FUJ00088799



| | |
|---|---|
| **Document Title:** | Post Office Account User Access Procedure |
| **Document Reference:** | SVM/SEC/PRO/0012 |
| **Document Type:** | Procedure |
| **Release:** | Not Applicable |
| **Abstract:** | This document establishes the controls that Post Office Account has to meet to manage user access to its assets based on its contractual requirements. |
| **Document Status:** | APPROVED |
| **Author & Dept:** | Donna Munro |
| **External Distribution:** | None |
| **Security Risk Assessment Confirmed** | YES |

## Approval Authorities:

| Name | Role | Signature | Date |
|---|---|---|---|
| James Davidson | Operations Director | See Dimensions for record | |
| Ian Howard | PO Account CISO | See Dimensions for record | |
| Ellie Sims | HR Manager, Enterprise Business Unit Private Sector Division | See Dimensions for record | |

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

FUJ00088799



# 0 Document Control

## 0.1 Table of Contents

FUJ00088799

FUJ00088799



## 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 |

## 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 : | Donna.Munro GRO |
| **Mandatory Review** | |
| Role | Name |
| Tony Atkinson | Head of Service Management |
| Ian Howard | CISO |
| Chris Mitchell | PMO Resource Manager |
| Ellie Sims | PO Account HR Representative |
| Tony Atkinson | PO Account Head of Service Management |
| Leighton Machin | Service Desk SDM |
| Chris Bourne | OBC/DMN Manager |
| Janet Reynolds | Operations Support |
| David Wilcox* | Reference Data Manager |
| Sarah Bull | Branch Services & Release Management SDM |
| Steve Parker | SSC Manager |

FUJ00088799



| | |
|---|---|
| Alex Kemp | Networks SDM |
| Sandie Bothick | Service Desk SDM |
| Optional Review | |
| Position/Role | Name |
| Dave Jackson | Practice Head - Northern Implementations |
| Adrienne Thompson | Team Manager SoP Northern Ireland |
| Catherine Irvine | Service Manager, Network Security Support, Infrastructure Svces |
| Pete Thompson | Head of Service Operations |

( * ) = Reviewers that returned comments

## 0.4 Associated Documents (Internal & External)

| Reference | Version | Date | Title | Source |
|---|---|---|---|---|
| PGM/DCM/TEM/0001 (DO NOT REMOVE) | 4.0 | 21-Nov-2008 | PO Account HNG-X Generic Document Template | Dimensions |
| SVM/SEC/PRO/0002 | | | Horizon Online Security Pass Procedure | Dimensions |
| SVM/SEC/PRO/0006 | | | PO Account System Access | Dimensions |
| ARC/SEC/ARC/0003 | | | HNG-X Technical Security Architecture | Dimensions |
| DES/PPS/HLD/0003 | | | Active Directory HLD | Dimension |
| DEV/APP/LLD/0028 | | | Active Directory LLD | Dimension |
| DEV/GEN/SPG/0012 | | | Active Directory Support Guide | Dimensions |
| SVM/SDM/SD/0017 | | | Security Management Service: Service Description | Dimensions |
| SVM/SEC/PRO/0033 | | | PO Account Risk management Process | Dimensions |
| SVM/SEC/POL/0003 | | | PO Account Information Security Policy | Dimensions |
| BS ISO/IEC 27001:2005 | | | Information technology — Security techniques —Information security management systems Requirements | External |
| BSI ISO/IEC 27002:2005 | | | Information technology —Security techniques —Code of practice forinformation security management | External |
| BS/ISO IEC 20002 | | | Contact PO Account Security for details | External |
| SVM/SEC/PRO/0036 | | | RMGA Supplier Security Audit Process | Dimensions |
| SVM/SEC/POL/0005 | | | Post Office Ltd Community Information Security Policy (CISP) | POL –owned and / Dimensions |

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

FUJ00088799



## 0.5 Abbreviations/Definitions

| Abbreviation | Definition |
|---|---|
| BM | Business Management |
| BMS | 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 PO Ltd Information Security Management Forum |
| PO Ltd | Post Office Limited |
| PO Account | Post Office Account |
| Line 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 |

## 0.6 Changes Expected

| Changes |
|---|
| Changes following Final Review |

## 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

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

.

FUJ00088799



# 1 Introduction

The User Access Process 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 – the CSPOA Security Operations Team.

It 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.

This process does not cover the PO Account engineer's access as this is covered in SVM/SEC/PRO/0002 Horizon Online Security Pass Procedure.

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

Appendix A Section 5.1 refers to the control sections required for user management in ISO 27001. Section 5.2 explains ISO 27002 user management requirements used as the basis of PO Ltd's CISP requirements and also refers to Fujitsu Corporate Procedures that are required to follow Fujitsu's Business Management System (BMS).

FUJ00088799



# 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 or ERIC where shared services are used, shall be followed.

For shared services Line Mangers will apply for resources via a RIO or Eric according to the Fujitsu corporate procedures as detailed on Cafevik at IRRELEVANT

Once employment is confirmed the Line Manager will initiate the relevant security clearance process that is carried out by Fujitsu Group Security. The forms requesting security clearance can be found via Cafevik IRRELEVANT These forms will ensure that the individual has the required Fujitsu Services basic checks and the PO Account specific Credit Check and Criminal Record check completed.

Once the individual is accepted into the role and the relevant clearance level granted the Line 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 then HR and the Line Manager will be notified and the circumstances discussed with the PO Account CISO and Security Operations Manager to agree 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 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 then the Line Manager must follow HR policies and procedures for a termination. These are found on the Cafevik at http://www.cafevik.fs.fujitsu.com/index.aspx?portal=152.

## 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 regular 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 registry 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 authoriser, approver and dates that this access was granted last reviewed and revoked. Details of the fields held within this registry are shown in Appendix B.

FUJ00088799



# 3 Roles

| Role | Account or Corporate | Function |
|---|---|---|
| HR | Fujitsu Corporate | Process New 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 Managers | PO Account | Manager responsible for resources working in their area of responsibility |
| System Owners | PO Account<br>Fujitsu Corporate<br>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 |
| 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 |

FUJ00088799



# 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 joining the PO Account and these are shown in the Figure 1.0 Diagram of User System Access Process Flow for New Joiners.

1. The Line Manager shall contact CSPOA Security Operations Team and request that system access forms are provided. These are detailed in SVM/SEC/PRO/0006 PO Account System Access and examples are shown in Appendix C.

2. The CSPOA Security Operations Team shall provide the New User Access Forms to the Line Manager and request they are completed and returned in the follow manner:

   - The Line Manager shall complete all the mandatory information on the form for the required individual and then click on the 'Email Completed Form to POA Security Ops' button
   - A Signed hard copy shall then be returned in the post to **CSPOA Security Operations Team, 4th floor, BRA01**

   These forms shall be filed and stored in the security operations secure room 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 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 set up for the user.

5. CSPOA Security Operations Team shall notify the relevant system owners via an e-mail containing the completed request form and a Triole for Service (TFS) call shall be raised and suspended whilst access is granted.

6. The System Owners shall set up access within one working day of receiving a correctly completed request form with the exception of Dimensions access which shall require two working days.

7. The System Owners shall follow their own processes and work instructions to configure the user and shall update the TFS call on completion of this configuration.

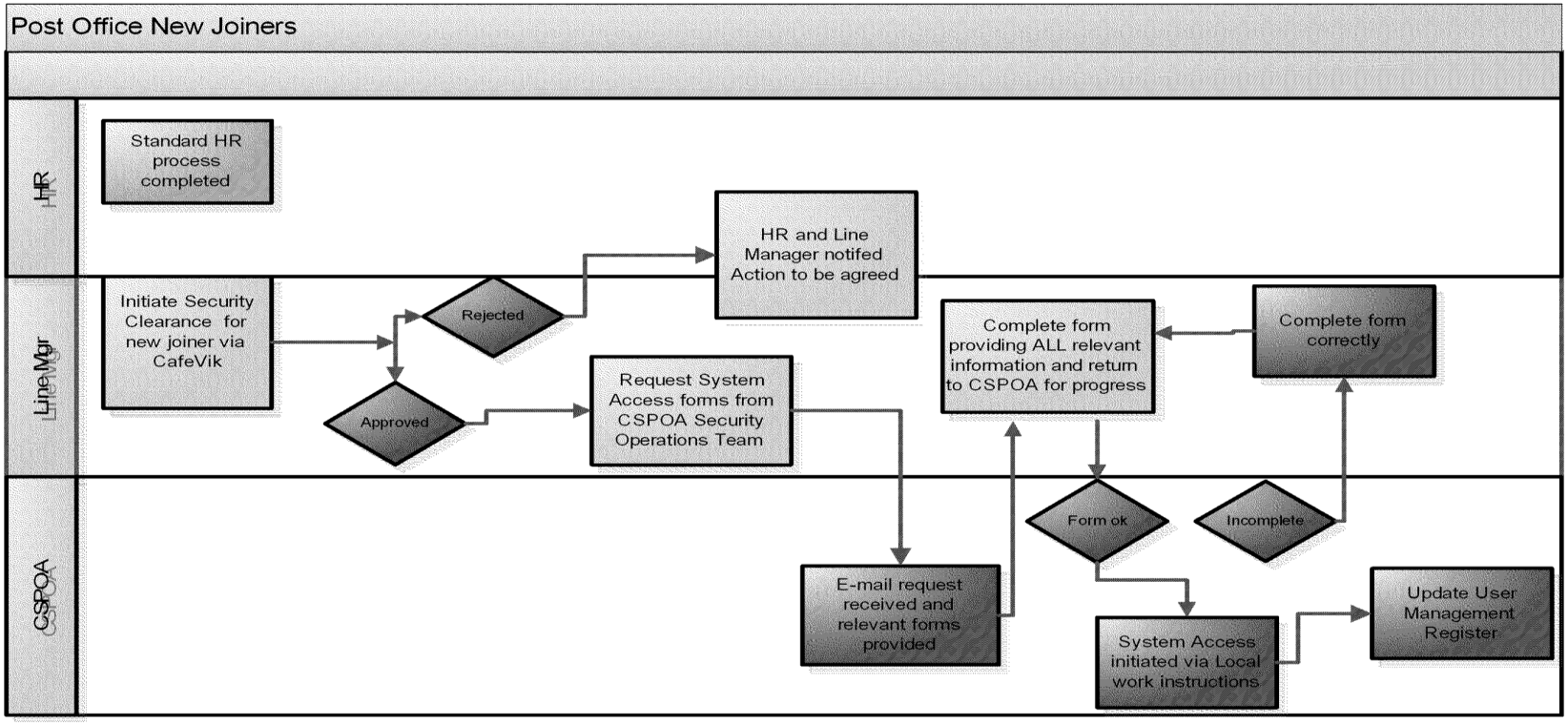
8. CSPOA Security Operations Team shall then close the TFS call and update the register.

FUJ00088799

FUJ00088799



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



FUJ00088799



## 4.2 Moving, Transferring or Change of Access Rights

In addition to individuals who join PO Account as new staff to Fujitsu Services, there are cases where people with key skills are brought onto the account to perform specific specialist functions categorised as follows:

1. Contractor or Third Party Staff
2. Fujitsu Staff not on the PO Account
3. Fujitsu Staff allocated to the PO Account.

A. PO Ltd Staff

Details of the process flow are shown in the Figure 1.1 Diagram of User system access flow for Moving, Transferring, and Amending access

### 4.2.1 Contractor or Third Party Staff

Access for Contractor or Third Party staff is agreed within the relevant contracts and operating level agreements with those organisations and is out of scope of this document.

### 4.2.2 Fujitsu Staff not on the PO Account

For all Fujitsu shared services provided to PO Account the Business Management (Resourcing Manager) shall notify the CSPOA Security Operations Team of the relevant Line Manager on the account. The Line Manager shall then follow the process in Section4.1 for obtaining access to the relevant systems for the user.

### 4.2.3 Resources allocated to the PO Account

1. The Line Manager shall contact CSPOA Security Operations Team and request that User Change System Access Forms are provided. These are detailed in SVM/SEC/PRO/0006 PO Account System Access and examples are shown in Appendix C.

2. The CSPOA Security Operations Team shall provide the Access Forms to the Line Manager and request they are completed and returned in the follow manner:

   - The Line Manager shall complete all the mandatory information on the form for the required individual and then click on the 'Email Completed Form to POA Security Ops'button
   - A Signed hard copy shall then be returned in the post to **CSPOA Security Operations Team, 4th floor, BRA01**

   These forms shall be filed and stored in the security operations secure room 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 Manager to amend.

FUJ00088799



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

5. CSPOA Security Operations Team shall notify the relevant system owners via an e-mail containing the completed request form and a Triole for Service (TfS) call shall be raised and suspended whilst access is granted.

6. The System Owners shall set up access within one working day of receiving a correctly completed request form with the exception of Dimensions access which shall require two working days.

7. The System Owners shall follow their own processes and work instructions to configure the user and shall update the TFS call on completion of this configuration.

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

### 4.2.4 PO Ltd Staff

PO Ltd 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. However, as PO Ltd work jointly with Fujitsu Reference Data and Fujitsu Test teams in Bracknell, physical access is required for these staff.

Detailed below are the steps that must be followed in order for a Post Office employee to obtain a Fujitsu pass to permit them site access. A sample access form is shown in Appendix C.

1. PO Ltd Test and Release Managers shall send an email detailing the PO Ltd employee that requires access along with a completed PO Ltd ID Card and Access Request Form.

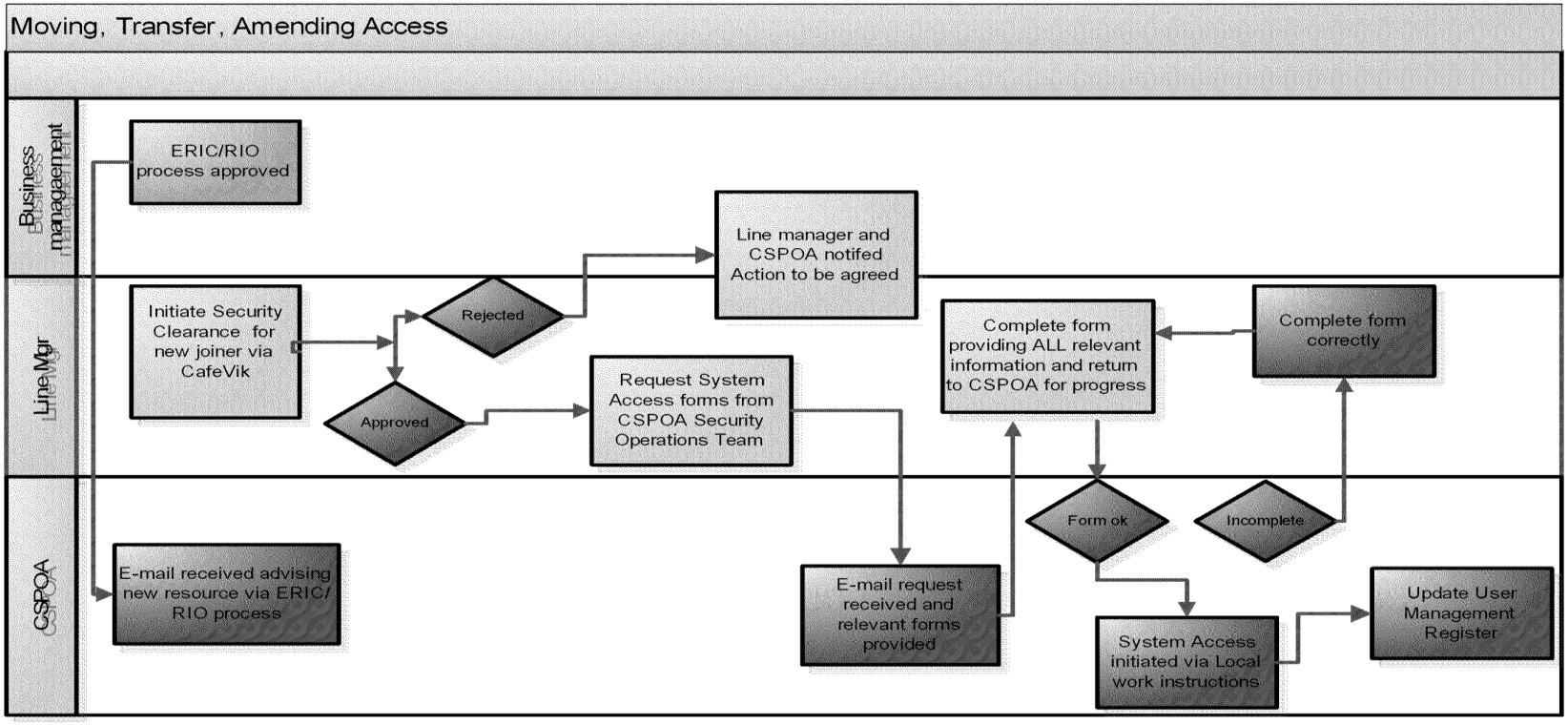
2. Fujitsu Test Managers shall receive, verify and approve the completed form.

3. Once approval is received the form shall be sent by Fujitsu Test Managers to Site Facilities to set physical access up.
4. Site Facilities shall provide the access and confirm to Fujitsu Test Managers once this has been set up.

FUJ00088799



**Figure 1.1 Diagram of User system access flow for Moving, Transferring, and Amending access**



FUJ00088799



## 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.

There are six types of leavers:

a) Contractor or Third Party Staff

b) PO Ltd Staff

c) Staff who are leaving Fujitsu

d) Staff who are terminated with immediate effect

e) Fujitsu staff whose assignment with PO Account has been completed

f) PO Account staff who are moving to another part of Fujitsu

### 4.3.1 Contractor or Third Party Staff

Contractor or Third Party staff are the responsibility of the relevant organisation and are subject to contractual and operating level agreements and are out of scope of this document.

### 4.3.2 PO Ltd Staff

PO Ltd staff that are provided with access to Fujitsu systems are the responsibility of PO Ltd. However, as PO Ltd work jointly with Fujitsu Reference Data and Fujitsu Test teams in Bracknell, the removal of physical access is required for these staff.

Detailed below are the steps that must be followed in order for a Post Office employee's Fujitsu pass permitting them site access be revoked.

1. PO Ltd Test and Release Managers shall send an email detailing the PO Ltd employee that requires their access to be revoked along with an Access Removal Form.

2. Fujitsu Test Managers shall receive, verify and approve the completed form.

3. Once approval is received the form shall be sent by Fujitsu Test Managers to Site Facilities to remove physical access.

4. Site Facilities shall remove the access and confirm to Fujitsu Test Managers once this has been completed.

### 4.3.3 Staff who are leaving Fujitsu

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

**This process must be implemented 3 days prior to the individuals last working day**

1. The Line Manager shall contact CSPOA Security Operations Team by voice prompt and e-mail providing the leaver's details and requesting a revocation form.

FUJ00088799



2. The CSPOA Security Operations Team shall provide the revocation form and request it is completed and returned in the follow manner:

   - The Line Manager shall complete all the mandatory information on the form for the required individual and then click on the 'Email Completed Form to POA Security Ops' button
   - A Signed hard copy shall then be returned in the post to **CSPOA Security Operations Team, 4th floor, BRA01**

   These forms shall be filed and stored in the security operations secure room 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 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 set up for the user.

5. CSPOA Security Operations Team shall arrange for floor access to be revoked using Fujitsu Corporate Processes.

6. CSPOA Security Operations Team shall notify the relevant system owners via an e-mail containing the completed removal form and a Triole for Service (TfS) call shall be raised and suspended whilst access is removed.

7. The System Owners shall follow their own processes and work instructions to remove the user and shall update the TFS call on completion of this configuration.

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

## 4.3.4 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 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 4.3.3 is applied retrospectively to individuals that are terminated with immediate effect.

## 4.3.5 Fujitsu staff whose assignment with PO Account has been completed

For all Fujitsu shared services provided to PO Account the Business Management (Resourcing Manager) shall notify the Line Manager of the expiry of the individual's assignment to the account. The Line Manager shall then follow the process in Section 4.3.3 for removing access to the relevant systems for the user.

FUJ00088799



## 4.3.6 PO Account staff who are moving to another part of Fujitsu

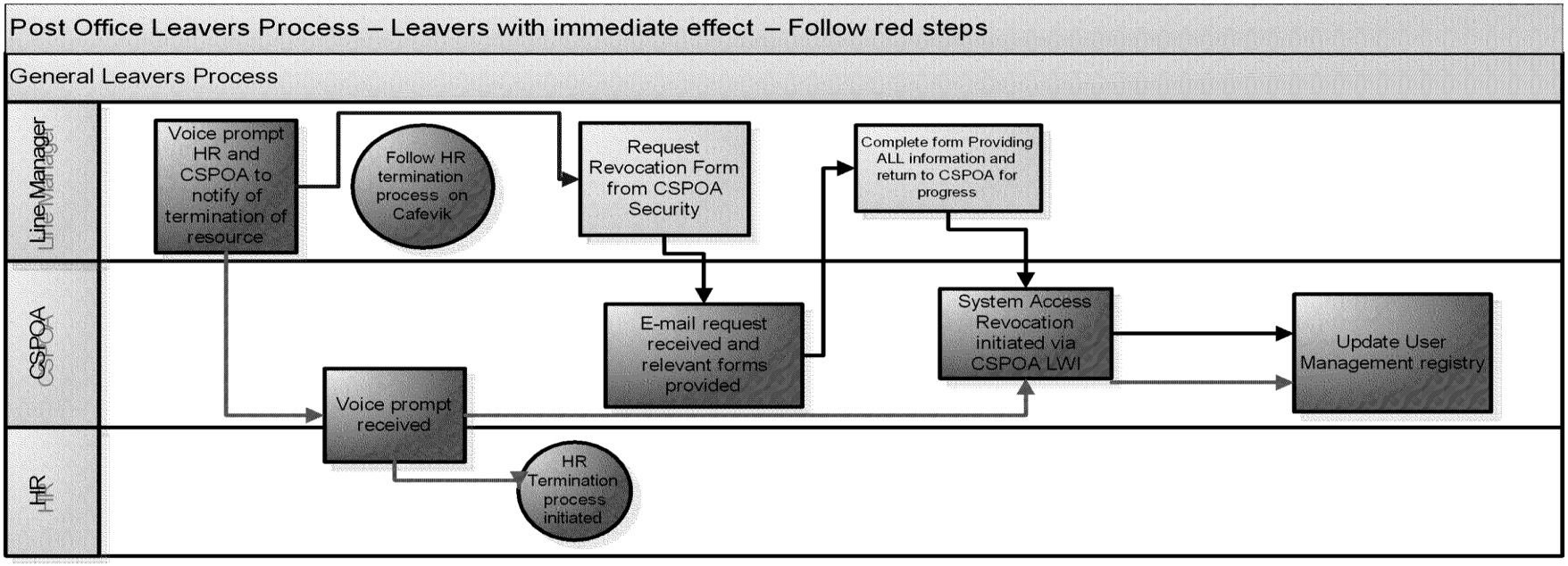
Line Managers whose staff are directly employed as part of Post Office Account and move to another part of Fujitsu shall follow the process in Section 4.3.3 for the termination of user's rights that are associated directly with systems dedicated to PO Account.

FUJ00088799



**Figure 1.2 Diagram of User system access flow for Leavers**

**Leavers with Immediate Effect is covered in RED**



FUJ00088799



# 5 Management

The User Access Process is 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 regular 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 Managers.
2. Line Managers shall review whether the current access of their employees is still in line with their job role.
3. Line managers shall consider whether any users require their access be amended and they shall follow the process defined in Section 3 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.

## 5.2 Reporting

- CSPOA Operational Security will audit access rights and roles with each functional area, this will be carried out on a biannual basis as minimum and will report findings in the Operational Security monthly dashboard report.
- 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 these will be disabled and the line manager contacted to confirm if situation with the user. Report findings will be detailed in the monthly Operational Security dashboard report.
- PMO will provide a report to CSPOA security on a monthly basis detailing all joiners, leavers and movers on the account from RIO's and ERIC's.
- CSPOA Operational Security will report on the following:

  This is not an exhaustive list

  - Individuals added to the Ikey Exemption List in the previous month
  - Individuals who have had system access levels amended for temporary reasons
  - Individuals added to the exceptions list detailing changes to the account
  - Joiners, Leavers and movers to the Account
  - POL SAP access report
  - Data Centre Access
- Reports will be reviewed jointly with PO Ltd at the regular Information Security Management Forum (ISMF)

## 5.3 Audit

FUJ00088799



All areas involved in the processes detailed in Section 3 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 3
2. Only authorised individuals have access to the assets that their role requires
3. The access provided is managed, monitored, reviewed and controlled

All audits shall be undertaken using the process defined in SVM/SEC/PRO/0036.

FUJ00088799



# 6 Appendix A

## 6.1 ISO27001

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

In the ISO 27001 framework the controls that we are required to meet fall into the following generic areas, People, Infrastructure, Applications, Control, Operations and Management Review and Monitoring and are detailed in full on the Security Operations SharePoint.

## 6.2 Security Requirements

This section defines the policies for controlling access to the PO Account IT systems in compliance with the Post Office CISP.

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

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

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

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

- Group property and Facilities management IRRELEVANT
- Human Resources IRRELEVANT
- Fujitsu Services Security (in particular Security vetting) - IRRELEVANT
- Risk management IRRELEVANT
- Data centre Access IRRELEVANT
- Resource requests IRRELEVANT
- Fujitsu BMS IRRELEVANT

Documentation of PO Account's own policies, processes and procedures is held on Dimensions and follows guidance provide in SVM/SEC/POL/0003 PO Account Information Security Policy.

FUJ00088799



# 7 Appendix B: Registry Fields – this is not a exhaustive list

| Type of Asset | Information stored |
|---|---|
| Individual | Team Name |
| | Location |
| | Role |
| | Line Manager |
| | First Name |
| | Surname |
| | UK number |
| | Security Clearance level |
| System to be Accessed | Dimensions |
| | Doors |
| | HNG-X Live |
| | Peak |
| | POLMI |
| | TACACS |
| | Live TesQA |
| | TFS |
| | Test Rig Access – LST |
| | Test Rig Access SV&I |
| | Logica Groups |
| | POLSAP |
| | Database Root |
| | Database Access |
| | Database Administrator UNIX |
| | SharePoint |
| | Quality Centre |
| | Tivoli |
| | Visual SourceSafe |
| | CVS |
| | PVCS |
| | Live BCMS |
| | MSC |
| | Secure Floor access BRA01 |

FUJ00088799



# 8 Appendix C: Sample forms only

These screenshots of the forms are for information only and not for use; originals must be requested via CSPOA Security Operations Team as per the defined processes.

## 8.1 New user access form

| POA HNG-X NEW USER ACCESS FORM | |
|---|---|
| **USER INFORMATION** | *Please enter information below* |
| First name | |
| Surname | |
| Personnel No (inc Country Code) | |
| Permanent (Yes/No) | |
| Job Title | |
| Email Address | |
| Contact number | |
| Corporate Domain login name | |
| Location | |
| Team | |
| Name of Line Manager | |
| Application/Join Date (Enter in format dd/mm/yyyy) | |
| | |
| What Dimensions Access is Required? | *Select from List* |
| 1 : Documentation Only (viewing and creating documents) | Documentation Only |
| 2: Documentation and Software CM | |
| 3: None | |
| | |
| Additional Information | *Please enter full name below* |
| TFS - Clone the account privilages of this person | |
| PEAK - Clone the account privilages of this person | |
| | |
| **All users must provide a 4 digit number and a memorable word to aid any password or Ikey resets required in the future** | *Please enter information below* |
| 4 Digit Number | |
| Memorable Word | |
| | |
| **Authorisation** | *Please sign below* |
| Signature of Applicant | |
| Signature of Line Manager | |
| | |
| CSPOA Security OPS use only | |
| Form Received and checked by: | |
| Date: | |
| | |
| **Please e-mail this to "CSPOA Security" mail box using the button below** | |

FUJ00088799



## 8.2 Revocation Form

| POA HNG-X Revoke USER ACCESS FORM | |
|---|---|
| **USER INFORMATION** | ***Please enter information below*** |
| First name | |
| Surname | |
| Personnel No (inc Country Code) | |
| Name of Line Manager | |
| Revoke Date (Enter in format dd/mm/yyyy) | |
| | |
| **Authorisation** | ***Please sign below*** |
| Signature of Applicant | |
| Signature of Line Manager | |
| | |
| CSPOA Security OPS use only | |
| Form Received and checked by: | |
| Date: | |
| | |
| **Please e-mail this to "CSPOA Security" mail box using the button below and send the signed paper copy via internal post to POA CS Security Ops, 4th Floor, Bra01.** | |

## 8.3 Post Office Access form

*See next page.*

FUJ00088799



# ID CARD & ACCESS REQUEST FORM

Group Security USE ONLY

| Card Number Issued | | Date Processed | |
|---|---|---|---|

| Completed By | Date | Time |
|---|---|---|

| Section 1 - Employee Details - To be Completed in ALL instances | |
|---|---|
| Title | Please choose |
| Surname | |
| First Name | |
| UK Personal Number (Fujitsu staff and Contractors) | |
| Employment Type<br>a) Fujitsu Employee – FJ<br>b) Authorized Contractor / Temp – C<br>c) Tenant - T | <br>Yes ☐ No ☐<br>Yes ☐ No ☐<br>Yes ☐ No ☐ |
| Contact Telephone Number | |
| Email Address | |
| Base Site Number (Permanent Office Location) | |
| Work Site Number(s) (Sites that are visited on a regular basis) | |
| Business Unit Name | |

| Section 2 - New Card Request - Picture Must be Attached | |
|---|---|
| Employment Start Date | |
| Card Type Required<br>a) ID Security Access Card – HID (SAFE)<br>b) SOL02/10 ID Card – Mag Stripe<br>c) Post Office Horizon ID Badge<br>d) Fujitsu Engineer ID Badge | <br>Yes ☐ No ☐<br>Yes ☐ No ☐<br>Yes ☐ No ☐<br>Yes ☐ No ☐ |
| Employment End Date (Temporary staff only) | |
| Company / Contract Name (Contractor / Temp / Tenant) | |

| Section 3 - Replacement Card | |
|---|---|
| Reason for Replacement | Please choose |
| Date Lost/Stolen card reported to 7733 | |
| Previous Card Number if known | |
| Card Type Required<br>e) ID Security Access Card – HID (SAFE)<br>f) SOL02/10 ID Card – Mag Stripe<br>g) Post Office Horizon ID Badge<br>h) Fujitsu Engineer ID Badge | <br>Yes ☐ No ☐<br>Yes ☐ No ☐<br>Yes ☐ No ☐<br>Yes ☐ No ☐ |

| Section 4 - Access Level Request –SAFE Sites only | |
|---|---|
| HID Card Number | |
| Access Level Required | |
| Access Times Required | Please choose |
| Additional Level / Doors Access Required | |
| Access Times Required | Please choose |
| Fire Marshal | Yes ☐ No ☐ |

| Section 5 – Authorisation - To be Completed in ALL Instances | | | |
|---|---|---|---|
| Business Unit Manager Name | | | |
| Contact Telephone Number | | | |
| Authorised | Yes ☐ No ☐ | Date | Time |

| Facilities Verification | | | |
|---|---|---|---|
| Cost Centre (Site Code) | | Facilities Manager Name | |
| Authorised | Yes ☐ No ☐ | Date | Time |

post office access form.doc6 SF026 Issue 6