identify and react to security violations

FUJ00235010

Term	Definition
Directive controls	These are controls used to advise employees, third parties and contractors of the behaviour expected of them during their interfaces or use of RMGA or POL's information systems.
Integrity	The property of safeguarding the accuracy and completeness of assets
Non -repudiation	A means whereby the authenticity or integrity of the information cannot be refuted
Preventative Controls	These are controls like physical, administrative, and technical measures to preclude actions violating policy or increasing risk to system resources.
Recovery Controls	These controls are used once an incident has occurred that results in the compromise of integrity or availability, these controls are implemented to restore the system or operation to a normal operating state.
Reliability	The ability of a person or system to perform and maintain its functions in routine circumstances, as well as hostile or unexpected circumstances.

0.7 Changes Expected

Changes
Details of areas other than the management of users to be included

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 because of any error or omission in the same.

0.9 Security Risk Assessment

I consider there are security risks related to the content of this document, and I will follow Fujitsu Services Risk Assessment Process as described in C-MP 1.2 on Café VIK. I have inserted into Section 0.4 (above) a cross-reference to the SVM/SEC/PLA/0007 RMGA Security Risk Register where all risks are documented and will follow RMGA Risk management framework SVM/SEC/STD/0006.

.

FUJ00235010

1 Introduction

The User Management Guidelines is to help managers and users of both physical and technical assets within the RMGA account and FS supporting functions. It sets out how accesses to these assets are to be created, managed, and removed and explains how they are to be monitored and reviewed.

1.1 Scope

This document covers buildings, rooms, networks, support, estate management, applications and tools used by RMGA and any associated third parties (external and Fujitsu internal) to provide and meet both it's contractual and regulatory obligations to Post Office Ltd.

1.2 Purpose

This document establishes the controls that RMGA has to meet to manage user access to its assets, based on its contractual requirements stated in schedule A4 (Policies and Standards), in particular the following sections:

4.1.2 "Fujitsu Services shall be compliant with ISO 27001."

4.1.4 "Fujitsu Services shall adhere to the relevant parts of the CCD entitled "Community Information Security Policy for Horizon" (RM/POL/002*) and co-operate with Post Office to assist Post Office in complying with this standard and requirement.

4.1.5 "The confidentiality, integrity, validity, and completeness of data shall be maintained throughout all storage, processes, and transmissions, including during periods of Service Failure and recovery from Service Failure."

*RM/POL/002 has since been superseded by SVM/SEC/POL/0005.

FUJ00235010

1.2.1 ISO27001

ISO 27001 has two clear sections, the clauses which are detailed in sections 4-8 and those which are guidelines as to best practices in Annexes 5.-15, usually referred to with an A preceding them.

To assist users of this document detailed in Appendix A are those clauses of ISO 27001, their reference within the standard, the area which the controls are expected to be applied to, and the details of the control and its ownership. As can be seen ownership falls throughout the whole organisation and throughout all areas of the business.

In the ISO 27001 framework the controls that we are required to meet fall into the following generic areas, People, Infrastructure, Applications, Control, Operations and Management Review and Monitoring as is in Appendix A.

1.2.2 Security Requirements

Information Security is based on a number of precepts, the most important of which are defined as being; confidentiality, integrity and availability. In addition, other properties such as authenticity, accountability non-repudiation, and reliability are involved.

These are broad categories of security controls which can be employed to provide various levels of security to guard against specific or perceived 'risks' which have been jointly identified by Post Office Ltd and Fujitsu. This document defines the policies for controlling access to the RMGA IT system in compliance with the Post Office CISP.

BS/ISO IEC 20002, "A Code of Practice for Information Security Management," is primarily concerned with management and operational controls, but also sets out a number of technical security controls. BS/ISO IEC 20002 is used as the basis of RMGA Security Policy and Procedures to define the controls used throughout RMGA.

Fujitsu Services shall operate a quality management system, which complies with BS EN ISO 9001:2008.

Controlling access to IT resources requires a combination of directive, preventive, detective, corrective, and recovery controls that are used to manage hardware, software, operations, data, media, network equipment, support systems, physical areas, and personnel. They involve both manual procedures as well as technical controls on the IT system.

Documents defining the Corporate Fujitsu (UK & Ireland) related policies, processes and procedures that are used take precedence over any RMGA documentation, are held on Café Vik at:

- Group property and Facilities management http://www.cafevik.fs.fujitsu.com/index.aspx?portal=106
- Human Resources http://www.cafevik.fs.fujitsu.com/index.aspx?portal=152
- Fujitsu Services Security (in particular Security vetting) - http://www.cafevik.fs.fujitsu.com/index.aspx?portal=107
- Risk management http://www.cafevik.fs.fujitsu.com/index.aspx?portal=227
- Data centre Access http://www.is.fs.fujitsu.com/datacentres/
- Resource requests http://toolset1.fs.fujitsu.com/InternalRequests.asp

FUJ00235010

Documentation of RMGA's own Policies, processes and procedures is held on Dimensions and follows guidance given in SVM/SEC/POL/0003 RMGA Information Security Policy and SVM/SDM/POL/0027 RMGA Access Control Policy.

This document is therefore solely a set of guidelines concerned with the way that RMGA administers those people who join, move, or leave its account.

Reference to all technical details of how this is managed is shown in the document list included in section 0.4 of this document

1.2.3 DOORS Requirements

In addition to requirements placed on RMGA by Post Office Ltd user management requirements are detailed in DOORS RMGA's internal management requirement. These can be found in ProjectWeb.

FUJ00235010

2 Process

2.1 User management

User management within the RMGA is based on the creation and control of a complete list of all personnel who work on or have access to systems on the RMGA. This list is controlled by the CS Security team, and is reviewed and updated on a monthly basis to aid any Audit that may be recorded, with the following areas considered:

Joiners – On a monthly basis, all team managers notify the CS Security team of all personnel who join the RMGA after that person has gone through the required security checks.

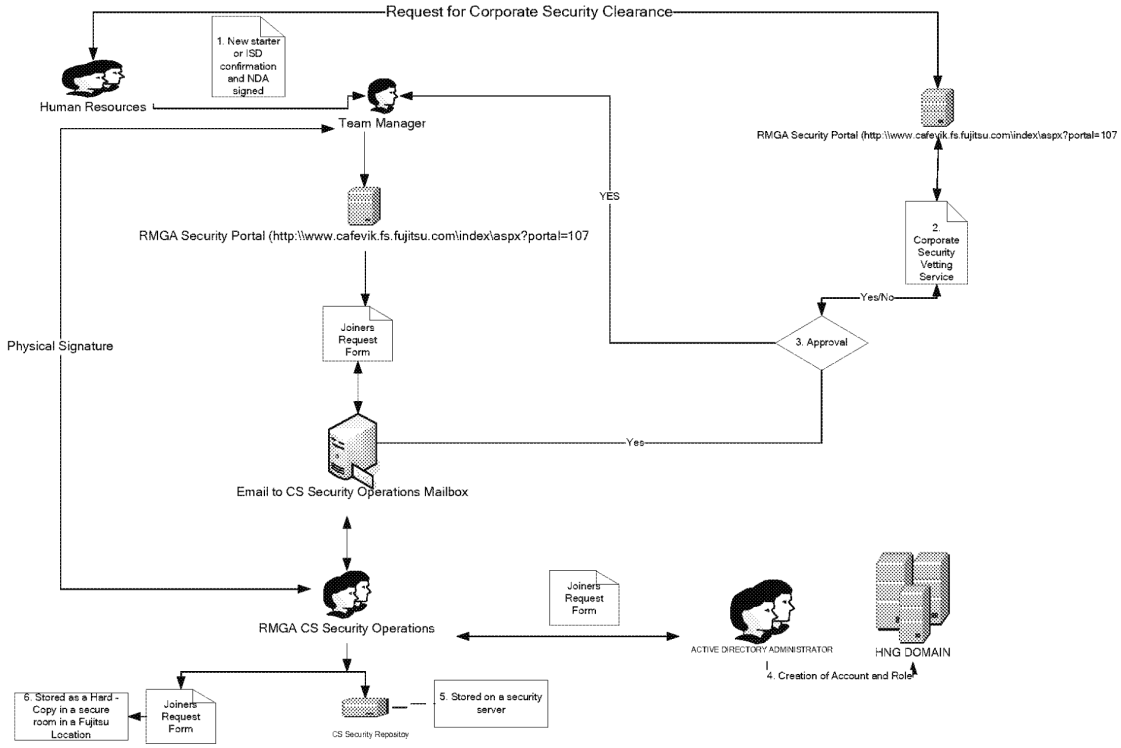
Leavers - On a monthly basis, all team managers notify CS Security team of anyone who no longer works on the RMGA. Any person who leaves the account, this list is used to check and remove any access permissions they may have had.

Movers – The CS Security team is informed of anyone who leaves one team and joins another team within the RMGA. Any person who changes their role within the account, the list is used to check that their access permission is still correct for their new role.

FUJ00235010

2.2 New Joiners

Figure 2.2 Diagram of User management for new joiners



Detailed below are the steps that must be followed prior to an individual who is new to Fujitsu Services joining RMGA.

1. Prior to an individual joining RMGA a line manager must follow HR Direct policies and procedures for a new starter these are found on the Cafevik Internal Website for Human Resources http://www.cafevik.fs.fujitsu.com/index.aspx?portal=152 and advise and guidance can be obtained from HR Professional services.

2. The line manager requesting the new person must ensure that any information passed to HR details clearly that the role, the function, and job details the individual will be undertaking. It must clearly state the person is working on the RMGA account and provide any forms required to HR and Group Security for reference checking. Details of any forms required for Security vetting are held on http://www.cafevik.fs.fujitsu.com/index.aspx?portal=107 .

3. HR will pass the forms detailing security checks to group security and they will ensure that they have Fujitsu Services basic checks and because the individual is working on the RMGA account specific Credit worthiness and Criminal Record checks. (N.B. if the individual is to work on any Government related Post Office Ltd functions there may be a requirement for additional checks and this will need to be stated by the line manager to HR)

FUJ00235010

4. The line manager will receive details back from HR confirming whether the individual is accepted or rejected in this role.
5. If the individual is rejected then HR procedures detailed at http://www.cafevik.fs.fujitsu.com/index.aspx?portal=152 will be followed and advice to the line manager can again be obtained from HR professional services.
6. If the individual is accepted into this role and requires access to the RMGA live network then the process described in SVM/SEC/PRO/006 "RMGA APPLICATION FOR ACCESS TO THE LIVE NETWORK" is followed and the form in Annex A sent by the line manager to Operational Security mailbox CSPOA Security.
7. Guidance as to the roles available and their functionality on the live network is detailed in DES/SEC/HLD/0004 HNG-X Authorization High Level Design and devgenspg0012 Active Directory Support Guide.
8. Details of this user and there role is then compared to the role definitions detailed in DES/SEC/HLD/0004 and provided they are documented in here then Operational Security will approve the individuals acceptance into the live network
9. The Operational Security will maintain a record of all users that have been approved and their roles and clearance levels and review this regularly.
10. The Operational Management of user access to the live systems is controlled under Operational Level agreements with FS SoP in Northern Ireland and is subject to OLA agreements for Data centres SDM/SDM/OLA/0014 and for NT and Unix SDM/SDM/OLA/0015 and users will then be set up using their procedures.
11. If users do not require access to the live network but other FS support systems for RMGA e.g. Dimensions, Doors, HP Openview , PEAK, Operational Change systems , then it is the responsibility of the team manager managing this function to ensure processes, procedures and work instructions are in place for the acceptance, change and removal of users from these systems. They must also ensure that the criterion for ISO 27001 compliance is available for RMGA audit.
12. In addition, Operational Security will notify Group property and Facilities management http://www.cafevik.fs.fujitsu.com/index.aspx?portal=106 to ensure that their access to dedicated RMGA locations is approved.

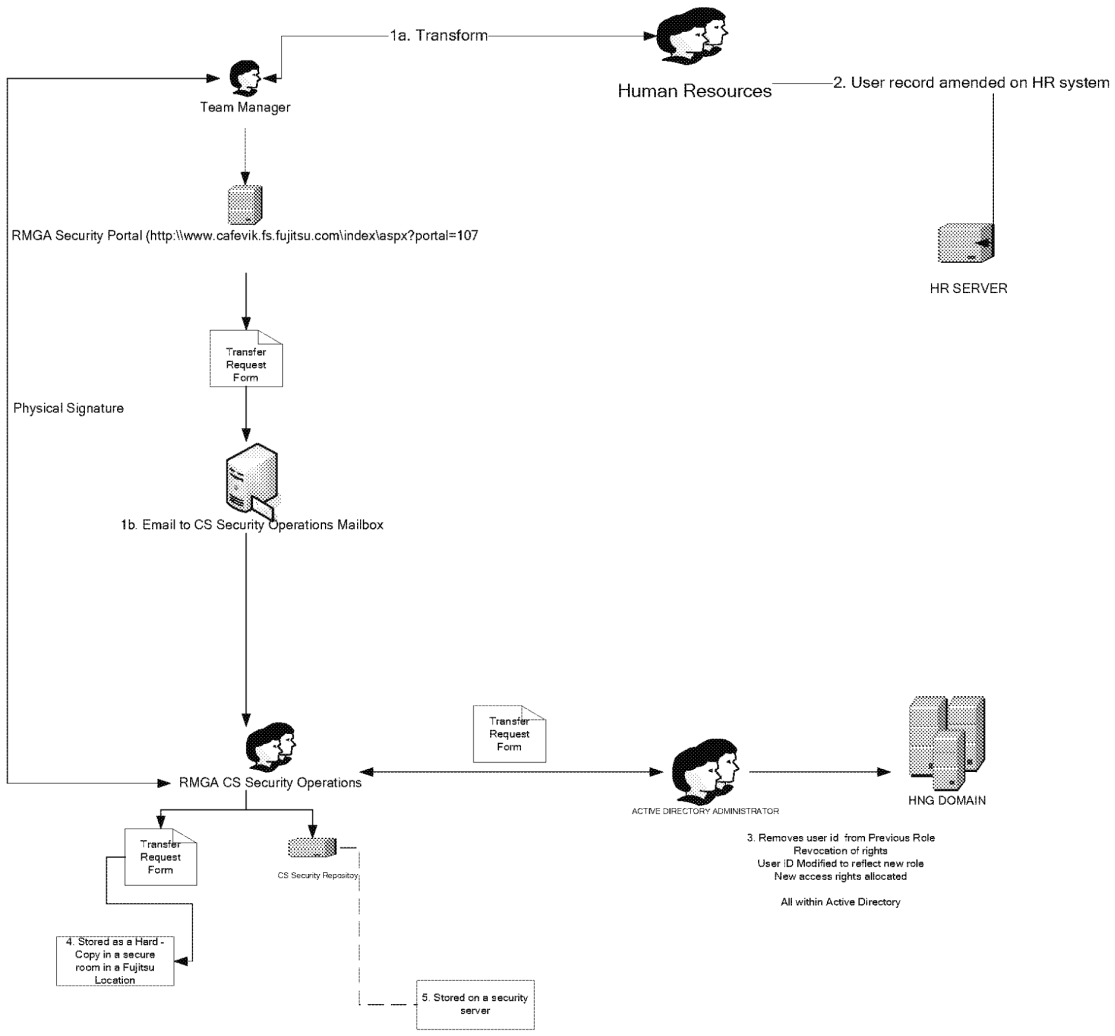
FUJ00235010

2.3 Movers

In addition to individuals who join RMGA as new staff in Fujitsu Services, there are cases where people with key skills are brought onto the account to perform specific specialist functions. This type of staff may be a contractor employed by Post Office Ltd, a third party employed by Fujitsu or an individual who belongs to another area of Fujitsu. This applies particularly to Post Office Ltd Joint test team, and individuals brought into the account from Architecture and Design practices.

In addition, individuals may change roles within the RMGA account and therefore their access will need to be reviewed.

Figure 2.3 Diagram of User management for movers



FUJ00235010

1. If a specialist is to be brought into the account then Line managers will obtain approval through RMGA's change management system to obtain the specialist resource by raising a Change Proposal as defined in PA/PRO/0001 Change Management Process.
2. Line Mangers will then apply for a RIO or Eric according to FS procedures as detailed on Cafevik at http://toolset1.fs.fujitsu.com/InternalRequests.asp and follow the corporate procedures.
3. The line manager must advise HR that these individuals are transferring into the account and provide the Eric and Rio references and the date that these individuals moved roles. The procedures for a these new RMGA staff are on the Cafevik Internal Website for Human Resources http://www.cafevik.fs.fujitsu.com/index.aspx?portal=152 and advise and guidance can be obtained from HR Professional services.
4. For any change of role, the line manager requesting the transferred person must ensure that any information passed to HR details clearly that the role, the function, and job details the individual will be undertaking. It must clearly state the person is working on the RMGA account and provide any forms required to HR and Group Security for reference checking. Details of any forms required for Security vetting are held on http://www.cafevik.fs.fujitsu.com/index.aspx?portal=107 .
5. HR will pass the forms detailing security checks to group security and they will ensure that they have Fujitsu Services basic checks and because the individual is working on the RMGA account specific Credit worthiness and Criminal Record checks. (N.B. if the individual is to work on any Government related Post Office Ltd functions there may be a requirement for additional checks and this will need to be stated by the line manager to HR). If these checks have already been undertaken as, it is an internal check then this may be skipped.
6. The line manager will receive details back from HR confirming whether the individual is accepted or rejected in this role.
7. If the individual is rejected then HR procedures detailed at http://www.cafevik.fs.fujitsu.com/index.aspx?rtal=152 will be followed and advice to the line manager can again be obtained from HR professional services.
8. If the individual is not employed by RMGA directly then they need to sign an NDA that requests them to maintain all information that they gather whilst on the account is confidential and must not go outside the account, without the specific permission of the RMGA CISO.
9. If the individual is accepted into this role and requires access to the RMGA live network then the process described in SVM/SEC/PRO/006 "RMGA APPLICATION FOR ACCESS TO THE LIVE NETWORK" is followed and the form in Annex A sent by the line manager to Operational Security mailbox CSPOA Security.
10. Guidance as to the roles available and their functionality on the live network is detailed in DES/SEC/HLD/0004 HNG-X Authorization High Level Design and devgenspg0012 Active Directory Support Guide.
11. Details of this user and their role is then compared to the role definitions detailed in DES/SEC/HLD/0004 and provided they are documented in here then Operational Security will approve the individuals acceptance into the live network
12. The Operational Security will maintain a record of all users that have been approved and their roles and clearance levels and review this regularly.
13. The Operational Management of user access to the live systems is controlled under Operational Level agreements with FS SoP in Northern Ireland and is subject to OLA agreements for Data centres SDM/SDM/OLA/0014 and for NT and Unix SDM/SDM/OLA/0015 and users will then be set up using their procedures.
14. RMGA Operational Security will be notified by the operational management team to the CSPOA Security mailbox when this has occurred and will update their records.

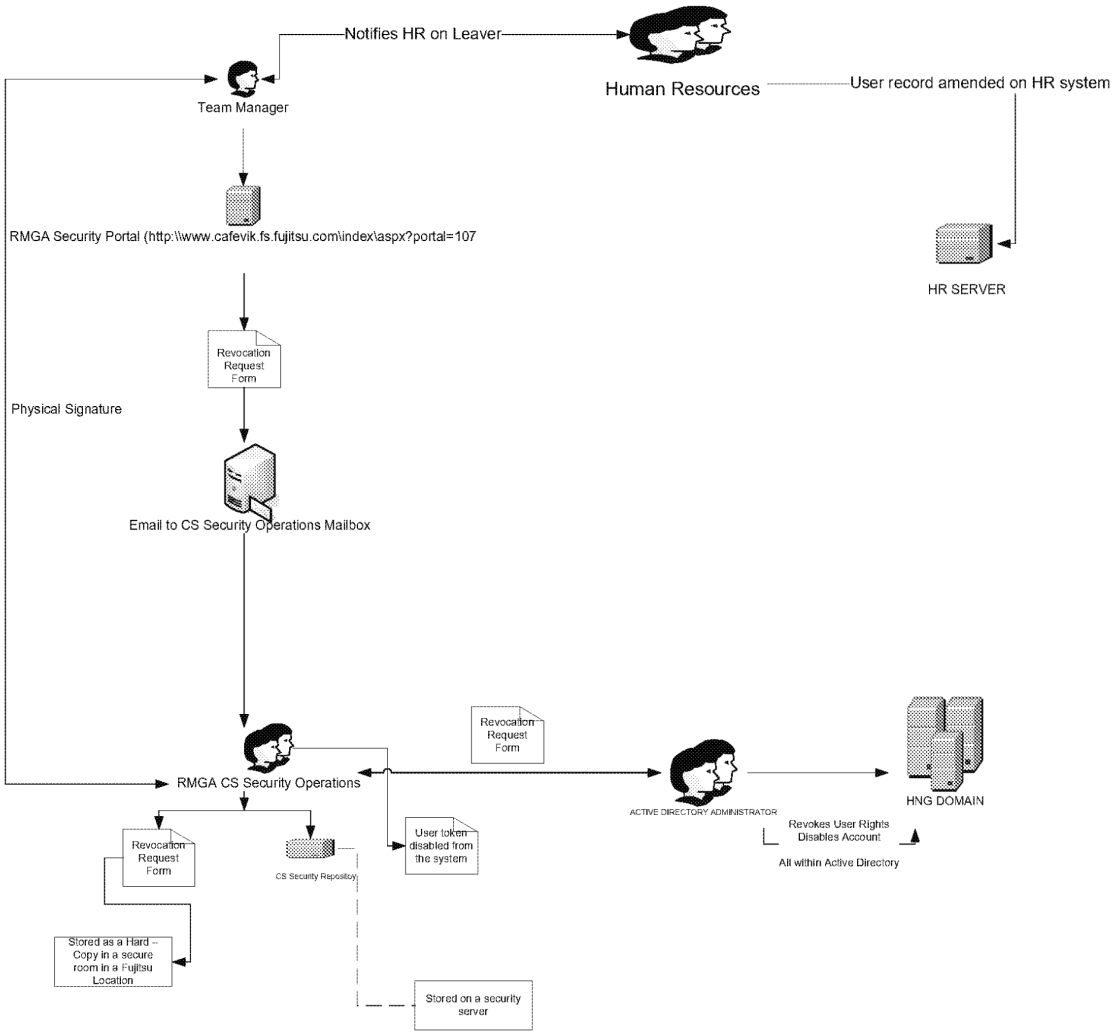
FUJ00235010

15. If users have access to the live network but other FS support systems for RMGA e.g. Dimensions, Doors, HP Openview , PEAK, Operational Change systems , then it is the responsibility of the team manager managing this function to ensure processes, procedures and work instructions are in place for the acceptance, change and removal of users from these systems. They must also ensure that the criterion for ISO 27001 compliance is available for RMGA audit.
16. In addition, Operational Security will notify Group property and Facilities management http://www.cafevik.fs.fujitsu.com/index.aspx?portal=106 to ensure that their access to dedicated RMGA locations is approved.

FUJ00235010

2.4 Leavers

Figure 2.4 Diagram of User management for leavers



1. Line managers are required to notify Human resources of an individual leaving the RMGA account
2. There are three types leavers
    a. Those whose assignment within RMGA has been completed
    b. Those who are leaving RMGA and moving to another part of Fujitsu Services
    c. Those leaving Fujitsu services completely.

FUJ00235010

3. For those individuals who fall into categories a and b above the process is the same.
    a. RMGA Operational Security must be notified by the individuals line manager that an ind`ividual has left, via the CSPOA Security mailbox.
    b. RMGA Operational Security must record the fact that the individual has left , date of leaving and the name of the manager informing them.
    c. If access to live systems has been granted, then RMGA Operational Security will advise Operational Management teams via a revocation of rights form that this user is no longer to be granted access to the live network.
    d. The Operational Management of user access to the live systems is controlled under Operational Level agreements with FS SoP in Northern Ireland and are subject to OLA agreements for Data centres SDM/SDM/OLA/0014 and for NT and Unix SDM/SDM/OLA/0015 and users will then be deactivated using those procedures.
    e. RMGA Operational Security will be notified by the operational management to the CSPOA Security mailbox when this has occurred and will update their records.
    f. The line manager must notify the team management of any support systems that this individual has access to on RMGA's behalf e.g. Dimensions, Doors, HP Openview , PEAK, Operational Change systems. Then it is the responsibility of the team manager managing this function to ensure processes, procedures and work instructions are in place for the removal of users from these systems. They must also ensure that the criterion for ISO 27001 compliance is available for RMGA audit.
    g. In addition, Operational Security will notify Group property and Facilities management http://www.cafevik.fs.fujitsu.com/index.aspx?portal=106 to ensure that their access to dedicated RMGA locations is removed.
    h. The line manager must also ensure that any dedicated RMGA assets used by this individual are returned to RMGA.
4. For those individuals who are leaving Fujitsu Services completely then the RMGA line manager must follow HR Direct policies and procedures for a termination these are found on the Cafevik Internal Website for Human Resources http://www.cafevik.fs.fujitsu.com/index.aspx?portal=152 and advice and guidance can be obtained from HR Professional services.
5. The line manager must ensure that any information passed to HR details clearly that the role, the function, and job details that the individual is leaving. It must clearly state the person was working on the RMGA account and provide any forms required by Group property and Facilities management http://www.cafevik.fs.fujitsu.com/index.aspx?portal=106 to ensure that their access to dedicated RMGA locations is removed.
6. The line manager must also notify the equipment management services team http://www.cafevik.fs.fujitsu.com/index.aspx?portal=105 so that any FS Resources are recovered

FUJ00235010

2.5 Review

1. Line Managers will review the access rights they have allocated to individuals and have evidence they have done so.
2. Operational Security will audit access rights and roles with each functional area regularly and have evidence it has done so.
3. Operational Level Agreements will be in place for all non-RMGA functions of FS involved in this process and these will be reviewed annually.
4. Operational Level agreements will include the requirement to report on joiners, movers and leavers to RMGA Operational Security monthly.
5. Senior management will review six monthly any risks relating to third parties and other areas of FS brought onto the RMGA.

FUJ00235010

2.6 Audit

All areas involved in the provision of this joiners, movers and leavers process must have records available to enable RMGA to provide evidence of the following for its ISO 27001 Compliance.

1. That any joiners movers and leavers into RMGA follow a planned process
2. Only authorised individuals have access to the assets that their role requires.
3. The access provided is managed, monitored, reviewed and controlled

FUJ00235010

3 Appendix A

Table 3 ISO 27001 Controls

ISO 27001 Section	Control Area	Control Details	Ownership	Framework Area
4.2.2 b	Implement and Operate the ISMS	Implement the risk treatment plan in order to achieve the identified control objectives, which includes consideration of funding and allocation of roles and responsibilities.	RMGA Senior Management Team	Management Review and Monitoring
4.3.3	Control of Records	Records shall be established and maintained to provide evidence of conformity to requirements and the effective operation of the ISMS. They shall be protected and controlled. The ISMS shall take account of any relevant legal or regulatory requirements and contractual obligations. Records shall remain legible, readily identifiable, and retrievable. The controls needed for the identification, storage, protection, retrieval, retention time and disposition of records shall be documented and implemented. Records shall be kept of the performance of the process as outlined in 4.2 and of all occurrences of significant security incidents related to the ISMS. EXAMPLE Examples of records are a visitors' book, audit reports and completed access authorization forms	All Management, FS HR FS Legal RMGA Commercial	Management Review and Monitoring

FUJ00235010

ISO 27001 Section	Control Area	Control Details	Ownership	Framework Area
5.1 c	Management Commitment	Management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS by: establishing roles and responsibilities for information security;	RMGA Senior Management	Management Review and Monitoring
A 6.1.2	Information security co-ordination	Information security activities shall be co-ordinated by representatives from different parts of the organization with relevant roles and job functions.	CISO HR	Management Review and Monitoring
A 6.2	External Parties	To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.	CISO Information Governance FS Legal FS Commercial Architecture and Design Security Operations	Control
A 6.2.1	Identification of risks related to external parties	The risks to the organization's information and information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access.	CISO Information Governance FS Legal FS Commercial Architecture and Design	Control
A 6.2.2	Addressing security when dealing with customers	All identified security requirements shall be addressed before giving customers access to the organization's information or assets.	CISO Information Governance FS Legal	Control

FUJ00235010

ISO 27001 Section	Control Area	Control Details	Ownership	Framework Area
			FS Commercial Architecture and Design Security Operations	
A 6.2.3	Addressing security in third party agreements	Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements.	CISO Information Governance FS Legal FS Commercial Architecture and Design Security Operations	Control
A 8.1	Human resources Prior to Employment	To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.	CISO Human Resources Information Governance	People
A 8.1.1	Roles and responsibilities	Security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with the organization's information security policy.	RMGA Senior Management Line managers FS HR	People
A 8.1.2	Screening	Background verification checks on all candidates for employment, contractors, and third party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be	FS HR	People

FUJ00235010

ISO 27001 Section	Control Area	Control Details	Ownership	Framework Area
		accessed, and the perceived risks.		
A 8.1.3	Terms and conditions of employment	As part of their contractual obligation, employees, contractors and third party users shall agree and sign the terms and conditions of their employment contract, which shall state their and the organization's responsibilities for information security.	FS HR	People
A 8.2	During Employment	To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.	FS HR CISO Information Governance Line Managers	People
A 8.2.1	Management responsibilities	Management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization.	Senior management Line managers	Control
A8.2.2	Information security awareness, education and training	All employees of the organization and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.	CISO Information Governance	People
A 8.3	Termination or change of employment	To ensure that employees, contractors, and third party users exit	FS HR Line managers	People

FUJ00235010

ISO 27001 Section	Control Area	Control Details	Ownership	Framework Area
		an organization or change employment in an orderly manner.		
A 8.3.2	Return of Assets	All employees, contractors and third party users shall return all of the organization's assets in their possession upon termination of their employment, contract, or agreement.	FS HR Line Managers	Operational
A 8.3.3	Removal of access rights	The access rights of all employees, contractors and third party users to information and information processing facilities shall be removed upon termination of their employment, contract, or agreement, or adjusted upon change.	Line managers Operational Security	Operational
A 9.1	Secure areas	To prevent unauthorized physical access, damage and interference to the organization's premises and information.	FS Facilities Management	Infrastructure
A 9.1.2	Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	FS Facilities Management	Infrastructure
A 9.1.6	Public access, delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	FS Facilities Management	Infrastructure
A.9.2.1	Equipment siting and protection	Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for	FS Facilities Management	Infrastructure

FUJ00235010

ISO 27001 Section	Control Area	Control Details	Ownership	Framework Area
		unauthorized access.		
A10.1.1	Documented operating procedures	Operating procedures shall be documented, maintained, and made available to all users who need them.	Line managers Operational Security	Control
A 10.1.4	Separation of development, test and operational facilities	Development, test, and operational facilities shall be separated to reduce the risks of unauthorised access or changes to the operational system.	Architecture and Design Change management Test	Infrastructure
A 10.4.1	Controls against malicious code	Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.	Information Governance	Control
A 10.7.4	Security of system documentation	System documentation shall be protected against unauthorized access.	Document management	People
A 10.8.3	Physical media in transit	Media containing information shall be protected against unauthorized access, misuse, or corruption during transportation beyond an organization's physical boundaries.	Line managers Operational Security	Control
A10.10.1	Audit logging	Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.	Line Managers Help Desk Operational Security	Management Review and Monitoring
A10.10.3	Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.	Architecture and Design Line managers Operational Security	Management Review and Monitoring
A 11	Access control			Control
A11.1	Business requirement for	To control access to information.	Senior Management Line Managers	Control

FUJ00235010

ISO 27001 Section	Control Area	Control Details	Ownership	Framework Area
	access control			
A11.1.1	Access control policy	An access control policy shall be established, documented, and reviewed based on business and security requirements for access.	Information governance	Control
A11.2	User access management			Management Review and Monitoring
A11.2.1	User Registration	There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.	Line Managers Operational Security	Operational
A 11.2.3	User password management	The allocation of passwords shall be controlled through a formal management process.	Line managers Operational Security	Operational
A 11.2.4	Review of user access rights	Management shall review users' access rights at regular intervals using a formal process.	Line Managers Operational Security Information Governance	Management Review and Monitoring
A 11.3	To prevent unauthorized user access, and compromise or theft of information and information processing facilities.			Control
A 11.3.1	Password use	Users shall be required to follow good security practices in the selection and use of passwords.	Users Information governance	Operational
A 11.3.2	Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.	Users Information Governance	Operational
A 11.4.1	Policy on use of network services	Users shall only be provided with access to the services that they	Information governance	Control

FUJ00235010

ISO 27001 Section	Control Area	Control Details	Ownership	Framework Area
		have been specifically authorized to use.		
A 11.4.2	User authentication for external connections	Appropriate authentication methods shall be used to control access by remote users.	Architecture and Design	Infrastructure
A 11.4.5	Segregation in networks	Groups of information services, users, and information systems shall be segregated on networks.	Architecture and Design	Infrastructure
A 11.4.6	Network connection control	For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network shall be restricted, in line with the access control policy and requirements of the business applications (see 11.1).	Architecture and Design	Infrastructure
A 11.5.2	User identification and authentication	All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.	Architecture and Design	Infrastructure
A 11.6.1	Information access restriction	Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policy.	Architecture and Design	Infrastructure
A13.1.2	Reporting Security Weaknesses	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.	Everyone	Control

FUJ00235010

ISO 27001 Section	Control Area	Control Details	Ownership	Framework Area
A15.1.5	Prevention of misuse of information processing facilities	Users shall be deterred from using information-processing facilities for unauthorized purposes.	Users	Control