FUJ00235012

Document Title:	Post Office Account User Access Work Instructions
Document Reference:	SVM/SEC/PRO/0012
Document Type:	Work Instruction
Abstract:	This document describes the controls that Post Office Account follow to manage user access to its assets, based on its contractual requirements to protect assets, systems and data.
Document Status:	APPROVED
Author & Dept:	ISM Jason Muir
External Distribution:	None
Security Risk Assessment Confirmed	YES

Approval Authorities:

Name	Role	Signature	Date
Jason Muir	Information Security Manager	See Dimensions for record	

FUJ00235012

0 Document Control

0.1 Table of Contents

FUJ00235012

FUJ00235012

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
1.0	17/07/2009	Approved version	N/A
1.1	09/02/2010	Amended CSPOA and CISO details	N/A
2.0	15/02/2010	Approval version	N/A
2.1	27/07/2010	Minor updates and improvements	N/A
2.2	27/08/2010	Insertion of new bullet in 2.5	N/A
2.3	13/10/2010	Updated in response to review comments.	N/A
3.0	25-Oct-2010	Approval version	N/A
3.1	30 Jul-2011	Amendments made to add additional responsibilities	N/A
3.2	21-09-2011	Amendment to process and additional flow diagrams added	N/A
3.3	23-Sep-2011	Prep for formal review	N/A
3.4	18-Oct-2011	Revised following review	N/A
4.0	18-Oct-2011	Approval version	N/A
4.1	27-Nov-2012	Updated with comments from POL	N/A
4.2	12- 02-2013	Updates made to process	N/A
4.3	12-Mar-2013	Amended manager role to Line/Assignment Manager.	N/A
5.0	9-Jul-2013	Approved version	N/A
6.0	16 Dec 2013	Review - Final	
6.1	03 Jun 2014	Updated after internal audit and annual review	Annual Review
7.0	06-Jun-2014	Approval version	
7.1	01-Apr-2016	Diagrams updated & aligned to Fujitsu Security Policy Manual	N/A
7.2	21-Apr-2016	Amendment to section 6.2	N/A
8.0	22-Apr-2016	Approval version	
8.1	23-Jun-2016	Minor Amendments as a result of 2016 ISO27001 audit, remove reference to paper forms, add links to forms, rationalise review and reporting sections.	N/A
9.0	28-Jun-2016	Approval version	
9.1	27-Jul-2017	Minor Amendments to document Hyperlinks as a result of SharePoint migration	N/A
10.0	28-Jul-2017	Approval version	
10.1	26-Oct-2017	Addition of TESQA & APPSUP access management	
11.0	07-Nov-2017	Approval version	
11.1	16-Jan-2019	Update to Appendix B – POA Role based Access	N/A
12.0	18-Jan-2019	Approval version	
12.1	21-Jan-2019	Update to Appendix C – List of POA systems	
13.0	22-Jan-2019	Approval version	
13.1	04-Feb-2020	Update to Section 8 Appendix C – List of POA systems	

FUJ00235012

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
13.2	30-Mar-2020	Various minor updates	
13.3	09-Jun-2020	Approval version, downgrade to LWI, update links, names	
13.4	04-Aug-2020	Changes to address remaining comments from review of 13.2	
14.0	19-Aug-2020	Approval version	

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 :	
Review Comments to :	Jason Muir and Post Office Account Document Management
Mandatory Review	
Role	Name
CISO	Steve Browell
Crypto Key Manager	Andy Dunks
Security Analyst	Niall Vincent
Security Analyst	Chris Stevens
Security Analyst	Ifran Khan
Optional Review	
Position/Role	Name
Security Operations Manager	Farzin Denbali
Quality and Compliance Manager	Bill Membery
Document Manager	Matthew Lenton
PMO	Abi Loveday; James Guy

(*) = Reviewers that returned comments

0.4 Associated Documents (Internal & External)

Reference	Version	Date	Title	Source
PGM/DCM/TEM/0001 (DO NOT REMOVE)		See Dimensions for latest version	POA HNG-X Generic Document Template	Dimensions
ARC/SEC/ARC/0003		See Dimensions for latest version	HNG-X Technical Security Architecture	Dimensions
SVM/SDM/SD/0017		See Dimensions for latest version	Security Management Service: Service Description	Dimensions
SVM/SEC/POL/0005 [POL Ref: RM/POL/002]		See Dimensions for latest version	Post Office Ltd Community Information Security Policy (CISP)	POL–owned and / Dimensions
SVM/SEC/POL/0003		See Dimensions for	POA HNG-X Information Security	Dimensions

FUJ00235012

Reference	Version	Date	Title	Source
		latest version	Policy	
SVM/SEC/STD/0026		See Dimensions for latest version	POA ISM Terms Of Reference	Dimensions
		See EMEIA Connect for latest version	Fujitsu EMEIA Security Master Policy Manual	EMEIA Connect
		See EMEIA Connect for latest version	Fujitsu EMEIA Security Policy	EMEIA Connect
		See EMEIA Connect for latest version	Minimum Security Controls – Access Management	EMEIA Connect
		NWE PAM process	http://emeia.fujitsu.local/emeia/c/P0004/Process_Maps/PAM_Process.htm	EMEIA Connect
		NEW PAM Procedure	http://emeia.fujitsu.local/emeia/sites/cdc/d/EBMS/Security/PAM_procedure.htm	EMEIA Connect

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

0.5 Abbreviations/Definitions

Abbreviation	Definition
BM	Business Management
EBMS	EMEIA Business Management System
CCD	Contract Controlled Document
CISO	Chief Information Security Officer
CISP	Post Office Ltd Community Information Security Policy
CSPOA	Post Office Account Operational Security Team
HR	Human Resources
ISMF	Joint Fujitsu and POL Information Security Management Forum known as M6
POL	Post Office Limited
POA	Post Office Account
Line/Assignment Manager	Manager responsible for resources working in their area of responsibility
System Owners	Team who maintain access to specific systems in the Post Office Account
TfSNow	Triole For Service: Help Desk Call Management System
ISM	Information Security Manager

0.6 Changes Expected

Changes
None

0.7 Accuracy

FUJ00235012

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.

0.8 Security Risk Assessment

There are no specific risks associated with the content of this document.

FUJ00235012

1 Introduction

This Post Office Account User Access Work Instruction details how access is given to both physical and technical assets within the POA and Fujitsu supporting functions, and is managed by a central point, namely the CSPOA Security Operations Team.

This document sets out how access to these assets shall be created, managed and removed and reports and monitors these requirements. The CSPOA Security Operations Team controls the access to systems and any asset dedicated to POA and receives reports from other functions within Fujitsu who provide a shared service to the account.

1.1 Purpose

This document establishes the controls that POA has to meet to manage user access to its assets, based on its contractual requirements in particular those shown below from Schedule A4 Legislation Policies and Standards:

> *4.1.2 Fujitsu Services shall be compliant with ISO 27001.*
>
> *4.1.3 Security for the Services, HNG-X Development, Associated Change Development and Equipment shall be managed and organised by Fujitsu Services in accordance with the CCD entitled POA Information Security Policy" (SVM/SEC/POL/0003) as applicable and, …the CCD entitled "Security Management Service: Service Description" (SVM/SDM/SD/0017).*
>
> *4.1.4 Security Standards Fujitsu Services shall adhere to all parts applicable to the Fujitsu domain, as defined in Section 2 Definitions of the CRD entitled "Community Information Security Policy for Horizon" (SVM/SEC/POL/0005) and co-operate with Post Office to assist Post Office in complying with this standard and requirement.*
>
> *4.1.5 Data Security The confidentiality, integrity, availability, and completeness of data shall be maintained throughout all storage, processes, and transmissions, including during periods of Service Failure and recovery from Service Failure.*

Fujitsu shall adhere to all applicable parts of the NEW Security Legal Register.

Appendix A Section 6.1 refers to the control sections required for user management in the Fujitsu EMEIA Security Master Policy Manual.

Section 9.2 explains user access management requirements and also refers to Fujitsu Corporate Procedures that are required to follow Fujitsu's EMEIA Business Management System (EBMS).

FUJ00235012

2 User System Access

2.1 Pre-requisites for allocation and removal of Access

Prior to access being requested for Post Office Account specific assets, Fujitsu HR processes for joiners and movers onto POA, including MINATO, where Shared Services are used, shall be followed.

For Shared Services, Assignment Managers will apply for resources via MINATO according to Fujitsu corporate procedures.

Once employment is confirmed the Line Manager will initiate the relevant security clearance process that is carried out by Fujitsu Group Security if the resource is new to Fujitsu. If an existing employee then clearance will already exist and will be checked by POA.

Once the individual is accepted into the role and the relevant FPVS clearance level is granted or under way, the Assignment Manager can then apply for support system accesses to be set-up and for Fujitsu Facilities management to provide physical access to relevant locations for the role.

If the individual fails clearance, HR and the Line Manager will be notified and the circumstances discussed with the POA Information Security Manager and Operational Security Manager to determine how to proceed.

In addition, if an individual moves away from POA or leaves Fujitsu then the Fujitsu HR processes are to be invoked by the individual's Line/Assignment Manager, and the CSPOA Security Operations Team notified of this to ensure revocation of their access from all POA specific assets.

For those individuals who are leaving Fujitsu Services completely, the Line/Assignment Manager must follow HR policies and procedures for a termination. These can be found on EMEIA Connect.

All 3rd party access also follows the same guidance as detailed in this document.

2.2 CSPOA User Registry

The User Access Process on the POA is based on the creation and control of a registry of all personnel who work on the account.

This register is controlled by the CSPOA Security Operations Team, and is maintained and updated in line with requests being submitted and tracks all personnel working on the account, the system access they have been given, and any security clearance level that they have been granted. It is also subject to a monthly review as described in section 5.1

It will also aid any audit that may be required, by providing the details of personnel and access levels granted.

The Post Office Account User Access Database (Secure and Restricted access) holds the information about each individual who have been granted access and the systems that they have been granted access to. In addition it contains details of the requestor, and dates that this access was granted and revoked. Details of the systems held within this registry are shown in Appendix C.

FUJ00235012

3 Roles

Role	Account or Corporate	Function
HR	Fujitsu Corporate	Process Starters, movers and Leavers to Fujitsu
Site Facilities	Fujitsu Corporate	Process passes to allow access to Fujitsu buildings and rooms
Group Security	Fujitsu Corporate	Process clearances for individuals joining Fujitsu including special clearances for those joining POA.
Line/Assignment Managers	POA	Manager responsible for resources working in their area of responsibility
System Owners	POA / Fujitsu Corporate	Teams that maintain access to specific systems for the Post Office Account
CSPOA Security Operations Team	POA	The team on POA that manage, control and report on both physical and system access.
CISO (if appointed)	POA	The individual responsible for all aspects of Security on POA.
Information Security Manager	POA	The individual responsible for all aspects of Security on POA in the absence of a CISO.
Fujitsu Test Managers	POA	POA Test Managers who work jointly with POL Test Teams
User Management Team (part of Programme Management Office)	POA	Responsible for organising and maintaining Account induction. Review and report on Joiners, Movers and Leavers
Contractor/Third Party	Supplier	An organisation or person that is not a member of Fujitsu or POL staff
POL Staff	POL	An individual that is employed by POL
POL Test and Release Managers	POL	POL staff who work jointly with POA Test Teams

FUJ00235012

4 Processes

4.1 Post Office Account New Joiner

Detailed below are the steps that must be followed for an individual who is new to Fujitsu Services and/or joining the POA from another area within Fujitsu and these are shown in the Figure 1.0 Diagram of User System Access Process Flow for New Joiners/movers.

1. The Assignment Manager should complete the latest New User Access Form from the POA Security Operations PORTAL and complete all information required and return to CSPOA Security Operations Team by emailing to CSPOA.Securit GRO

2. The New User Access Form must be completed and returned in the following manner:

    - The Line/Assignment Manager shall complete all information on the form for the required individual and then email the completed form to POA Security Operations.
    - Where a New User form is completed by or on behalf of a new user, the Line/Assignment Manager must be copied in (cc'd) on the email request as a means of awareness & authorisation.

3. CSPOA Security Operations Team shall check the form is completed correctly, and in line with NEW Fujitsu Security Policy. If any information is missing or incorrect then the form will be rejected and returned to the Line/Assignment Manager to amend.

    - The new starter form has a "Start Date" stated on the form, however POA Sec Ops may receive a completed form well in advance of the start date by some weeks. In this case POA Sec Ops hold onto the form and set a Outlook reminder to not process the access request until a maximum of one week prior to the requested date.

4. CSPOA will check that FPVS Security Clearance is in place or has started.

5. When a correct form has been received and checked, and clearance in place/started then the CSPOA Security Operations Team shall arrange for all relevant access to be set up for the user.

6. CSPOA Security Operations Team shall notify the relevant system owners via an e-mail (which is generated from the user management database). A TfSNow call will be raised for back-end system requirements and a copy of the completed request form will be attached to the TfSNow call, where required.

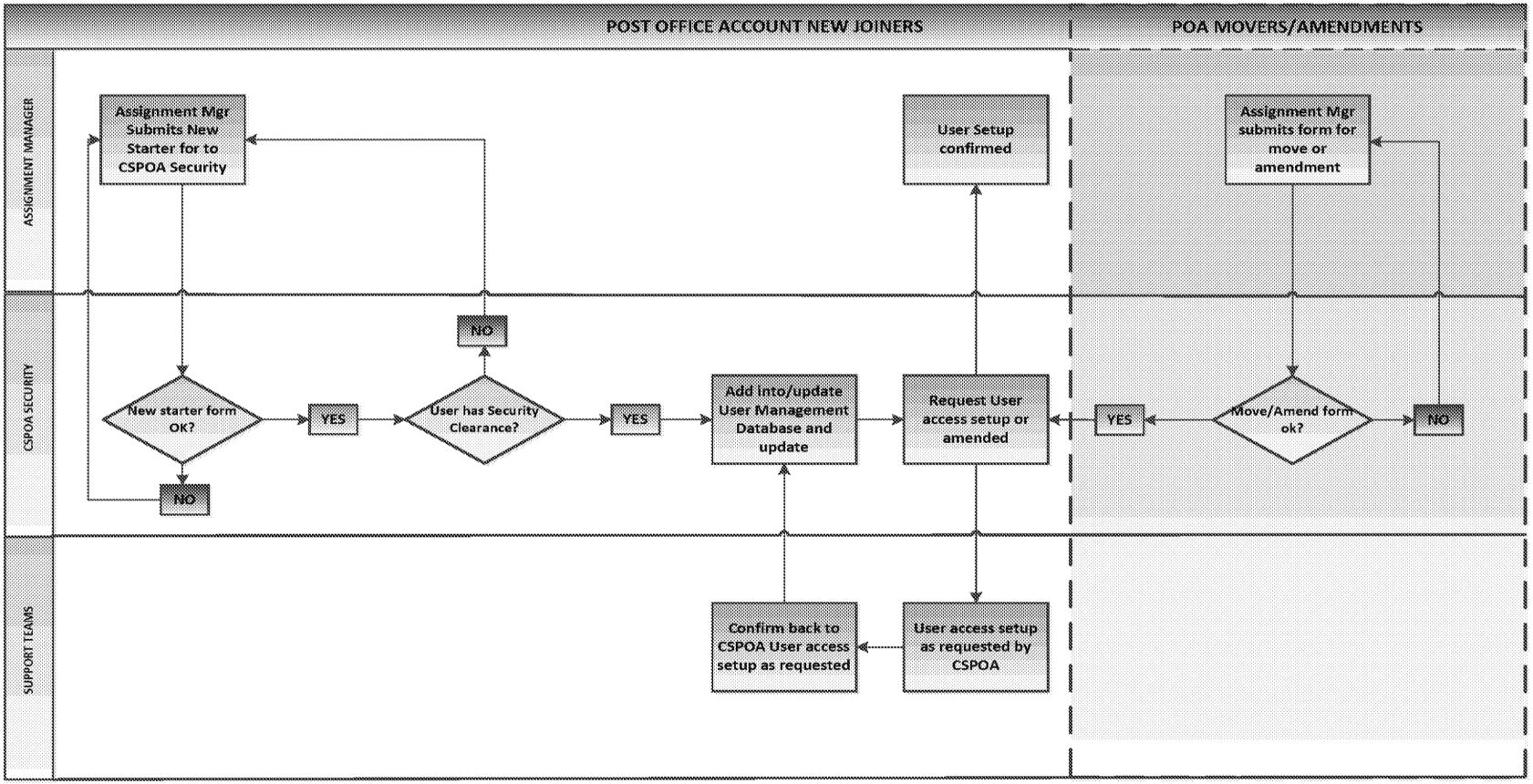
7. The System Owners shall follow their own processes and work instructions to configure the user.

8. CSPOA Security Operations Team shall then close the TfSNow call and update the register.

9. All forms and records are securely stored electronically, and kept for audit purposes..

FUJ00235012

Figure 1.0 Diagram of User System Access Process Flow for New Joiners



FUJ00235012

4.2 Moving within POA or amendment to access

In addition to individuals who join POA as new staff to POA and/or Fujitsu, there are cases where people are moved within the POA. The Assignment Manager should complete the latest new Mover form from the POA Security Operations PORTAL and complete all information required and return to CSPOA Security Operations Team by emailing to CSPOA.Security GRO

Details of the process flow are shown in the Figure 1.0 Diagram of User system access flow under the POA Movers/Amendments heading on the right hand side.

4.2.1 Fujitsu Staff not on the POA

For any Fujitsu shared services that are provided to POA, the Line Manager shall notify the CSPOA Security Operations Team of the relevant Assignment Manager on the account. The Assignment Manager shall then follow the process in Section 4.1 for obtaining access to the relevant systems for the user.

4.2.2 POL Staff and 3rd parties

Post Office Ltd staff (and 3rd parties) that are provided with access to Fujitsu systems are the responsibility of POL to verify and authenticate, and to ensure that appropriate access has been granted. Access should be granted as detailed in section 4.1 but replacing Line Manager with Post Office assigned line manager.

4.2.3 Requests for TESQA & APPSUP access elevated privileges

The APPSUP role and TES_TESQA_USER accesses are temporarily applied to user accounts when required for investigations into TESQA & BDB queries. The roles are then removed again once work is complete. Temporary access is managed via change control (TfS) and that it should reference a Peak/TfSNow Change reference as justification on the requirement for the elevated access. Access is only granted upon approval of Post Office, Fujitsu require three written approvals from POL (Service, Security, Commercial). This approvals process is managed by POA Service team. Details of the approvals are added to the associated TfS ticket.

4.3 Leavers

Detailed below are the steps that must be followed prior to or upon an individual leaving the POA, and these are detailed in the Figure 1.2 Diagram of User system access flow for Leavers.

4.3.1 POL Staff

Post Office Ltd staff that are provided with access to Fujitsu systems are the responsibility of POL. Access should be revoked as detailed in section 4.3.3 but replacing Line Manager with Post Office Assigned Line manager.

4.3.2 Staff who are leaving Fujitsu

Detailed below are the steps that must be followed for an individual who is leaving Fujitsu Services and/or the POA and these are shown in the Figure 1.2 Diagram of User system access flow for Leavers.

FUJ00235012

1. The Line/Assignment Manager shall contact CSPOA Security Operations Team by e-mail providing the leaver's details and complete the necessary form from the POA Web PORTAL page.

2. The Revocation form must be completed and returned in the following manner:

    - The Line/Assignment Manager shall complete all information on the form for the required individual and email the completed form to POA Security Ops' button

    These forms shall be filed and stored securely, and kept for audit purposes.

3. CSPOA Security Operations Team shall check the form is completed correctly. If any information is missing or incorrect then the form will be rejected and returned to the Line/Assignment Manager to amend.

4. When a correct form has been received and checked then the CSPOA Security Operations Team shall arrange for all relevant access to be removed for the user.

5. CSPOA Security Operations Team shall arrange for floor/door access to be revoked using Fujitsu Corporate Processes using an automated function from the CSPOA Security Operations database.

6. CSPOA Security Operations Team shall notify the relevant system owners via an e-mail, and where backend system access is held, a TfS call shall be raised and progressed to the system owners requesting revocation of access.

7. The System Owners shall follow their own processes and work instructions to remove the user, confirm revocation to CSPOA and CSPOA will update the TfS call.

8. CSPOA Security Operations Team shall then close the TfSNow call and update the register and confirm with relevant teams that access has been revoked.

4.3.3 Staff who are terminated with immediate effect

For those users whose employment is terminated either from the POA or Fujitsu Services with immediate effect, the Line/Assignment Manager must immediately contact HR and the CSPOA Security Operations Team via telephone and then follow the Fujitsu Corporate Leaver's Process making sure all the relevant forms are completed. The process in Section 4.3.2 is applied retrospectively to individuals that are terminated with immediate effect.

4.3.4 Fujitsu staff whose assignment with POA has been completed

For all Fujitsu shared services provided to POA the Assignment Manager shall notify the Line Manager of the expiry of the individual's assignment to the account. The Assignment Manager shall then follow the process in Section 4.3.2 for removing access to the relevant systems for the user.

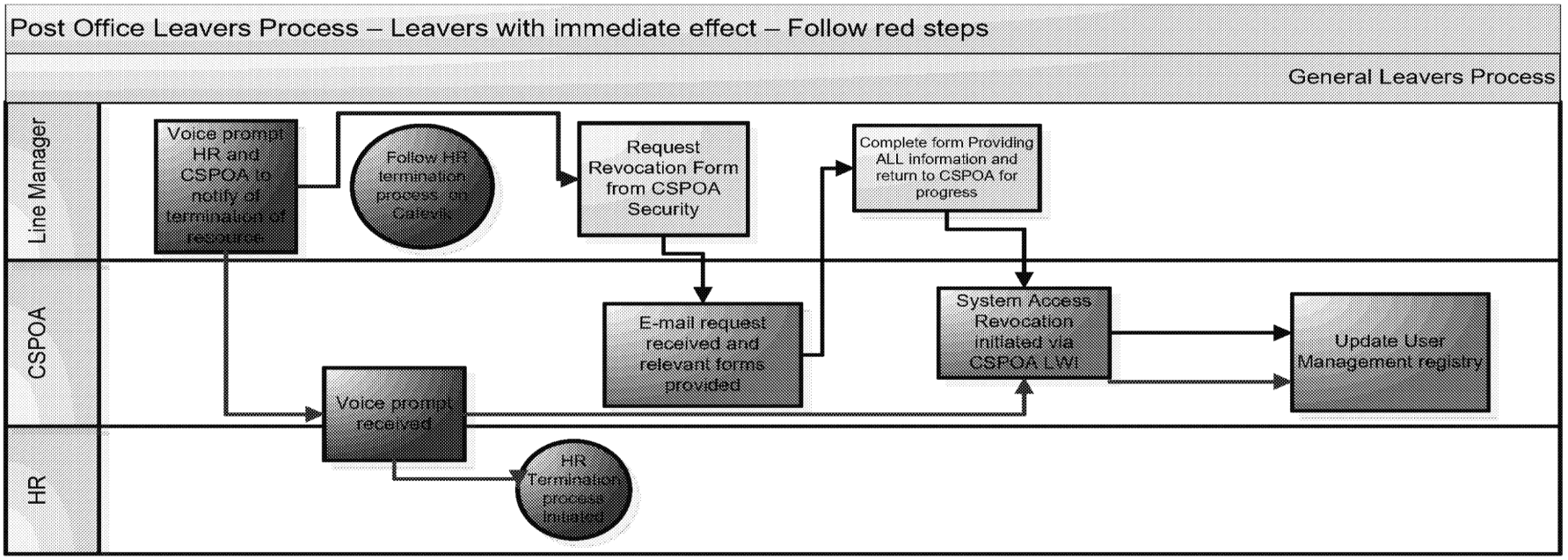
4.3.5 POA staff who are moving to another part of Fujitsu

Line/Assignment Managers whose staff are directly employed as part of Post Office Account and move to another part of Fujitsu shall follow the process in Section 4.3.2 for the termination of user's rights that are associated directly with systems dedicated to POA.

FUJ00235012

Figure 1.2 Diagram of User system access flow for Leavers

Leavers with Immediate Effect is covered in RED



FUJ00235012

5 Management

Key steps within this User Access Procedure are reviewed, reported and audited to ensure that it is functioning effectively and efficiently. Below are the details of how this is achieved.

5.1 Review

The POA User Management Team shall undertake a monthly review of the access granted to individuals and its continued appropriateness.

To achieve this:

1. POA User Management Team shall produce details of all users contained in the registry and their access levels and shall email these to the relevant Line/Assignment Managers.
2. Line/Assignment Managers shall review whether the current access of their employees is still in line with their job role.
3. Line/Assignment Managers shall consider whether any users require their access be amended and they shall follow the process defined in Section 4.2 to do so.
4. Line Mangers shall confirm each employee's current access rights requirements and shall email these details to POA User Management Team within 10 working days of receipt of the original e-mail from POA User Management Team.
5. CSPOA Operational Security will audit access rights and roles with each functional area; audits will be conducted on a minimum monthly basis.
6. CSPOA security will review all human accounts that have HNG-X live access for accounts that have been unused for a period of 90 days or over.
7. CSPOA security will review individuals added to the Ikey Exemption List.
8. CSPOA security will review Joiners, Leavers and movers to the Account.
9. Card swipe/floor access attempts report.

5.2 Reporting

Post Office User Management Team provide a report on a monthly basis detailing all joiners, leavers and movers on the Account.

5.3 Audit

All areas involved in the processes detailed in Section 4 must have records available to enable POA to provide evidence of the following for audit purposes.

1. That any joiners, movers and leavers into POA follow the planned Processes in Section 4
2. Only authorised individuals have access to the assets that their role requires
3. The access provided is managed, monitored, reviewed and controlled.

FUJ00235012

6 Appendix A

6.1 Fujitsu EMEIA Master Security Policy Manual

All framework controls that we are required to meet are detailed in full in the Fujitsu EMEIA Security Policy Manual, which aligns to ISO27001:2013, and also follows the Fujitsu Minimum Security Controls Framework.

6.2 Security Requirements

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 are held on EMEIA Connect at:-

- EMEIA Security Master Policy: GRO
- Security Policy Manual: GRO
- Minimum Security Controls GRO GRO

Post Office Account's own policies, processes and procedures are held on Dimensions and follows guidance provided in the Fujitsu EMEIA Master Security Policy Manual which is aligned to ISO27001:2013.

7 Appendix B: POA Role-based Team access

POA system access is governed on a role based structure so individual's access is pre-determined by their Team membership. See Team Access below for the corporate systems applicable on an individual team basis

Team Access.xlsx

8 Appendix C: List of POA systems

See below a complete list of all systems managed by POA Security Operations under their Joiners, Movers & Leavers Process with attached Excel file for Azure systems administration.

FUJ00235012

System
Annual Leave Calendar
Azure - Development
Azure - EPaaS
Azure AD Global Admin (Restricted)
Azure ADNP
Azure ADPR
Azure Confluence (AD)
Azure Github (AD)
Azure Jira (AD)
Azure Nexus (AD)
Azure POUK01
BCMS
CACTI
CISCO Prime (NCP)
Confluence (APT)
Database Access
DEV Lan to Integration/SVI
Dimensions 12
DRS Workstation
Floor Access
FMNOS Platform
Fortinet Firewalls
Franjiban
GDC Jump Box POL Azure
HORice
Impacting Tool
ITG Network Access
Jenkins (APT)
Jira (APT)
Juniper SRX
MSAD
MSAD (Terminal Services Only)
PEAK
POUK01 Root Management Group
Quality Centre
Qualys
Rig Owner Account (02 account)
SCM Workstation Users
Shared TfSNow
Sharepoint

FUJ00235012

Slack
Spectrum (NCS)
Spinnaker
Splunk
SVN/APT
TACACS
Tesqa
Test Rig Access
TfSNow - Change
TfSNow - Incidents
Tivoli
Tripwire
VMware vCentre

POA Systems v0.9.xlsx

FUJ00235012

Appendix D: URL for user access forms

The latest user access forms to be used can be found as detailed in the URL's below.

8.1 New user access form

A copy of the new user form can be found here:

GRO

8.2 Revocation Form

A copy of the Revocation form can be found here:

GRO

8.3 Mover Form

A copy of the mover form can be found here:

GRO

9 Appendix E: Live Systems Emergency Access

If emergency access is required for a user to the live system, then the request needs to be approved by the requestor's assignment manager - this in turn then needs to be approved by the Sec Ops Manager (or alternative cover such as CISO or other Manager as agreed cover), the request cannot be actioned until we have approval.

Once approved by all parties a TfSNow call needs to be raised and sent to POA-NT Team for MSAD account to be created/re-instated and approval email MUST be attached to the call, it is imperative that how long the access is required is stated on the call. CSPOA Security will then need to call NT Team to inform them of the request.

The emergency access request then shall be updated on the User Management Database and will need to be recorded as 'Users with heightened Privileges'.