FUJ00089673

Post Office Account User Access Procedure

FUJITSU RESTRICTED (COMMERCIAL IN CONFIDENCE)

Document Title:	Post Office Account User Access Procedure
Document Reference:	SVM/SEC/PRO/0012
Document Type:	Procedure
Abstract:	This document establishes 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
Steve Godfrey	CISO	See Dimensions for record	

FUJ00089673

0 Document Control

0.1 Table of Contents

FUJ00089673

FUJ00089673

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	

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.*

FUJ00089673

Review Comments by :	
Review Comments to :	Niall Vincent and Post Office Account Document Management
Mandatory Review	
Role	Name
CISO	Steve Godfrey
Crypto Key Manager	Andy Dunks
Security Analyst	Niall Vincent
Optional Review	
Position/Role	Name
Security Analyst	Farzin Denbali

(*) = 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	PO Account 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		See Dimensions for latest version	Post Office Ltd Community Information Security Policy (CISP)	POL–owned and / 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

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

FUJ00089673

CISP	Post Office Ltd Community Information Security Policy
CSPOA	Post Office Account Operational Security Team
HR	Human Resources
ISMF	Joint Fujitsu and PO Ltd Information Security Management Forum known as M6
PO Ltd	Post Office Limited
PO Account	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
TFS	Triole For Service: Help Desk Call Management System
ISM	Information Security 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 Security Risk Assessment

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

FUJ00089673

1 Introduction

This Post Office Account User Access Procedure details how access is to be gained to both physical and technical assets within the PO Account 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 PO Account 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 PO Account 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.”
>
> 4.1.4 “Fujitsu Services shall adhere to the relevant parts of the CCD entitled “Community Information Security Policy for Horizon” (CISP) (SVM/SEC/POL/0005) and co-operate with Post Office to assist Post Office in complying with this standard and requirement.
>
> 4.1.5 “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.”

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).

FUJ00089673

2 User System Access

2.1 Pre-requisites for allocation and removal of Access

Prior to access being requested for PO Account specific assets Fujitsu HR processes for joiners and movers onto the account, including processes for RIO, RAR or ERIC, where shared services are used, shall be followed.

For shared services Assignment Mangers will apply for resources via a RIO, RAR or Eric 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 FPV1 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 PO Account CISO and Operational Security Manager to determine how to proceed.

In addition, if an individual moves away from PO Account 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 PO Account 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.

2.2 CSPOA User Registry

The User Access Process on the PO Account 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 on a daily/as needed basis 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 will also aid any audit that may be required, by providing the details of personnel and access levels granted.

The user access database holds the information about each individual who has 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 fields held within this registry are shown in Appendix B.

FUJ00089673

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 PO Account.
Line/Assignment Managers	PO Account	Manager responsible for resources working in their area of responsibility
System Owners	PO Account Fujitsu Corporate Fujitsu Core	Team who maintain access to specific systems for the Post Office Account
Resourcing Manager	PO Account	Member of the Business Management Team who manages and monitors resource forecasting on PO Account.
CSPOA Security Operations Team	PO Account	The team on PO Account that manage, control and report on both physical and system access.
CISO	PO Account	The individual responsible for all aspects of Security on PO Account
Fujitsu Test Managers	PO Account	PO Account Test Managers who work jointly with PO Ltd Test Teams
Business Management	PO Account	Responsible for organising and maintaining account induction
Contractor/Third Party	Supplier	An organisation or person that is not a member of Fujitsu or PO Ltd staff
PO Ltd Staff	PO Ltd	An individual that is employed by PO Ltd
PO Ltd Test and Release Managers	PO Ltd	PO Ltd staff who work jointly with PO Account Test Teams

FUJ00089673

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 PO Account 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 joiner form from the POA Security Operations Portal and complete all information required and return to CSPOA Security Operations Team by emailing to GRO

2. The New User Access Forms Line/Assignment Manager 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 click on the 'Email Completed Form to POA Security Ops' button

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

3. CSPOA Security Operations Team shall check the form is completed correctly, and in line with PO Account 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 FPV1 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.

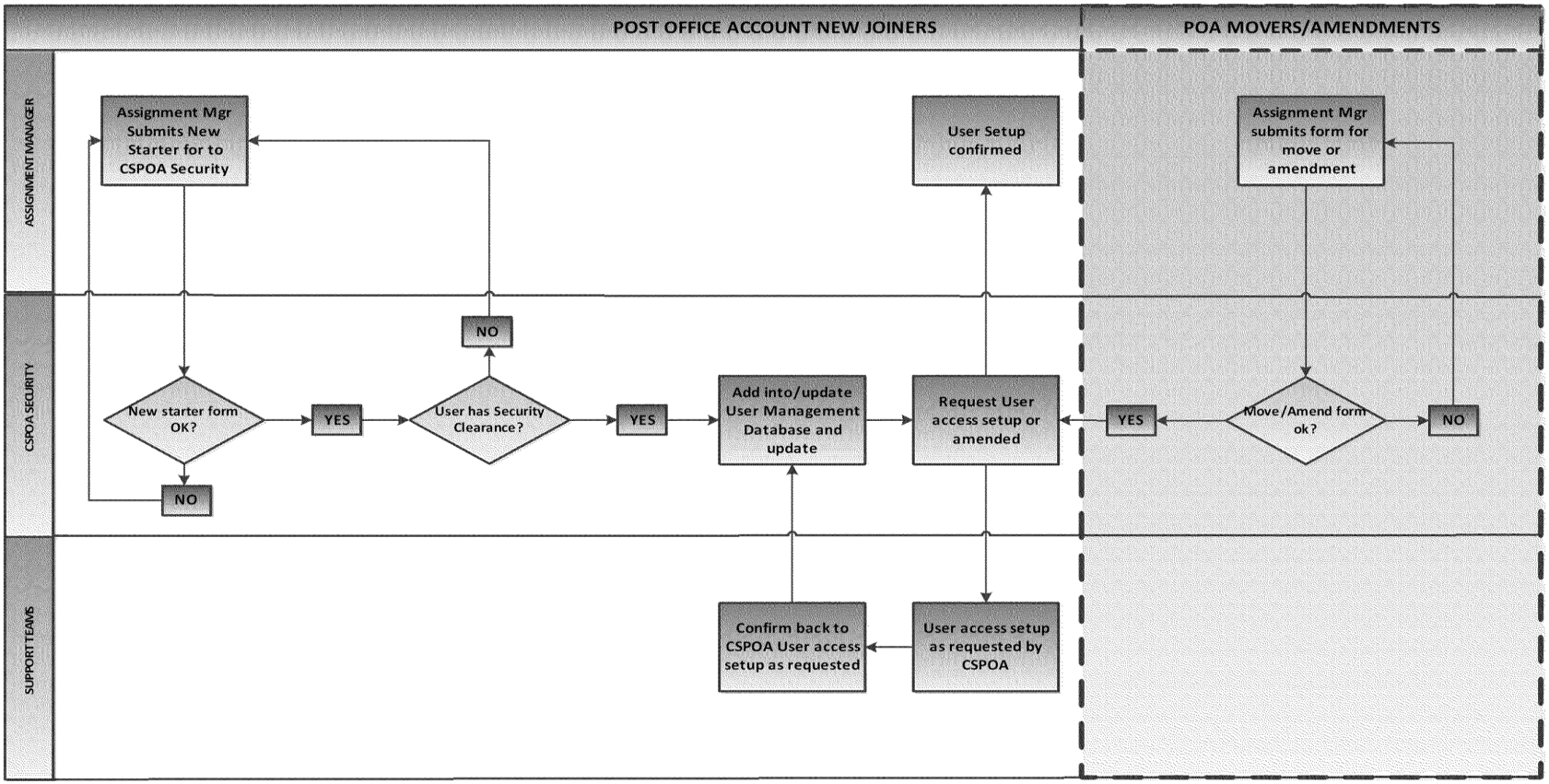
6. CSPOA Security Operations Team shall notify the relevant system owners via an e-mail (which is generated from the user management database). A TfS call will be raised for back-end system requirements and a copy of the completed request form will be attached to the TfS call , where required

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 TFS call and update the register.

FUJ00089673

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



FUJ00089673

4.2 Moving within POA account or amendment to access

In addition to individuals who join PO Account as new staff to POA and/or Fujitsu, there are cases where people are moved within the PO account. 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 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 PO Account

For any Fujitsu shared services that are provided to PO Account, 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 PO Ltd Staff

Post Office staff that are provided with access to Fujitsu systems are the responsibility of PO Ltd 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 an MSC as justification on the requirement for the elevated access.

4.3 Leavers

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

4.3.1 PO Ltd Staff

Post Office staff that are provided with access to Fujitsu systems are the responsibility of PO Ltd. 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 PO Account and these are shown in the Figure 1.2 Diagram of User system access flow for Leavers.

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:

FUJ00089673

- The Line/Assignment Manager shall complete all information on the form for the required individual and then click on the 'Email Completed Form to POA Security Ops' button

These forms shall be filed and stored electronically, 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 access to be revoked using Fujitsu Corporate Processes 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 TFS 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 PO Account 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 PO Account has been completed

For all Fujitsu shared services provided to PO Account 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.

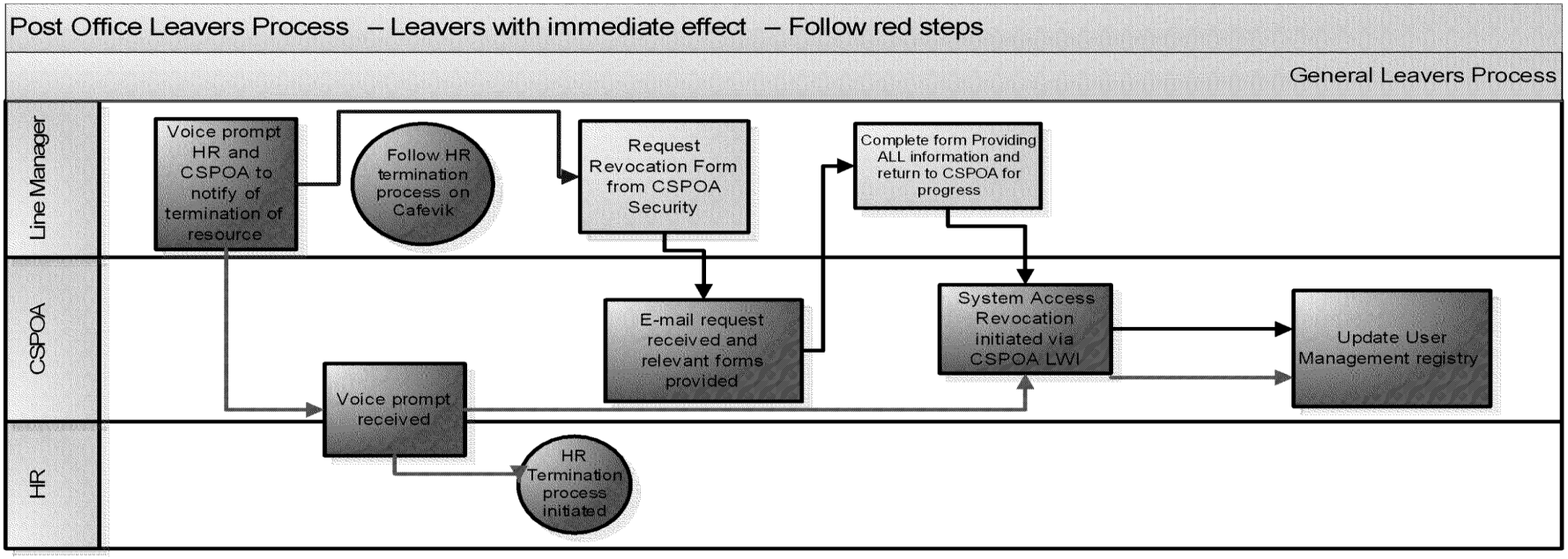
4.3.5 PO Account staff who are moving to another part of Fujitsu

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 PO Account.

FUJ00089673

Figure 1.2 Diagram of User system access flow for Leavers

Leavers with Immediate Effect is covered in RED



FUJ00089673

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

To achieve this:

1. CSPOA Security Operations 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 CSPOA Security Operations Team within 10 working days of receipt of the original e-mail from CSPOA Security Operations Team.
5. CSPOA Operational Security will audit access rights and roles with each functional area; this will be carried out 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. Individuals added to the Ikey Exemption List.
8. Joiners, Leavers and movers to the Account.
9. Card swipe/floor access attempts report.

5.2 Reporting

CSPOA will provide a report to Post Office Account PMO 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 PO Account to provide evidence of the following for audit purposes.

1. That any joiners, movers and leavers into PO Account 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.

FUJ00089673

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 take precedence over any PO Account documentation, are held on EMEIA Connect at:-

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

Documentation of PO Account's own policies, processes and procedures is held on Dimensions and follows guidance provide in the Fujitsu EMEIA Master Security Policy Manual which is aligned to ISO27001:2013.

FUJ00089673

7 Appendix B: List of Systems

Systems in scope	Dimensions 9
	Doors
	HNG-X Live
	Peak
	POLMI
	TACACS
	Live TESQA
	TFS
	Test Rig Access – LST
	Test Rig Access SV&I
	Accenture Groups
	POLSAP
	Database Root
	Database Access
	Database Administrator UNIX enabled Y/N
	SharePoint
	Quality Centre
	Tivoli
	Visual SourceSafe
	SVN (CVS)
	Dimensions12 (was PVCS)
	Live BCMS
	MSC
	Secure Floor access BRA01
	HORice

FUJ00089673

8 Appendix C: 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:

IRRELEVANT

8.2 Revocation Form

A copy of the Revocation form can be found here:

IRRELEVANT

8.3 Mover Form

A copy of the mover form can be found here:

IRRELEVANT

9 Appendix D: 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, the request cannot be actioned until we have approval.

Once approved by all parties a TFS 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'.