



Post Office Account User Access Guide
**FUJITSU RESTRICTED (COMMERCIAL IN
CONFIDENCE)**



Document Title: Post Office Account User Access Guide

Document Reference: SVM/SEC/PRO/0012

Document Type: Guide

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: Jack Steptoe

External Distribution: None

Information Classification: See section 0.8

Approval Authorities:

Name	Role	Signature	Date
Steven Browell	Chief Information Security Officer	See Dimensions for record	



Post Office Account User Access Guide
**FUJITSU RESTRICTED (COMMERCIAL IN
CONFIDENCE)**



0 Document Control

0.1 Table of Contents

0	DOCUMENT CONTROL	2
0.1	Table of Contents	2
0.2	Document History	4
0.3	Review Details	5
0.4	Associated Documents (Internal & External)	6
0.5	Abbreviations/Definitions	7
0.6	Changes Expected	8
0.7	Accuracy	8
0.8	Information Classification	8
1	INTRODUCTION	9
1.1	Purpose	9
2	USER SYSTEM ACCESS	10
2.1	Pre-requisites for allocation and removal of Access	10
2.2	CSPOA User Database	10
2.3	Privileged Access Management (PAM)	12
3	ROLES	13
4	PROCESSES, PROCEDURES & CONTROLS	14
4.1	Joiners	14
4.1.1	Fujitsu Staff not on the POA	17
4.1.2	POL Staff and 3 rd parties	17
4.2	Moving within POA or amendment to access	18
4.2.1	Requests for TESQA & APPSUP access elevated privileges	18
4.2.2	Emergency Access to Live Systems	18
4.3	Leavers	18
4.3.1	Staff who are terminated with immediate effect	20
4.3.2	Fujitsu shared services staff whose POA assignment has been completed	20
4.3.3	POA staff who are moving to another part of Fujitsu	20
4.3.4	POL Staff	20
4.4	Privileged Access	20
4.5	Break Glass Accounts	20
4.6	Requesting a new High Privileged Account	20
4.6.1	Verification Process	20
4.6.2	Adding access and controls	21
4.6.3	Updating the PAM Register	21
5	MANAGEMENT	22
5.1	Review	22
5.1.1	Team Verification (Standard User Access Verification)	22
5.1.2	Privileged User Access Verification	24
5.1.3	Floor Access (Dedicated POA areas)	25
5.1.4	Other Access	25
5.1.5	Other CSPOA Regular Checks	26
5.2	Information Security Management Review (ISMR)	26



Post Office Account User Access Guide
FUJITSU RESTRICTED (COMMERCIAL IN
CONFIDENCE)



5.3	Audit	26
-----	-------------	----



Post Office Account User Access Guide
FUJITSU RESTRICTED (COMMERCIAL IN
CONFIDENCE)



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	



Post Office Account User Access Guide

FUJITSU RESTRICTED (COMMERCIAL IN CONFIDENCE)



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	
14.1	25-Aug-2021	Amended CSPOA details Diagrams updated Amendment to section 4.2.3 Amendment to section 5.1 Update to Appendix B – POA Role based Access	
14.2	08-Sep-2021	Changes to address comments from review of 14.1	
14.3	20-Sep-2021	Changes to address comments from review of 14.2 Removed Appendices and incorporated the text into the body of the document. Added screenshots to various sections. Added section 5.1.5 (CSPOA Spot Checks)	
14.4	27-Sep-2021	Changes to address comments from review of 14.3	
14.5	04-Oct-2021	Changes to address comments from review of 14.4	
15.0	18-Oct-2021	Approval version	
15.1	09-May-2022	Amended ISM details Amendments to section 4.3	
15.2	31-Aug-2022	Amended the approval Authority Amended sections 1.1, 2.2 and 4.3 following review	
16.0	01-Sep-2022	Approval version	
16.1	13-Mar-2023	Refined Privileged Access process. Links to other documents added. Minor typo and grammar edits. Links checked and correctly described. Headers and Footers fixed to link to previous.	
16.2	14-Mar-2023	Updated system table and abbreviations	
16.3	15-Mar-2023	Changes to address further comments from review of 16.2	
17.0	17-Mar-2023	Approval version	
17.1	09-Jun-2023	Addition of section 4.6 Requesting a new High Privileged Account	
17.2	20-Jun-2023	Corrections and insertion of additional information in sections 4.6.1, 4.6.2, 4.6.3, following review comments.	
18.0	20-Jun-2023	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:	jack.steptoer GRO and PostOfficeAccountDocumentManagement GRO
Mandatory Review	



Post Office Account User Access Guide
FUJITSU RESTRICTED (COMMERCIAL IN
CONFIDENCE)



Role	Name
CISO	Steven Browell
Security Governance Manager	Chris Stevens
Security Operations Manager	Farzin Denbali
Optional Review	
Position/Role	Name
Document Manager	Matthew Lenton
PMO User Management Team	James Guy
Security Analyst	Ifran Khan
Security Analyst	Beverly Brown
Security Analyst	Jack Steptoe
Security Analyst	Hassan Shakeel
Security Analyst	Idunnu Aganna

(*) = 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 latest version	POA HNG-X Information Security Policy	Dimensions
SVM/SEC/STD/0026		See Dimensions for latest version	POA ISM Terms Of Reference	Dimensions
SVM/SDM/PRO/4293		See Dimensions for latest version	Horizon Data Changes Process Work Instruction	Dimensions
SVM/SEC/POL/4538		See Dimensions for latest version	POA Privileged Account Policy	Dimensions
SVM/SEC/PRO/4537		See Dimensions for latest version	POA Privileged Account Release Procedure	Dimensions
Legal Register for Information Security		See EBMS	Fujitsu Legal Register for Information Security	NWE Connect
Ask Security		See NWE Connect for latest version	Fujitsu Europe Security Master Policy	Ask Security
Ask Security		See NWE Connect for latest version	Fujitsu Europe Security Policy Manual	Ask Security
Ask Security		See NWE Connect for latest version	Minimum Security Controls Framework – Access Management.	Ask Security



Post Office Account User Access Guide
FUJITSU RESTRICTED (COMMERCIAL IN
CONFIDENCE)



Reference	Version	Date	Title	Source
Europe Privileged Access Management Process		See EBMS	Europe Privileged Access Management Process	NWE Connect
Europe Privileged Access Management Work Instruction		See EBMS	Europe Privileged Access Management Work Instruction	NWE 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
APT	
AWS	Amazon Web Services (Post Office Cloud)
BCMS	Branch Change Management System
BM	Business Management
CACTI	Open Source - Network Analysis Tool
CCD	Contract Controlled Document
CISO	Chief Information Security Officer
CISP	Post Office Ltd Community Information Security Policy
CSPOA	Cyber Security Post Office Account (Operational Security Team)
DXC	Corporate Data Exchange Proxy
DXI	Internet Data Exchange Proxy
EBMS	Europe Business Management System
EFT	Electronic Funds Transfer
HORice	Horizon Information Centre
HR	Human Resources
IRE11/IRE19	Fujitsu Belfast Data Centres
ISM	Information Security Manager
ISMR	Fujitsu internal Information Security Management Review meeting
ITG	Information Technology Group
ITM	IBM Tivoli Monitoring
Line/Assignment Manager	Manager responsible for resources working in their area of responsibility
LT	Leadership Team (the Delivery Executive and direct reports)
Minato	The resource management platform for authorised Fujitsu NWE users
MSAD	Microsoft Active Directory
MSSQL	Microsoft Structured Query Language
MVM	McAfee Vulnerability Manager
NCP	Network Management Toolset server
NSM	McAfee Network Security Manager



Post Office Account User Access Guide
**FUJITSU RESTRICTED (COMMERCIAL IN
CONFIDENCE)**



Abbreviation	Definition
NWB	Network Banking
OEM	Oracle Enterprise Manager
PAM	Privileged Access Management
POL	Post Office Limited
POA	Post Office Account
SMC	Fujitsu Systems Management Centre
SMP	Service Management Portal
System Owners	Team who maintains access to specific systems in the Post Office Account
TACACS	Terminal Access Controller Access Control System
TESQA	Transaction Enquiry Service Query Application
TfsNow	Triole For Service: Help Desk Call Management System
TPM	Tivoli Provisioning Manager

0.6 Changes Expected

Changes
None

0.7 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.

0.8 Information Classification

The author has assessed the information in this document for risk of disclosure and has assigned an information classification of FUJITSU RESTRICTED (COMMERCIAL IN CONFIDENCE).



Post Office Account User Access Guide
**FUJITSU RESTRICTED (COMMERCIAL IN
CONFIDENCE)**



1 Introduction

This Post Office Account User Access Guide details how access is given to both physical and IT system assets within the Post Office Account (hereafter referred to as POA) and Fujitsu supporting functions, and is managed by a central point, namely the Cyber Security POA(CSPOA) Operations Team.

This document sets out how access to these assets shall be created, managed, removed and how these requirements are reported and monitored. CSPOA 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 POA.

1.1 Purpose

This document establishes the controls that POA must meet to manage user access to its assets, based on its contractual requirements, in particular those 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 Fujitsu Legal Register for Information Security.

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 and technical controls on the IT system. The Fujitsu Europe Business Management System (EBMS) outlines the processes to be followed to create, amend, and revoke Privileged Access for a given account. The Fujitsu Corporate Procedures below follow EBMS.

All framework controls that POA is required to meet are detailed in full in the Fujitsu Europe Security Policy Manual, which aligns to ISO27001:2013, and follows the applicable Fujitsu Europe Minimum Security Controls Framework – Access Management.



Post Office Account User Access Guide
**FUJITSU RESTRICTED (COMMERCIAL IN
CONFIDENCE)**



2 User System Access

2.1 Pre-requisites for allocation and removal of Access

Prior to access being requested for POA specific assets, Fujitsu HR processes for joiners and movers onto POA, shall be followed.

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

Once employment has been confirmed, the appropriate security clearance is initiated and managed by Fujitsu Group Security. If an existing employee, then clearance will already exist. Note that there is no POA specific security clearance required.

Once the individual has been accepted into the role, the Assignment Manager can apply for access to the support systems 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 Security Governance Manager and Security Operations Manager to determine how to proceed.

In addition, if an individual moves away from POA or leaves Fujitsu, the Fujitsu HR processes are to be invoked by the individual's Line/Assignment Manager, and CSPOA notified, 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 AskHR.

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

2.2 CSPOA User Database

The User Access Process on the POA is based on the creation and maintenance of a User Access Database (Secure and Restricted access) of all personnel who work on POA.

This database is controlled by CSPOA and is maintained and updated in line with requests being submitted. It tracks all personnel working on POA, details of the requestor, the system access they have been given, dates access was granted and revoked and any security access level they have been granted. It is also subject to a monthly review as described in section 5.1.

The database also aids any audit that may be required, by providing the details of personnel and access levels granted.

Below is an example from the User Access Database (with redactions as necessary) showing the system access granted to the user. Other tabs (Events, Security Info, Floor Access, MSAD and Network Drives) will show any additional system access and security access.

[illegible]

CSPOA manage the following systems under their Joiners, Movers and Leavers Process:

System	Environments
Annual Leave Calendar	
APT Access (includes Jira, Confluence, SVN/APT)	
Atlassian/Jira Cloud	
AWS Access	Integration, Development, Non-Production and Production
BCMS	
Bigfix	SV&I, LST and Live
CACTI	LST and Live
Cisco Prime (NCP)	LST and Live
Oracle and MSSQL Databases	SV&I, LST and Live
Dimensions 14	
DXC SMP	
DXI (001-004)	
Franjiban	
HORIce	LST and Live
Impacting Tool	
Ingenico e-Portal	LST and Live
Ingenico My Service	
ITG Network Access	
ITM	SV&I, LST and Live
MSAD	DXT, SV&I, LST and Live
MVM Vulnerability Scanner	



Post Office Account User Access Guide
FUJITSU RESTRICTED (COMMERCIAL IN
CONFIDENCE)



Netcool	SV&I, LST and Live
Network Security Manager (NSM)	
Nineveh IRE19	
OEM	SV&I, LST and Live
PEAK	
Reconciliation EFT Workstation	
Reconciliation NWB Workstation	
Shared TfSNow	
SharePoint & POA Teams (UK-POA)	
SMC Website (Admin)	
Spectrum (NCS)	
TACACS	LST and Live
TBSM	SV&I, LST and Live
TESQA	
TESQA Admin	
TfSNow - Change	
TfSNow - Incidents	
TPM (Tivoli Provisioning Manager)	
Tripwire	LST and Live
Zanzibar IRE11	
Zephyr	

2.3 Privileged Access Management (PAM)

Some specialist support staff require Privileged Access to be able to keep systems working, investigate issues, and make necessary and required updates. Such access relies on PAM processes.

A privileged account has additional abilities to a "standard" user account and may include access rights to operating systems or to application software and databases.

System privileges and levels of access required to perform management functions are higher than those assigned to standard users. Therefore, the allocation and use of privileges is restricted and controlled, and the principle of least privilege is used. The principle of least privilege refers to the concept and practice of restricting access rights to only those resources required to perform the authorised activities. Individuals are not granted unnecessary privileges.

The management of PAM accounts is completed using a variety of tools such as an Access database, Excel spreadsheets, email, and SharePoint. A central database is held which records all access across all environments.

Privileged Access is reviewed monthly as explained in Section 5.1.2 below.

The Fujitsu Europe Business Management System (EBMS) provides a process and work instruction that POA follows:

- Europe Privileged Access Management Process
- Europe Privileged Access Management Work Instruction



Post Office Account User Access Guide
FUJITSU RESTRICTED (COMMERCIAL IN
CONFIDENCE)



3 Roles

The table below lists the Fujitsu, POA, POL and Third-Party teams and individuals, and the functions they perform in relation to user access.

Role	POA or Corporate	Function
HR	Fujitsu Corporate	Process Joiners, Movers and Leavers to Fujitsu
Site Facilities	Fujitsu Corporate	Process passes to allow access to Fujitsu buildings, floors, and rooms
Group Security	Fujitsu Corporate	Process clearances for individuals joining Fujitsu.
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 POA
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.
Security Governance Manager and Security Operations Manager (acting jointly as the Information Security Manager)	POA	The individuals 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 POA induction. Review and report on Joiners, Movers and Leavers
Contractor/Third Party	Supplier	An organisation or person that is not part of Fujitsu or POL
POL Staff	POL	An individual who is employed by POL
POL Test and Release Managers	POL	POL staff who work jointly with POA Test Teams



4 Processes, Procedures & Controls

4.1 Joiners

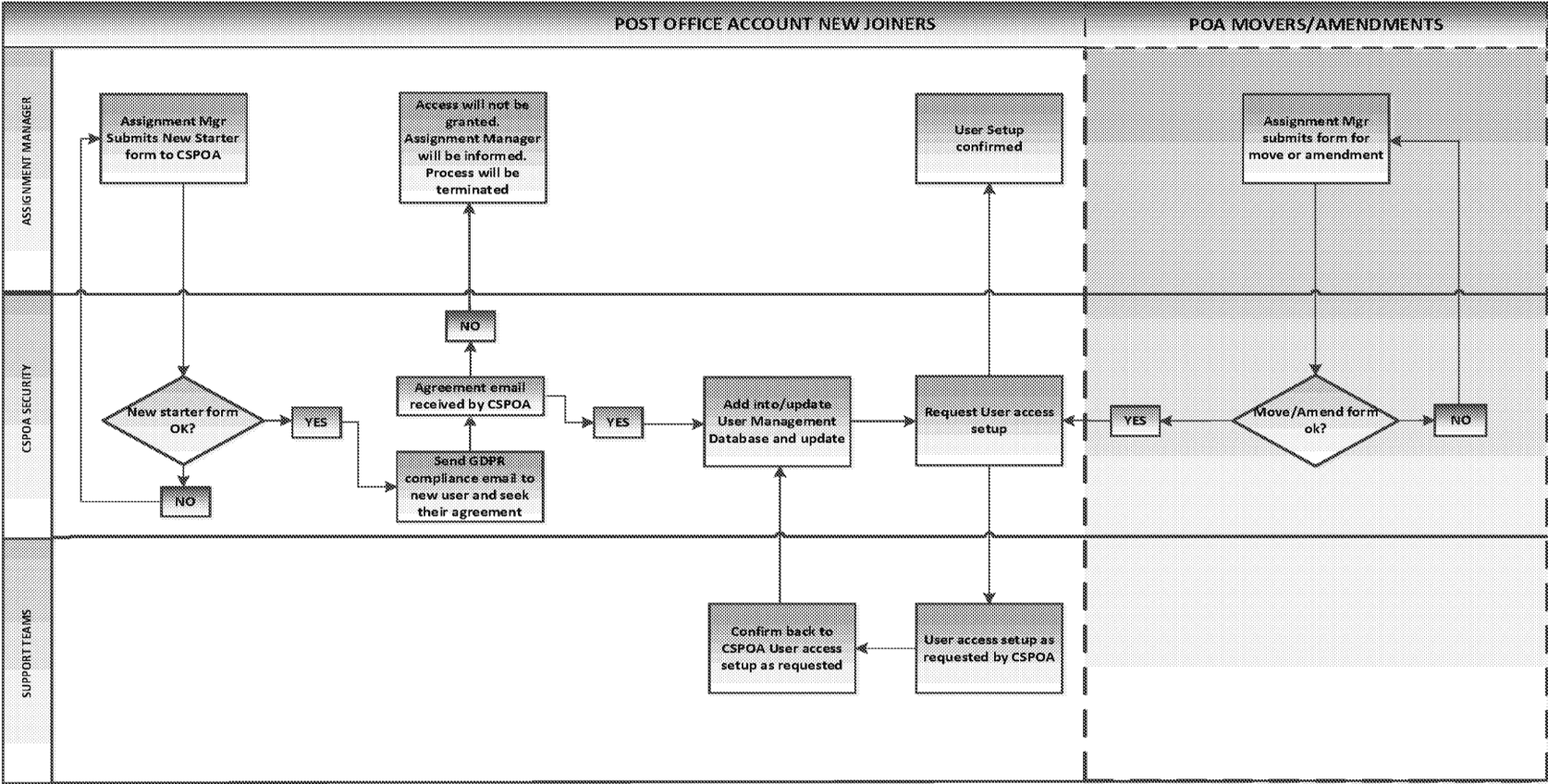
Detailed below are the steps that must be followed when an individual joins Fujitsu and POA or joins the POA from another area within Fujitsu. The Assignment Manager will apply for role-based access to the support systems to be set-up for a new user, and for Fujitsu Facilities management to provide physical access to relevant locations for the role. The process flow is shown in Figure 1.0, Diagram of User System Access Process Flow for New Joiners.



Post Office Account User Access Guide
FUJITSU RESTRICTED (COMMERCIAL IN CONFIDENCE)



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





Post Office Account User Access Guide
FUJITSU RESTRICTED (COMMERCIAL IN
CONFIDENCE)



The following steps must be followed:

1. The Assignment Manager shall complete the latest New User Access Form from the POA Security Operations Portal with all required information. The completed form shall be returned to CSPOA via email to CSPOA.Security@**GRO**. Privileged Access requests must come from either a Fujitsu or POL email address. All access follows least privilege and role-based principles as outlined in Fujitsu EBMS. Where a New User form has been completed by or on behalf of a new user (by a person other than the Line/Assignment Manager), the Line/Assignment Manager must be copied in on the email request for awareness and authorisation.

Below is an example of the email CSPOA receive for an individual who has joined the POA (with redactions as necessary):



2. CSPOA shall check the form to ensure that it has been completed correctly. If any information is missing or incorrect, the form will be rejected and returned to the Line/Assignment Manager for amendment.
 - A "Start Date" will be stated on the New User Access Form. However, CSPOA may receive a completed form weeks in advance of the stated start date. In that case, CSPOA shall retain the form and set an Outlook reminder to not process the access request until a maximum of one week prior to the requested start date.
 - Some requests may be time bound. If that is the case, then CSPOA will set an Outlook reminder to action the "Leaver" activity at the agreed date/time.

3. CSPOA shall email the new starter to:

- Inform them that their personal data (name and personnel number) may be shared with POL in accordance with our obligations.
- Seek acknowledgement, and agreement for their Name and Personnel number to be supplied to POL.

This is a GDPR compliance requirement and access to POA systems cannot be granted without this agreement.

4. If privileged access is being requested, CSPOA will seek additional authorisation from a member of the POA Leadership Team (LT) or a second member of the LT if the Assignment Manager is already a member of the LT (introduced March 2023).
5. Once the correct New User Access Form, the GDPR agreement, and any required additional LT approvals have been received, CSPOA shall arrange for all relevant access to be set up for the user.
6. CSPOA shall e-mail (generated from the user management database) the relevant System Owners and request user access to be set up. 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. In addition, POL Jira ticket(s) will be raised for Post Office Cloud access, where required.
NOTE - System Owners must only make changes to User accounts when instructed to do so by CSPOA.



Post Office Account User Access Guide

FUJITSU RESTRICTED (COMMERCIAL IN CONFIDENCE)



Below are examples of the emails CSPOA send to the relevant System Owners for user access to be set up (with redactions as necessary):

New user: [Redacted]

To: [Redacted] - POA Programme Office, POA User Request Requests
[Redacted] - POA User Management, [Redacted] - PostOfficeAccountSOM+PRO R, CSPOA Security

Dear Administrator,

Please add the following user to your system:

Full name	PN	Email	Team	Line Mgr	StartDate	Peak Clone	TFS Clone
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	04/03/2021 14:14:53		

PN	System	Owner address
UK992054 Annual Leave Calendar	POA Programme Office	GRO
UK992054 APT Access (includes: Jira,CE,SN,APT)	postofficeaccount	GRO
UK992054 Dimensions 12	PostOfficeAccount/241617	GRO
UK992054 ITG Network Access	Postal Parcelled Parcel.com: Access: Nachtsch	GRO
UK992054 Peak	postofficeaccount	GRO
UK992054 Shippoint	postofficeaccount	GRO

New user: [Redacted]

To: [Redacted] - PostOfficeAccount SOM+PRO R, CSPOA Security

Dear administrator,

Please can you add the following user to Dimensions and confirm once done;

User information

Full Name: [Redacted]

Job Title: [Redacted]

Department: [Redacted]

Location (while working on RMGA account):

Work phone: [Redacted]

Email: [Redacted]

RMGA Manager: [Redacted]

Corporate domain login id: [Redacted]

RightNow Personnel No (for Country code): [Redacted]

Access Required
(for commercial only viewing and creating documents): No

Software CRM and Documentation: No

Regards Security Team

7. The System Owners shall follow their own processes and work instructions to configure the user access. The System Owners will then update the TfSNow call to confirm the action they have taken which will notify CSPOA of completion.
8. CSPOA shall then close the TfSNow call and the Jira ticket(s) and update the register.
9. Electronic copies of all forms and records are stored securely and retained for audit purposes.

4.1.1 Fujitsu Staff not on the POA

For any Fujitsu shared services staff who are provided to POA, the Line Manager shall notify CSPOA of the relevant Assignment Manager POA has appointed. The Assignment Manager shall then follow the process in Section 4.1 for obtaining access to the relevant systems for the user.

4.1.2 POL Staff and 3rd parties

It is the responsibility of POL to verify, authenticate, and ensure that appropriate access has been granted to POL staff (and its 3rd parties) who have been provided with access to Fujitsu systems.



Post Office Account User Access Guide
FUJITSU RESTRICTED (COMMERCIAL IN
CONFIDENCE)



The PAM processes and principle of least privilege still apply. Access should be granted as detailed in Section 4.1, replacing Line Manager with Post Office assigned line manager.

All POL requests for TESQA and HORice access must be authorised by POL's Head of Contract Management & Deployment - Franchise Partnering or POL CISO.

4.2 Moving within POA or amendment to access

In addition to individuals who join POA and/or Fujitsu as new staff, 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 with all information required, and return to CSPOA 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.

Below is an example of the email CSPOA receive for an individual moving within the POA (with redactions as necessary):



4.2.1 Requests for TESQA & APPSUP access elevated privileges

The TES_TESQA_USER access is applied to user accounts when required for investigations into TESQA queries. Such requests must be authorised by POL's Head of Contract Management & Deployment - Franchise Partnering or POL CISO. There are a limited number of TESQA licences available and the request for access from POL involves removing the licence from one user and assigning it to another.

SVM/SDM/PRO/4293 describes the process for granting temporary APPSUP access.

4.2.2 Emergency Access to Live Systems

If a user requires emergency access to the live system outside business hours, the request must be approved by the CSPOA duty manager and be documented retrospectively. Note that the access may not be given outside business hours if the System Owners are not available to set up the required access.

4.3 Leavers

Detailed below are the steps that must be followed prior to or upon an individual leaving Fujitsu and/or the POA. The following steps must be followed:

1. Assignment Managers must submit a Leaver form as soon as possible prior to user leaving Fujitsu and/or the POA. The Assignment Manager should complete the latest Leaver Form from the POA Security Operations Portal with all information required, and return to CSPOA by emailing to CSPOA.Security@GRO. Below is an example of the email CSPOA receive for an individual leaving Fujitsu and/or the POA (with redactions as necessary):



Post Office Account User Access Guide

FUJITSU RESTRICTED (COMMERCIAL IN CONFIDENCE)



Leaver Form [REDACTED]

[REDACTED] To: CSPOA Security

From: [REDACTED] 54 93 [REDACTED]

Dear Sec Ops

Please see the attached leaver form for [REDACTED]

2. CSPOA shall check the form to ensure that it is completed correctly. If any information is missing or incorrect, the form will be rejected and returned to the Assignment Manager for amendment.
3. When a correct form has been received and checked, CSPOA shall arrange for all relevant access to be removed for the user, on the day the user leaves Fujitsu and/or the POA. Below is an example of the email CSPOA send to the relevant System Owners for user access to be removed (with redactions as necessary):

Revoke user [REDACTED]

[REDACTED] To: POA Programme Office; POA SharePoint Requests; POA User Management; Post Office Account Change Management; CSPOA Security

Dear Administrators

Please revoke the following user on your system:

Full name	PN	Email	Team	Line Mgr	EndDate
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

PN	System	Owner address
[REDACTED]	Annual Leave Calendar	POAProgrammeOffice GRO
[REDACTED]	APT Access (includes Jira,Chf,SVN/APT)	poausermanagement GRO
[REDACTED]	Impacting Tool	PostOfficeAccountChangeManagement GRO
[REDACTED]	Peak	poausermanagement GRO
[REDACTED]	Sharepoint	poasharepointrequests GRO

Regards CSPOASecurity

4. CSPOA shall arrange for floor/door access to be revoked by emailing Fujitsu Facilities Management and requesting removal of Floor/door access. CSPOA shall arrange for Network drive access to be revoked using Fujitsu Corporate Processes.
5. CSPOA shall notify the relevant System Owners via e-mail, and where backend system access is held, a TfSNow call shall be raised and progressed to the System Owners requesting revocation of access. In addition, POL Jira ticket(s) will be raised for revocation of access to Post Office Cloud, where required.
NOTE – System Owners must only make changes to User accounts when instructed to do so by CSPOA.
6. The System Owners shall follow their own processes and work instructions to remove the user and confirm revocation to CSPOA. CSPOA will then update the TfSNow call.
NOTE - All access (including MSAD) must be revoked within 5 days of user leaving the Account.



Post Office Account User Access Guide
FUJITSU RESTRICTED (COMMERCIAL IN
CONFIDENCE)



7. CSPOA shall then close the TfSNow call, the Jira ticket(s), update the register and confirm with relevant teams that access has been revoked.

8. Electronic copies of all forms and records are stored securely and retained for audit purposes.

4.3.1 Staff who are terminated with immediate effect

For those users whose employment is terminated with immediate effect, the Line/Assignment Manager must immediately contact HR (via AskHR portal) and CSPOA (by phone/Microsoft Teams) and then follow the POA Leaver's process, making sure all the relevant forms are completed. The process in Section 4.3 will be applied retrospectively to individuals whose employment is terminated with immediate effect.

4.3.2 Fujitsu shared services staff whose POA assignment has been completed

For all Fujitsu shared services staff on POA assignment, the Assignment Manager shall notify the Line Manager of the expiry of the individual's assignment to POA. The Assignment Manager shall then follow the process in Section 4.3 for removing access to the relevant systems for the user.

4.3.3 POA staff who are moving to another part of Fujitsu

Line/Assignment Managers whose staff are directly employed as part of POA and move to another part of Fujitsu shall follow the process in Section 4.3 for the termination of user's rights that are associated directly with systems dedicated to POA.

4.3.4 POL Staff

POL staff who are provided with access to Fujitsu systems are the responsibility of POL. Access should be revoked as detailed in section 4.3, replacing Line Manager with Post Office Assigned Line manager.

4.4 Privileged Access

Employees granted privileged access to any systems are required to comply with the POA Privileged Account Policy [SVM/SEC/POL/4538]. This includes a statement on the required password policy rules.

4.5 Break Glass Accounts

Employees who require temporary access to privileged accounts – such as local administration accounts – to provide them with additional access they do not require within their normal duties must follow the POA Privileged Account Release Procedure [SVM/SEC/PRO/4537]. These are typically referred to as Break Glass accounts.

4.6 Requesting a new High Privileged Account

All accounts must be authorised by the JML process. A new High Privileged Account is requested via an Access Request form completed by the Assignment Manager of the owner of the account(s). There are no exceptions to this process. If, during a project, a new account is required, it must be requested via the stated JML process.

1. A Joiner Form with the "NEW - Privileged User Account Tab", completed with all required details, to be submitted by an Assignment Manager. The form, and therefore the Assignment Manager, must state who the Account Owner will be. This CANNOT be an email group and must be a designated individual
2. Any documentation/information for the new account must be shared with POA SecOps
3. POA SecOps will additionally note the Assignment Manager's direct Leadership Team Owner (LTO) only if a human account.

4.6.1 Verification Process



Post Office Account User Access Guide
**FUJITSU RESTRICTED (COMMERCIAL IN
CONFIDENCE)**



POA SecOps will share the SVM/SEC/POL/4538 POA Privileged Account Policy (Sections 5.2, 5.3 & 5.4) with the Account Owner. This states the policy compliance requirements that must be met for the account. The Account Owner will be asked to confirm their acceptance of the policy before the account is authorised for creation. The Account Owner will also be required to acknowledge that compliance with the policies will need verifying quarterly.

POA SecOps will also ask the LTO to provide additional authorisation if a human account. If the LTO is not available, then POA SecOps will redirect the request to another member of the LT. Without LTO authorisation the new account will NOT be created.

4.6.2 Adding access and controls

Upon review of the form and confirmation of authorisation by Account Owner and Assignment Manager, POA SecOps will request the new account creation by raising a TfSnow Incident and assigning it to the relevant system administrators. If the system administrators do not use TfSnow, then an Incident will be raised and updated by SecOps to ensure TfSnow has a record of the actions taken. The TfSnow Incident will remain open until the account is created and the PAM register has been updated in full.

4.6.3 Updating the PAM Register

All new privileged accounts are recorded on the PAM register Database and owners are contacted every 90 or 365 days (depending on level of privilege the account holds) to verify the compliance of the account with the POA Privileged Account Policy.



Post Office Account User Access Guide
**FUJITSU RESTRICTED (COMMERCIAL IN
CONFIDENCE)**



5 Management

All access is validated monthly to ensure that the access supplied is still required and appropriate, including standard user access for all POA systems and privileged user access for the Production environment. Access is revoked if:

- Verification of the continued need for access is not received
- Role has changed and access is no longer appropriate or required
- User account has not been used for more than 90 days

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 and CSPOA Teams shall undertake a monthly review of the access granted to individuals and its continued appropriateness.

5.1.1 Team Verification (Standard User Access Verification)

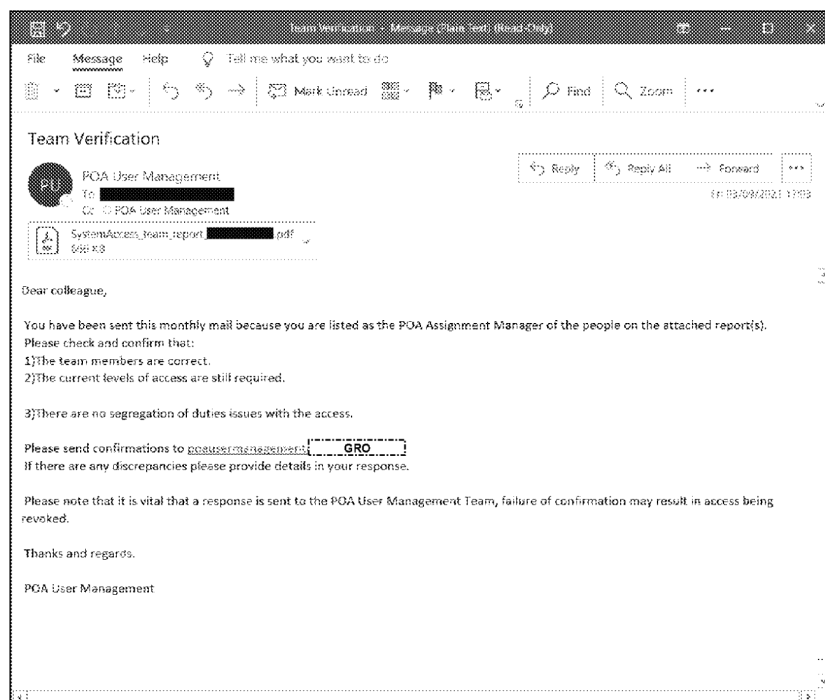
1. POA User Management Team shall produce details of all users contained in the register and their access levels and shall email these to the relevant Line/Assignment Managers.
2. Line/Assignment Managers shall review whether the current access of their employees is still in line with their job role.
3. Line/Assignment Managers shall consider whether any users require their access be amended and they shall email these details to POA User Management Team within 15 working days of receipt of the original e-mail.
4. Line Mangers shall confirm each employee's current access rights requirements and shall email these details to POA User Management Team within 15 working days of receipt of the original e-mail from POA User Management Team. If a response has not been received by POA User Management Team within 15 working days, CSPOA will be informed, and users' access may be removed.
5. CSPOA will audit access rights and roles with each functional area; the results of which will be presented at the monthly Team Access Review meeting with POA User Management.

Below is an example of the Team Verification email and the System Access Report (user access levels, with redactions as necessary):



Post Office Account User Access Guide

FUJITSU RESTRICTED (COMMERCIAL IN CONFIDENCE)





Post Office Account User Access Guide

FUJITSU RESTRICTED (COMMERCIAL IN CONFIDENCE)



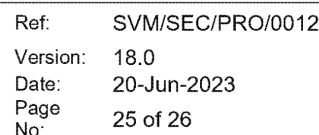
Team:	App Dev/4th Line-Dev Man	Assignment Mgr:	[REDACTED]
Name	Per. No.	List of accessible systems	
[REDACTED]	[REDACTED]	Annual Leave Calendar, AWS Access, Dimensions 12, PEAK, Sharepoint, TFS/Know - Change	
Team:	App Dev/4th Line-Integratio	Assignment Mgr:	[REDACTED]
Name	Per. No.	List of accessible systems	
[REDACTED]	[REDACTED]	Annual Leave Calendar, APT Access (includes Jira, CI, SVN/APT), AWS Access, Dimensions 12, Impacting Tool, Sharepoint	
Team:	App Dev/4th Line-Applicatio	Assignment Mgr:	[REDACTED]
Name	Per. No.	List of accessible systems	
[REDACTED]	[REDACTED]	Annual Leave Calendar, APT Access (includes Jira, CI, SVN/APT), AWS Access, Dimensions 12, Frenjiban, Impacting Tool, Ingenico e-Portal, ITG Network Access, MSAD LST, PEAK, Sharepoint	
Team:	App Dev/4th Line-Architectu	Assignment Mgr:	[REDACTED]
Name	Per. No.	List of accessible systems	
[REDACTED]	[REDACTED]	Annual Leave Calendar, APT Access (includes Jira, CI, SVN/APT), Atlassian/Jira Cloud, AWS Access, Dimensions 12, Frenjiban, Impacting Tool, ITG Network Access, PEAK, Quality Centre, Sharepoint	
Team:	App Dev/4th Line-Dev Mana	Assignment Mgr:	[REDACTED]
Name	Per. No.	List of accessible systems	
[REDACTED]	[REDACTED]		

03 September 2021

Page 2 of 4

5.1.2 Privileged User Access Verification

1. A more detailed access verification check is conducted monthly, specifically for Production Privileged Access. CSPOA shall produce details of all users with Privileged Access and email these to the relevant Line/Assignment Managers. As part of this monthly verification process, segregation of duties is also checked to ensure there are no segregation issues e.g., due to changes to a user's role or responsibilities.
2. Line/Assignment Managers shall review whether the current Privileged Access of their employees is still in line with their job role.
3. Line/Assignment Managers shall consider whether any users require their Privileged Access to be amended and they shall email these details to CSPOA within 15 working days of receipt of the original e-mail.
4. Line Mangers shall confirm each employee's current Privileged Access rights requirements and shall email these details to CSPOA within 15 working days of receipt of the original e-mail. If a response has not been received by CSPOA within 15 working days, users' Privileged Access will be removed. This will be presented at the monthly Team Access Review meeting with POA User Management.
5. CSPOA will also ask the applicable POA Leadership Team (LT) manager to review privileged access rights of employees within teams under their remit on a quarterly basis (introduced March 2023).
6. Below is an example of the Privileged User Access email (with redactions as necessary):



[illegible]

2. CSPOA will review the list of individuals who have been added to the iKey Exemption List.
3. POA User Management Team provide a monthly report detailing all Joiners, Movers and Leavers on POA for CSPOA to review.

5.1.5 Other CSPOA Regular Checks

Over and above the Assignment Manager and PAM access monthly verifications, CSPOA conduct other regular checks of systems. These regular checks are performed on a number of selected systems each month. The current active user account list is obtained and then compared to the central records held. Inconsistencies are investigated and appropriate action taken. A record is kept of which system has been checked, when, and the outcome.

5.2 Information Security Management Review (ISMR)

A summary of the status of monthly verification activities is provided to the POA LT at the Fujitsu internal monthly ISMR meeting to ensure any issues/non-conformance receives the appropriate level of POA management attention and action.

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. Any Joiners, Movers and Leavers into POA follow the planned processes detailed 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.

The reports and reviews can be found in CSPOA Monthly Report.