FUJ00088005

Document Title:	**CSR+ ACCESS CONTROL AND USER ADMINISTRATION Processes and Procedures Description**
Document Type:	Processes and Procedures Description
Release:	CSR+
Abstract:	This document describes the processes and procedures required to provide the access control and user administration functions at post office counters
Document Status:	Approved
Author & Dept:	Helen Pharoah, Technical Design Authority
Contributors:	Richard Glanville, Eugene Dempsey
Reviewed By:	ICL Pathway: Margaret Cudlip, Alan D'Alvarez, John Dicks, Dean Felix, Graham Hooper, Alison Peacock, Keith Simons, Steve Warwick, Martin Whitehead. Bob Booth, Horizon Product Management
Comments By:	
Comments To:	Document Controller & Author
Distribution:	ICL Pathway Library, Pamela Coe, Andrew Donnelly, Brendan Nugent, Mik Peach.

FUJ00088005

0.0 Document Control

0.1 Document History

Version No.	Date	Reason for Issue	Associated CP/PinICL No.
0.1	20/08/99	Initial draft for ICL Pathway and Horizon review.	
0.2	01/10/99	Draft for ICL Pathway and Post Office Counters Ltd review.	
0.3	19/11/99	Draft for ICL Pathway and Post Office Counters Ltd review.	
0.4	14/01/00	Draft for ICL Pathway and Post Office Counters Ltd review.	
1.0	11/02/00	Approved.	

0.2 Approval Authorities

Name	Position	Signature	Date
Bob Booth	ACUA Product Manager, POCL Assurance, Horizon Programme		
Terry Austin	Development Director, ICL Pathway		

0.3 Associated Documents

Reference	Version	Title	Source
CR/FSP/0004	5.2	Service Architecture Design Document	ICL Pathway
CS/DES/012	1.0	CSR+ Access Control and User Administration PPD Design	ICL Pathway
CS/PRO/091	1.0	CSR+ Automated Payment Service PPD	ICL Pathway
CS/PRO/092	1.0	CSR+ Horizon System Helpdesk PPD	ICL Pathway
CS/PRO/093	1.0	CSR+ Introduction PPD	ICL Pathway
CS/PRO/094	1.0	CSR+ Order Book Control Service PPD	ICL Pathway

FUJ00088005

CS/PRO/095	1.0	CSR+ Electronic Point of Sale Service PPD	ICL Pathway
CS/PRO/096	1.0	CSR+ Logistics Feeder Service PPD	ICL Pathway
CS/PRO/097	1.0	CSR+ Operating Environment PPD	ICL Pathway
PA/STR/013	1.0	ICL Pathway Core System Release Plus Contents Description	ICL Pathway
SD/DOC/009	1.0	Horizon OPS Desktop Messages and Help Text: CSR+	ICL Pathway
SD/SPE/016	9.0	Horizon OPS Menu Hierarchy: Release 2	ICL Pathway
		Authorised-user Password Procedure	POCL

0.4 Abbreviations/Definitions

Abbreviation	Definition
ACUA	Access Control and User Administration
AP	Automated Payment
APS	Automated Payments Service
CSR+	Core System Release Plus
EPOSS	Electronic Point of Sale Service
HSH	Horizon System Helpdesk
ICL	International Computers Limited
LFS	Logistics Feeder Service
OBCS	Order Book Control Service
OPS	Office Platform Service
PIN	Personal Identity Number
PMMC	PostMaster's Memory Card
POCL	Post Office Counters Ltd
POLO	Post Office Logon
PPD	Processes and Procedures Description

0.5 Changes in this Version

Version	Changes
0.2	Comments received on V0.1 incorporated. POLO messages updated.

FUJ00088005

	Process for moveable outlets included. Processor shutdown facility included. Group added to User summary report (CCN391).
0.3	Comments received on V0.2 incorporated. Addition of access to final accounting facilities to the Auditor E group (CCN 557).
0.4	Comments received on V0.3 incorporated.
1.0	Comments received on V0.4 incorporated. Addition of confirmation message after either Shutdown or Restart has been selected. Correction of screen displayed following user deletion.

0.6 Changes Expected

Changes
Change of first line of support from HSH to NBSC (CRP0111).

FUJ00088005

0.7 Table of Contents

FUJ00088005

1 Purpose

This PPD describes the processes and procedures at post office counters in respect of access control and user administration, in accordance with ICL Pathway Core System Release Plus (CSR+).

This PPD provides a description of all the processes involved in order to enable the contractual agreement of procedures and to be a source from which authors can develop the further user documentation needed.

2 Scope

This PPD describes the following processes and procedures:

- Access control:
  - Post Office Logon (POLO)
  - System initialisation
  - System access
- Administrative functions:
  - User administration
  - User reports
- Data input rules:
  - User names
  - Full names
  - Passwords
  - Groups
- Security guidelines
- Fallback procedures

This PPD is one of a set of PPDs provided for CSR+. The way in which the set fits together is described in the CSR+ Introduction PPD [Ref. CS/PRO/093].

The use of the Horizon system and the method for contacting the Horizon System Helpdesk is described in the CSR+ Operating Environment PPD [Ref. CS/PRO/097].

FUJ00088005

With the exception of Post Office Logon messages, the text of which is given explicitly in this PPD, the screen messages described in this PPD are summarised and suffixed with a cross-reference in the form: '[Message *Collection:ObjectName*]' where *Collection* is the Collection name and *ObjectName* is the ObjectName within this collection. These relate to an entry in the Horizon OPS Desktop Messages and Help Text: CSR+ [Ref. SD/DOC/009] that defines the text of the message.

The Horizon System Helpdesk calls described in this PPD are cross-referenced to the calls described in the CSR+ Horizon System Helpdesk PPD [Ref. CS/PRO/092] as follows: 'Telephone the Horizon System Helpdesk [HSH call *ref*]' where *ref* is the call reference, for example SEC003. (Note that these cross-references are provided solely to assist PPD reviewers; the call references are not relevant to the helpdesk callers.)

Note: when the term 'workstation' is used in this PPD, it refers to the Horizon system PCs at the outlet. A workstation is sometimes also referred to as a counter.

3 Overview

Different levels of access are provided to the Horizon system according to role.

- Routine access

  All users are given a level of access to the system as determined by their responsibilities in the office. For example, only managers are allowed to create users. A full list of the applications to which each type of user is allowed access is given in the Horizon OPS Menu Hierarchy document: CSR+ [Ref. SD/SPE/033].

- Non-routine access

  If a Post Office Counters Ltd Retail Network Manager, Auditor, Investigator or other support personnel require access to the system then this will be obtained via the process described in *Section 9.3.1 Authorised-user passwords*.

Many access parameters are centrally configurable in the Horizon system's message store, for example session inactivity timeout and password expiry, and are set to values defined by Post Office Counters Ltd (see *Section 9.5 Centrally-configurable parameters*).

FUJ00088005

4 Post Office Logon

Post Office Logon allows a member of the outlet staff to unlock the file store of a system and gain access to the Horizon counter system. This procedure is used in either of the following circumstances:

- When the system is first started:
  - After installation (see *Section 4.1 Initialisation*).
  - After a workstation has been replaced (see *Sections 4.5 Replacement Gateway workstation* and *4.6 Replacement non-Gateway workstation*).
- When a workstation processor is switched back on after being powered off (see *Section 4.2 Regaining access to a switched-off workstation*).

The procedure involves the use of a memory card called a PMMC (PostMaster's Memory Card) and a PIN (Personal Identity Number). (Note that the PIN is actually a string of alphanumeric characters.)

4.1 Initialisation

This procedure generates the key with which the filestore is locked, and writes it to the PMMC. This procedure is performed when the system is installed, and is therefore a one-off activity.

To undertake this procedure, the entire Horizon system should be switched on; for further details refer to *Section 6.1 Daily Horizon system start-up*. The engineer will leave the Horizon system switched on after installation.

Two PMMCs are supplied with the system. One is used in the initialisation procedure and the other is a spare in case the first is mislaid.

4.1.1 Gateway workstation initialisation

The Gateway workstation is the link between the post office and the central systems. It is the processor of this workstation that must be initialised first to unlock the file store and gain access to the Horizon system. It will also be this processor that needs to be used in the event of changing PINs or lost PINs/PMMCs. The Gateway workstation will be identified as such by the words 'GATEWAY WORKSTATION' displayed on the top left of the screen.

Prior to initialisation the screen will display an animated picture of a hand inserting a card into the smart card reader with the instruction 'Please insert your Postmasters Memory Card (PMMC) …'.

For details regarding the location of the smart card reader, refer to the CSR+ Operating Environment PPD [Ref. CS/PRO/097].

FUJ00088005

4.1.1 Gateway workstation initialisation (contd)

Step 1. Insert one of the PMMCs into the reader, as the diagram on the screen illustrates. (Keep the other as a spare.)

Step 2. The counter printer should print a PIN on the counter printer's tally roll. (This is referred to as the PIN record.)

EXCEPTION A: If the counter printer does not print the PIN:

- Proceed as described in *Section 4.7.1 Counter printer failure*.

Step 3. The system displays the following message: 'Did the printer print the PIN completely (15 characters) and legibly?'

Proceed as follows:

SCENARIO A: If the counter printer has printed the PIN completely and legibly:

- Select the Yes option. The system displays the PIN number screen prompting you to enter your PIN.
- Remove the PIN record from the printer.
- Proceed to step 4.

SCENARIO B: If the counter printer has not printed the PIN completely and legibly:

- Select the No option. The system displays the message: 'Do you want to view the PIN on the screen instead?'
- Proceed as described in either Scenario B.1 or B.2 of step 3 in *Section 4.7.1 Counter printer failure*.

Step 4. Enter the PIN using the keyboard and select the Proceed option.

EXCEPTION A: If the PIN cannot be entered because the keyboard is not working:

- Telephone the Horizon System Helpdesk [HSH call POHC09].

Step 5. The system displays the message 'Attempting to get new security data. Please wait...' followed by 'Writing to the PMMC. Please wait...'.

EXCEPTION A: If the entered PIN is not accepted:

- Proceed as described in *Section 4.7.2 PIN entry failures*.

EXCEPTION B: If the system does not obtain the security data successfully:

- Proceed as described in *Section 4.7.3 Communication failures*.

FUJ00088005

4.1.1 Gateway workstation initialisation (contd)

Step 6. Proceed as follows:

SCENARIO A: Where there are no other workstations:

- The system displays the following set of instructions:

  'PLEASE

  (1) Remove the PMMC and store in a secure location,

  (2) Store the PIN record in a secure location, separate from the PMMC,

  (3) Touch PROCEED then please wait whilst the Horizon system is being started.'

- Gently remove the PMMC from the card reader.
- Store the PMMC in a secure location, ensuring it is separate from the PIN record.
- Store the PIN record in a secure location separate from the PMMC.
- Select the Proceed option.
- Proceed to step 7.

SCENARIO B: Where there are other counter workstations (non-Gateway):

- The system displays the following set of instructions:

  'PLEASE

  (1) Remove the PMMC,

  (2) Use PMMC and PIN to initialise other workstations,

  (3) Touch PROCEED then please wait whilst the Horizon system is being started.'

- Gently remove the PMMC from the card reader.
- Select the Proceed option.
- For each other counter workstation in turn, follow the instructions in *Section 4.1.2 Non-Gateway workstation initialisation*.

Step 7. The system displays the message 'Starting services. Please Wait…' and initialises, during which there will be a time lapse and access will be prohibited. (The length of the time lapse cannot be specified exactly as it will vary depending upon the circumstances in which the system is being initialised and the size of the message store on the counter in question.) When the Riposte logo appears initialisation is complete.

Step 8. You may now log on to the Horizon system (see *Section 6.2 Logon*).

FUJ00088005

4.1.2 Non-Gateway workstation initialisation

Non-Gateway workstations include any additional workstations, other than the Gateway workstation, connected to the Horizon system within the post office.

Both the PIN and the PMMC are required to perform this procedure. If either the PIN record or the PMMC is unavailable, follow the procedure in *Section 4.3 Lost PIN/PMMC.*

Prior to initialisation, the workstation should be switched on and the screen will display an animated picture of a hand inserting a card into the card reader with the instruction 'Please insert your Postmasters Memory Card (PMMC) …'.

If this procedure is being followed at any time other than initialisation, and this screen is not displayed, the workstation must be shut down and switched off (see *Section 6.15 Shutting down a processor*) and switched on again to obtain this screen.

Step 1. Insert the PMMC into the reader, as the diagram on the screen illustrates.
(The system displays the PIN Number screen.)

Step 2. The following message is displayed: 'Please enter your PIN'.

Step 3. Enter the PIN using the keyboard.

EXCEPTION A: If the PIN cannot be entered because the keyboard is not working:

- Telephone the Horizon System Helpdesk [HSH call POHC09].

Step 4. Select the Proceed option.

EXCEPTION A: If the entered PIN is not accepted:

- Proceed as described in *Section 4.7.2 PIN entry failures*.

Step 5. The system displays the following set of instructions:

'PLEASE

(1) Remove the PMMC,

(2) Use PMMC and PIN to initialise other workstations if required, otherwise store PMMC and PIN in separate secure locations,

(3) Touch PROCEED then please wait whilst the Horizon system is being started.'

Step 6. Gently remove the PMMC from the card reader.

Step 7. Select the Proceed option.

FUJ00088005

4.1.2 Non-Gateway workstation initialisation (contd)

Step 8. The system displays the message 'Starting services. Please Wait…' and initialises, during which there will be a time lapse and access will be prohibited. (The length of the time lapse cannot be specified exactly as it will vary depending upon the circumstances in which the system is being initialised and the size of the message store on the counter in question.) When the Riposte logo appears initialisation is complete.

Step 9. You may now log on to the Horizon system (see *Section 6.2 Logon*).

Step 10. Repeat steps 1 to 9 for each non-Gateway workstation to be initialised.

Step 11. Store the PMMC in a secure location, ensuring it is separate from the PIN record.

Step 12. Store the PIN record in a secure location, separate from the PMMC.

4.2 Regaining access to a switched-off workstation

If either the PIN record or the PMMC is unavailable, follow the procedure in *Section 4.3 Lost PIN/PMMC.*

If a power failure has taken all the workstations down, then access must first be regained on the Gateway workstation. (If the Gateway workstation cannot be started, then, provided that the PIN record and the PMMC are available, access can be regained on the non-Gateway workstations. However, there will no external communication with the centre.)

4.2.1 Regaining access to a switched-off non-Gateway workstation

The procedure to regain access to the Horizon system in the event of the processor of a non-Gateway workstation being switched off is as follows:

Step 1. Switch on the workstation's processor and the remaining components of the workstation as outlined in *Section 6.1 Daily Horizon system start-up*.

EXCEPTION A: If the processor and components are already switched on (this could be the case where the power has now been restored after a power failure):

- Proceed to step 2.

Step 2. Follow the instructions outlined in *Section 4.1.2 Non-Gateway workstation initialisation*.

FUJ00088005

4.2.2 Regaining access to a switched-off Gateway workstation

The procedure to regain access to the Horizon system in the event of the processor of a Gateway workstation being switched off is as follows:

Step 1. Switch on the workstation's processor and the remaining components of the workstation as outlined in *Section 6.1 Daily Horizon system start-up*.

EXCEPTION A: If the processor and components are already switched on (this could be the case where the power has now been restored after a power failure):

- Proceed to step 2.

Step 2. Insert the PMMC into the reader, as the diagram on the screen illustrates.
(The system displays the PIN Number screen.)

Step 3. The following message is displayed: 'Please enter your PIN'.

Step 4. Enter the PIN using the keyboard.

EXCEPTION A: If the PIN cannot be entered because the keyboard is not working:

- Telephone the Horizon System Helpdesk [HSH call POHC09].

Step 5. Select the Proceed option.

EXCEPTION A: If the entered PIN is not accepted:

- Proceed as described in *Section 4.7.2 PIN entry failures*.

Step 6. Proceed as follows:

SCENARIO A: If the system displays the message 'This office has been scheduled to receive new security data. The delivery of this data is expected to take a short time. You may choose to delay this operation to another time. Do not delay the data delivery unnecessarily':

SCENARIO A.1: To proceed with the operation:

- Select the Proceed option.
- Proceed to step 7.

SCENARIO A.2: To delay the operation:

- Select the Delay option.
- Proceed to step 12.

SCENARIO B: If the system does not display this message:

- Proceed to step 12.

FUJ00088005

4.2.2 Regaining access to a switched-off Gateway workstation (contd)

Step 7. The counter printer should print a new PIN on the counter printer's tally roll.

EXCEPTION A: If the counter printer does not print the PIN:

- Proceed as described in *Section 4.7.1 Counter printer failure*.

Step 8. The system displays the following message: 'Did the printer print the PIN completely (15 characters) and legibly?'

Proceed as follows:

SCENARIO A: If the counter printer has printed the PIN completely and legibly:

- Select the Yes option. The system displays the PIN number screen prompting you to enter your PIN.
- Remove the PIN record from the printer.
- Proceed to step 9.

SCENARIO B: If the counter printer has not printed the PIN completely and legibly:

- Select the No option. The system displays the message: 'Do you want to view the PIN on the screen instead?'
- Proceed as described in either Scenario B.1 or B.2 of step 3 in *Section 4.7.1 Counter printer failure*.

Step 9. Enter the new PIN using the keyboard and select the Proceed option.

EXCEPTION A: If the PIN cannot be entered because the keyboard is not working:

- Telephone the Horizon System Helpdesk [HSH call POHC09].

Step 10. The system displays the message 'Writing to the PMMC. Please wait...'.

EXCEPTION A: If the entered PIN is not accepted:

- Proceed as described in *Section 4.7.2 PIN entry failures*.

Step 11. The system displays the message 'Attempting to get new security data. Please wait...' followed by '' 'Writing to the PMMC. Please wait...' and optionally by 'Processing. Please wait...'.

EXCEPTION A: If the system does not obtain the security data successfully:

- Proceed as described in *Section 4.7.3 Communication failures*.

FUJ00088005

4.2.2 Regaining access to a switched-off Gateway workstation (contd)

Step 12. Proceed as follows:

SCENARIO A: Where there are no other workstations:

- The system displays the following set of instructions:

  'PLEASE

  (1) Remove the PMMC and store in a secure location,

  (2) Store the PIN record in a secure location, separate from the PMMC,

  (3) Touch PROCEED then please wait whilst the Horizon system is being started.'

- Proceed to step 13.

SCENARIO B: Where there are other workstations (non-Gateway):

- The system displays the following message:

  'At the earliest convenient opportunity the new PMMC and PIN should be used to initialise each of the other workstations at this office.'

- Select the OK option.
- The system displays the following set of instructions:

  'PLEASE

  (1) Remove the PMMC,

  (2) Use PMMC and PIN to initialise other workstations if required, otherwise store PMMC and PIN in separate secure locations,

  (3) Touch PROCEED then please wait whilst the Horizon system is being started.'

- Proceed to step 13.

Step 13. Gently remove the PMMC from the card reader.

Step 14. Select the Proceed option.

Step 15. The system displays the message 'Starting services. Please Wait…' and initialises, during which there will be a time lapse and access will be prohibited. (The length of the time lapse cannot be specified exactly as it will vary depending upon the circumstances in which the system is being initialised and the size of the message store on the counter in question.) When the Riposte logo appears initialisation is complete.

Step 16. You may now log on to the Horizon system (see *Section 6.2 Logon*).

FUJ00088005

4.2.2 Regaining access to a switched-off Gateway workstation (contd)

Step 17. Proceed as follows:

SCENARIO A: Where only the Gateway was switched off and no new security data was received:

- Store the PMMC in a secure location, ensuring it is separate from the PIN record.
- Store the PIN record in a secure location separate from the PMMC.
- This ends the procedure.

SCENARIO B: Where there are either other counter workstations (non-Gateway) switched off or new security data was received:

- For each other counter workstation in turn, follow the instructions in *Section 4.1.2Non-Gateway workstation initialisation.*

Note: If the non-Gateway workstations are not already switched off then this may be done at a convenient time so that the post office has minimum disruption.

4.3 Lost PIN/PMMC

This procedure must be followed in the event that a workstation is switched off and either the PIN record or the PMMC is unavailable. Without the PIN and PMMC, the protected filestore cannot be unlocked. The procedure in this section describes how the Post Master and helpdesk create a new set of both PMMC and PIN to unlock the protected filestore. No data is lost on the counter. If, however, the old set of PMMC and PIN are subsequently found, they will not work on the counter.

This procedure is performed at the Gateway workstation.

Note:

- If the original workstation switched off was not the Gateway workstation, then, to avoid disabling the office, this procedure can be left until a more convenient time. This means that it will not be possible to use the affected workstation though all others will be available.

FUJ00088005

4.3 Lost PIN/PMMC (contd)

Step 1. If you have lost your PMMC, check that you have the spare.

EXCEPTION A: If you do not have a spare PMMC:

- Telephone the Horizon System Helpdesk [HSH call SEC002].

Step 2. Ensure the Gateway workstation is switched on and displaying the animated picture and the instruction to 'Please insert your Postmasters Memory Card (PMMC) …'.

(If the Gateway workstation was not the one switched off, any user at this workstation must log out and the processor must be shut down and switched off (see *Section 6.15 Shutting down a processor)* and switched on again to obtain this screen.)

SCENARIO A: If the PIN is unavailable:

- Insert the PMMC into the card reader, as the diagram on the screen illustrates. The system displays the PIN Number screen.
- Select the Lost PIN option.
- Proceed to step 3.

SCENARIO B: If the PMMC is unavailable:

- Select the Lost PMMC option.
- The system displays the 'Please insert your spare Postmasters Memory Card (PMMC) …' screen. Insert the spare PMMC into the card reader.
- Proceed to step 3.

Step 3. The system displays the following screen requesting you to contact the Horizon System Helpdesk:

'Please telephone the Horizon System Help Desk and await instructions.

DO NOT proceed beyond this screen until directed by the Help Desk.'

Step 4. Telephone the Horizon System Helpdesk [HSH call SEC002].

Step 5. Proceed as instructed by the helpdesk:

SCENARIO A: If the operator tells you to touch the Proceed button:

- Select the Proceed option.
- Proceed to step 6.

FUJ00088005

4.3 Lost PIN/PMMC (contd)

SCENARIO B: If the operator tells you to touch the Fallback button:

- Select the Fallback option. (The system displays the Fallback Request Code screen. The screen contains a line of 15 alphanumeric characters.)
- Read out, over the telephone, the line of 15 alphanumeric characters. Await confirmation from the operator.
- Select the Proceed option. (The system displays the Fallback Response Code screen.)
- Type in the 15 alphanumeric characters provided by the operator and select the Proceed option.

EXCEPTION B.1: If the response code cannot be entered because the keyboard is not working:

- Advise the operator and await instructions.

- Proceed to step 6.

Step 6. The counter printer should print a new PIN record on the counter printer's tally roll.

EXCEPTION A: If the counter printer does not print the PIN:

- Proceed as described in *Section 4.7.1 Counter printer failure*.

Step 7. The system displays the following message: 'Did the printer print the PIN completely (15 characters) and legibly?'

Proceed as follows:

SCENARIO A: If the counter printer has printed the PIN completely and legibly:

- Select the Yes option. The system displays the PIN number screen prompting you to enter your PIN.
- Remove the PIN record from the printer.
- Proceed to step 8.

SCENARIO B: If the counter printer has not printed the PIN completely and legibly:

- Select the No option. The system displays the message: 'Do you want to view the PIN on the screen instead?'
- Proceed as described in either Scenario B.1 or B.2 of step 3 in *Section 4.7.1 Counter printer failure*.

FUJ00088005

4.3 Lost PIN/PMMC (contd)

Step 8. Enter the PIN using the keyboard and select the Proceed option.

EXCEPTION A: If the PIN cannot be entered because the keyboard is not working:

- Inform the operator (if still on the phone) or telephone the Horizon System Helpdesk [HSH call POHC09].

Step 9. Proceed as follows:

SCENARIO A: For a normal recovery (i.e. step 5 Scenario A):

- The system displays the message 'Attempting to get new security data. Please wait...' followed by **'**Writing to the PMMC. Please wait...'**.**
- Proceed to step 10.

EXCEPTION A.1: If the system does not obtain the security data successfully:

- Proceed as described in *Section 4.7.3 Communication failures*.

SCENARIO B: For fallback recovery (i.e. step 5 Scenario B):

- The system displays the message **'**Writing to the PMMC. Please wait...'**.**
- Proceed to step 10.

Step 10. The system displays the following set of instructions:

'PLEASE

(1) Remove the PMMC and store in a secure location,

(2) Store the PIN record in a secure location, separate from the PMMC,

(3) Touch PROCEED then please wait whilst the Horizon system is being started.'

Step 11. Advise the operator that this point has been reached. The operator may terminate the call.

Step 12. If there is an old PIN record, destroy it.

Step 13. Gently remove the PMMC from the card reader.

Step 14. Store the PMMC in a secure location, ensuring it is separate from the PIN record.

Step 15. Store the PIN record in a secure location separate from the PMMC.

Step 16. Select the Proceed option.

FUJ00088005

4.3 Lost PIN/PMMC (contd)

Step 17. The system displays the message 'Starting services. Please Wait…' and initialises, during which there will be a time lapse and access will be prohibited. (The length of the time lapse cannot be specified exactly as it will vary depending upon the circumstances in which the system is being initialised and the size of the message store on the counter in question.) When the Riposte logo appears initialisation is complete.

Step 18. You may now log on to the Horizon system (see *Section 6.2 Logon*).

4.4 Changing a PIN

If there is reason to believe that the integrity of the PIN has been compromised, as this may allow unauthorised access, the PIN must be changed. This can only be done at the Gateway workstation. Both the PIN and the PMMC are required to perform this procedure.

Changing the PIN affects the Gateway workstation only; the non-Gateway workstations do not need to be restarted. However, while the Gateway workstation is out of action (Riposte desktop not running) there is no external communication with the centre. Any non-Gateway counters will still be available for use.

Step 1. Ensure that you have your PMMC and PIN.

Step 2. Shut down the Gateway workstation's processor and switch off (see *Section 6.15 Shutting down a processor)*.

Step 3. Turn on the Gateway workstation's processor, by using the On/Off Switch.
(The screen displays an animated picture of a hand inserting a card into the card reader with the instruction 'Please insert your Postmasters Memory Card (PMMC) …'.)

Step 4. Insert the PMMC into the card reader, as the diagram on the screen illustrates.
(The system displays the PIN Number screen.)

Step 5. The following message is displayed: 'Please enter your PIN'.

Step 6. Enter the PIN using the keyboard.

EXCEPTION A: If the PIN cannot be entered because the keyboard is not working:

- Telephone the Horizon System Helpdesk [HSH call POHC09].

Step 7. Select the Change PIN option.

FUJ00088005

4.4 Changing a PIN (contd)

Step 8. The counter printer should print a new PIN on the counter printer's tally roll.

EXCEPTION A: If the counter printer does not print the PIN:

- Proceed as described in *Section 4.7.1 Counter printer failure*.

EXCEPTION B: If the entered PIN is not accepted:

- Proceed as described in *Section 4.7.2 PIN entry failures*.

Step 9. The system displays the following message: 'Did the printer print the PIN completely (15 characters) and legibly?'

Proceed as follows:

SCENARIO A: If the counter printer has printed the PIN completely and legibly:

- Select the Yes option. The system displays the PIN number screen prompting you to enter your PIN.
- Remove the PIN record from the printer.
- Proceed to step 10.

SCENARIO B: If the counter printer has not printed the PIN completely and legibly:

- Select the No option. The system displays the message: 'Do you want to view the PIN on the screen instead?'
- Proceed as described in either Scenario B.1 or B.2 of step 3 in *Section 4.7.1 Counter printer failure*.

Step 10. Enter the new PIN using the keyboard and select the Proceed option.

EXCEPTION A: If the PIN cannot be entered because the keyboard is not working:

- Telephone the Horizon System Helpdesk [HSH call POHC09].

Step 11. The system displays: 'Writing to the PMMC. Please wait…'.

EXCEPTION A: If the entered PIN is not accepted:

- Proceed as described in *Section 4.7.2 PIN entry failures*.

Step 12. The system displays the message: 'If you have an old PIN record, this should be destroyed NOW'.

Step 13. Destroy the old PIN record and select the OK option.

FUJ00088005

4.4 Changing a PIN (contd)

Step 14. The system displays the following set of instructions:

'PLEASE

(1) Remove the PMMC and store in a secure location,

(2) Store the PIN record in a secure location, separate from the PMMC,

(3) Touch PROCEED then please wait whilst the Horizon system is being started.'

Step 15. Gently remove the PMMC from the card reader.

Step 16. Store the PMMC in a secure location, ensuring it is separate from the PIN record.

Step 17. Store the PIN record in a secure location, separate from the PMMC.

Step 18. Select the Proceed option.

Step 19. The system displays the message 'Starting services. Please Wait…' and initialises, during which there will be a time lapse and access will be prohibited. (The length of the time lapse cannot be specified exactly as it will vary depending upon the circumstances in which the system is being initialised and the size of the message store on the counter in question.) When the Riposte logo appears initialisation is complete.

Step 20. You may now log on to the Horizon system (see *Section 6.2 Logon*).

4.5 Replacement Gateway workstation

If an engineer replaces the Gateway workstation of the Horizon system, the procedure below should be followed.

Note: in a multi-workstation office, non-Gateway workstations may be used in local mode (meaning that they have no communication with the external data centres and are functioning in isolation so that only transactions that do not require communication with the central system can be performed), until the Gateway workstation is re-started as described below. The non-Gateway workstations do not need to be restarted.

If the PIN record is lost, a new PIN can be generated. If the PMMC is lost, the spare can be used. If both PMMCs are unavailable, the engineer will telephone the Horizon System Helpdesk [HSH call SEC002].

FUJ00088005

4.5 Replacement Gateway workstation (contd)

Step 1. Insert the PMMC into the reader, as the diagram on the screen illustrates.

EXCEPTION A: If the PMMC is unavailable:

- Select the Lost PMMC option.
- The system displays the 'Please insert your spare Postmasters Memory Card (PMMC) …' screen. Insert the spare PMMC into the card reader.
- Perform steps 3 to 12 of *Section 4.3 Lost PIN/PMMC* (note that in step 5, Scenario B is not applicable) and then resume this procedure at step 6.

Step 2. The following message is displayed: 'Please enter your PIN'.

Step 3. Enter the PIN using the keyboard and select the Proceed option.

EXCEPTION A: If the PIN cannot be entered because the keyboard is not working:

- Telephone the Horizon System Helpdesk [HSH call POHC09].

EXCEPTION B: If the PIN is unavailable:

- Select the Lost PIN option.
- Perform steps 3 to 11 of *Section 4.3 Lost PIN/PMMC* (note that in step 5, Scenario B is not applicable) and then resume this procedure at step 6.

Step 4. The system displays the message 'Attempting to get new security data. Please wait...'.

EXCEPTION A: If the entered PIN is not accepted:

- Proceed as described in *Section 4.7.2 PIN entry failures*.

Step 5. The system displays the following set of instructions:

SCENARIO A: Where there are no other workstations:

'PLEASE

(1) Remove the PMMC and store in a secure location,

(2) Store the PIN record in a secure location, separate from the PMMC,

(3) Touch PROCEED then please wait whilst the Horizon system is being started.'

FUJ00088005

4.5 Replacement Gateway workstation (contd)

SCENARIO B: Where there are other workstations (non-Gateway):

'PLEASE

(1) Remove the PMMC,

(2) Use PMMC and PIN to initialise other workstations if required, otherwise store PMMC and PIN in separate secure locations,

(3) Touch PROCEED then please wait whilst the Horizon system is being started.'

Note: However, in this case, no other workstations require to be initialised.

EXCEPTION A: If the system does not obtain the security data successfully:

- Proceed as described in *Section 4.7.3 Communication failures*.

Step 6. Gently remove the PMMC from the card reader.

Step 7. Store the PMMC in a secure location, ensuring it is separate from the PIN record.

Step 8. Store the PIN record in a secure location separate from the PMMC.

Step 9. Select the Proceed option.

Step 10. The system displays the message 'Starting services. Please Wait…' and initialises, during which there will be a time lapse and access will be prohibited. (The length of the time lapse cannot be specified exactly as it will vary depending upon the circumstances in which the system is being initialised and the size of the message store on the counter in question.) When the Riposte logo appears initialisation is complete.

Step 11. You may now log on to the Horizon system (see *Section 6.2 Logon*).

4.6 Replacement non-Gateway workstation

If an engineer replaces a non-Gateway workstation of the Horizon system, follow the procedure in *Section 4.1.2 Non-Gateway workstation initialisation*, omitting step 10 as no other non-Gateway workstations require to be initialised.

4.7 General processes and procedures

This section describes processes and procedures generic to POLO transactions.

FUJ00088005

4.7.1 Counter printer failure

Counter printer failure will prevent the printing of the PIN record. If the problem cannot be overcome, the fallback process is to create a manual PIN record.

The procedure is as follows:

Step 1. The system displays the message 'Cannot print the PIN record' followed by the reason (for example, 'The counter printer is not responding. Check that it is turned on and connected.').

Step 2. Check the counter printer and take any remedial action as suggested in the message.

Step 3. Proceed as follows:

SCENARIO A: If the printer prints the PIN:

- The procedure continues with the message 'Did the printer print the PIN completely (15 characters) and legibly?'

SCENARIO B: If the printer does not print the PIN:

- Select the Cancel option on the 'Cannot print the PIN record' screen.
- The system displays the message: 'Do you want to view the PIN on the screen instead?'

SCENARIO B.1: If you want to view the PIN:

- Select the Yes option.
- The system displays the message: 'Please make a note of your new PIN' and shows the PIN on the screen.
- Write down the PIN and select Proceed.
- The procedure continues with the PIN number screen prompting you to enter your PIN.

SCENARIO B.2: If you do not want to view the PIN:

- Select the No option.
- The system displays the message: 'Failed to print PIN record. Please remove your PMMC and take remedial action with the printer.'
- Remove the PMMC. The system returns to the initial screen of the procedure.

FUJ00088005

4.7.2 PIN entry failures

If a typed-in PIN is not accepted, one of the following exceptions occurs and the user is given the opportunity to correct their entry.

EXCEPTION A: If the PIN field is empty, the system displays the message 'Please enter your current PIN before proceeding':

- Select the OK option.
(The system returns to the PIN entry screen.)
- Enter the PIN.

EXCEPTION B: If the PIN is invalid or incomplete (if there is a fault within the PIN, for example, not all characters provided, invalid character entered or a check on the whole PIN fails), the system displays the message ' There is a typing error in this PIN':

- Select the OK option.
(The system returns to the PIN entry screen.)
- Re-enter the PIN.

EXCEPTION B.1: If the PIN is not accepted (although entered correctly:

- Try re-entering the PIN a few times. If the PIN is still not accepted, telephone the Horizon System Helpdesk [HSH call SEC002].

EXCEPTION C: If the PIN is wrong, (the entered PIN passes the checks carried out in Exception B, but is not valid for this counter), the system displays the message 'This appears to be an invalid PIN, although it may be simply mis-typed. Check that you are using a true record of the current PIN, and the correct PMMC. If you are using a record of an out-of-date PIN, DESTROY IT IMMEDIATELY and use the current PIN record.':

- Select the OK option.
(The system returns to the PIN entry screen.)
- Check the PIN record as stated in the message.
- Re-enter the PIN.

FUJ00088005

4.1.3 Communication failures

If security data is not obtained successfully from the data centre, one of the following exceptions occurs:

EXCEPTION A: If the system displays the message 'Communication with the centre failed. Could not get new security data. Do you want to try again?':

- Proceed as follows:

SCENARIO A.1: To retry the attempt to get security data:

- Select the Yes option.
- The attempt is repeated.

(Note: there is no limit to the number of retries.)

SCENARIO A.2: To abandon the attempt to get security data:

- Select the No option.
- The system displays an error message (for example, 'Initialisation of the new counter has failed.') and returns to the initial screen of the procedure.

EXCEPTION B: If the system displays the message 'The received security data was unusable.':

- Select the OK option.
- The system displays an error message (for example, 'Initialisation of the new counter has failed.') and returns to the initial screen of the procedure.

FUJ00088005

5 System initialisation

After the Horizon system has been installed, the manager MUST perform the system initialisation procedure. This allows the manager to set up a user identity for themselves with manager access, after which they can create identities for other users.

Business rules:

- All users must have been through the Horizon Service Training Event and passed the competency test.

The set up procedure is as follows:

Step 1. Log on to the system with the user name ZSET01 and the password FIRST1 (see *Section 6.2 Logon*).

Step 2. Create a user identity for yourself with manager access (see *Section 7.1.1 Adding a user: procedure*).

Step 3. Log out (see *Section 6.12 Logout*).

Step 4. Log on as the new manager user.

Step 5. Delete the ZSET01 user (see *Section 7.3 Deleting a user*).

EXCEPTION A: If you are not able to delete the ZSET01 user (that is, you do not have manager access):

- Log out.
- Repeat steps 1 to 5, but in step 2 modify your existing user identity to give yourself manager access (see *Section 7.2.1 Modifying a user: procedure).*

Step 6. Create all additional users if required (see *Section 7.1.1 Adding a user: procedure*).

FUJ00088005

6 System access

This section describes the following system access procedures:

- Daily Horizon system start-up.
- Logon.
- Change of password by user.
- Enforced change of password facility.
- Forgotten password.
- Session mobility.
- Temporary lock.
- Session inactivity time-out.
- Over-riding the current user.
- Forced logout.
- Logout.
- Daily Horizon system shutdown.
- Moveable outlets.
- Shutting down a processor.

6.1 Daily Horizon system start-up

The start-up procedure for the counter system is as follows:

Step 1. Ensure the office equipment is connected to the power supply.

Step 2. Press the switch on the monitor to the 'I' or 'on' position.

Step 3. Press the switch on the counter printer to the 'I' or 'on' position.

(The reports printer need only be switched on when required.)

Note: The processor will only require switching on at the first time of operation and if there has been reason for it to be switched off, for example, if instructed by the Horizon System Helpdesk. In normal circumstances, the processor will be left switched on at all times to enable the transfer of data. No re-connection of any cables to the system should be done by the user - excepting ensuring that the power cable is plugged into the mains socket and turned on. Any other reconnection of cables requires a call to the Horizon System Helpdesk [HSH call POHC12].

If the processor is switched off by accident, the procedure described in *Section 4.2 Regaining access to a switched-off workstation* must be followed.

FUJ00088005

Note: Refer to the CSR+ Operating Environment PPD [Ref.CS/PRO/097] for hardware checks that should be performed if any of the equipment is not functioning correctly.

6.2 Logon

This function is used to enable a user to enter their user name and password in order to access the system.

System rules:

- The user is allowed a number of logon attempts before they are locked out of the system. The maximum number of logon attempts, the period during which the attempts are measured, and the period that the account remains locked if the number of attempts is exceeded, are configurable parameters (see *Section 9.5 Centrally-configurable parameters*).

The procedure to log on is as follows:

Step 1. Ensure that the system is displaying the initial screen with the Riposte logo in the centre of the screen.

Step 2. Touch the screen or press any key.
(The system displays the agreement screen [Message DesktopInfo:LogonAcknowledgement].)

Step 3. If you agree, select the Tick option.
(The system displays the Logon screen.)

Step 4. Enter your user name and select the Tick option.

Step 5. Enter your user password and select the Tick option.

Step 6. The system undertakes initialisation checks, and displays the date and time of the user's last successful logon and the number of failed attempts.

EXCEPTION A: If the logon attempt fails (that is, if the wrong user name or password has been entered):

- The system displays an error message prompts for re-entry [Message NS_TRState_ENG:IgnInvalidLogon].
- Proceed to step 4 or 5 as appropriate.

FUJ00088005

6.2 Logon (contd)

EXCEPTION B: If the maximum number of failed logon attempts has been reached:

- The user account is locked and the system returns to the initial screen with the Riposte logo in the centre of the screen. The lockout lasts until the preset period has expired (see *Section 9.5 Centrally-configurable parameters*) or the account is unlocked by the manager (see *Section 7.2.1.2 Modifying a user's options*).
- This ends the procedure.

Step 7. Check the logon details (that is, the date and time of the last successful logon and the number of failed attempts) on the screen.

SCENARIO A: If the logon details are recognised:

- Select the Tick option.
- Proceed to step 8.

SCENARIO B: If the logon details are not recognised:

- Select the Cross option.
- Telephone the Horizon System Helpdesk [HSH call SEC007].
- This ends the procedure.

Step 8. The system displays the Desktop.

EXCEPTION A: If there is currently no stock unit assigned to your logon account:

- The system assigns the default stock unit and advises you to notify your supervisor [Message EPOSS:MSG17].
- Select the Tick option.
  (The system displays the Desktop. The set of functions available to you will be limited.)

FUJ00088005

6.3 Change of password by user

This function allows the user to change their own password. For information on passwords, see *Section 9.3 Passwords*.

The procedure to change a password is as follows:

Step 1. From the Desktop, select the Administration option, the User option, then the Change Password option.
(The system displays the Change Password screen.)

Step 2. Enter the old password and select the Tick option.

EXCEPTION A: If, when re-entering the old password, you make a mistake, the system says that your password is incorrect and asks you to try again [Message NS_UserMaintenance_ENG:umOldPWordInvalid]:

- Select the Tick option.
(The system displays the Change Password screen.)
- Delete the password that you have entered.
- Re-enter your old password.
- Select the Tick option.
- Proceed to step 3.

Step 3. Enter the new password and select the Tick option. For password standards, see *Section 9.3 Passwords*.
(The system displays the Confirm Password screen.)

EXCEPTION A: If you enter a password that does not conform to password standards, the system says that it is unable to change your password as the new password is invalid [Message NS_UserMaintenance_ENG:umNewPWordInvalid]:

- Select the Tick option.
(The system displays the Change Password screen.)
- Delete the password that you have entered.
- Enter a password that conforms to password standards.
- Select the Tick option.
- Proceed to step 4.

FUJ00088005

6.3 Change of password by user (contd)

Step 4. Re-enter the new password and select the Tick option.
(The system returns to the Administration screen.)

EXCEPTION A: If, when re-entering the new password, you enter a password that does not match your new password, the system says that the password and confirmation do not match [Message ErrorMsgs:NoPwdMatch]:

- Select the Tick option.
(The system re-displays the Confirm Password screen.)
- Delete the password that you have entered.
- Re-enter your new password.
- Select the Tick option.
(The system returns to the Administration screen.)

6.4 Enforced change of password facility

This function is activated automatically when either the user's password has expired or the password has been allocated by the manager. The system prompts the user (after initial logon) to change their password.

The procedure is as follows:

Step 1. After entering your user name and password (see *Section 6.2 Logon*), the system says that the password has expired and you must change your password before logging on [Message NS_TRState_ENG:lgnPasswordExpiredMsg].

Step 2. Select the Tick option.
(The system displays the Change Password screen.)

Step 3. Enter the new password and select the Tick option. For password standards, see *Section 9.3 Passwords*.

EXCEPTION A: If you enter a password that does not conform to password standards, the system says that it is unable to change your password as the new password is invalid [Message NS_UserMaintenance_ENG:umNewPWordInvalid]:

- Select the Tick option.
(The system displays the Change Password screen.)
- Delete the password that you have entered.
- Enter a password that conforms to password standards.
- Select the Tick option.
- Proceed to step 4.

FUJ00088005

6.4 Enforced change of password facility (contd)

Step 4. Re-enter the new password and select the Tick option.
(The system returns to the Desktop.)

EXCEPTION A: If, when re-entering the new password, you enter a password that does not match your new password, the system says that the re-entered password does not match the new password [Message ErrorMsgs:NoPwdMatch]:

- Select the Tick option.
(The system displays the Change Password screen.)
- Delete the password that you have entered.
- Re-enter your new password.
- Select the Tick option.
(The system returns to the Desktop.)
- This ends the procedure.

6.5 Forgotten password

If a clerk forgets their password, the post office manager can reset the password (see *Section 7.2.1.3 Modifying a user's password*).

If the post office manager forgets their password they can gain access to the system via the process in *Section 9.3.1 Authorised-user passwords*), and reset the password on their normal user name (see *Section 7.2.1.3 Modifying a user's password*).

6.6 Session mobility

This function allows the ability to log on at another workstation, without having to log out at a previous one. Should the user need to switch workstations for one reason or another, they can simply log on in the normal fashion at another workstation. This will automatically log the user out of the previous workstation in the normal manner. Any activities that are being carried out will appear on the new workstation in the exact same state as on the previous workstation.

Session mobility is not permitted in some contexts; for example, when the system is processing a report or carrying out a critical function such as an AP smart card transaction.

FUJ00088005

6.7 Temporary lock (user-invoked)

The temporary lock function bars access to the system. A user can invoke a temporary session lock at any time by navigating to the Serve Customer menu, selecting the Functions option and then the Temporary Lock option. A user logon screen is displayed saying that the session is currently locked by *nn* (user's name) and that the user's password needs to be entered to unlock the screen [Message NS_TRState_ENG:msgStationLockedBy].

The user can re-activate the workstation as follows:

Step 1. Select the Tick option to accept the user name displayed.

Step 2. Enter the password and select the Tick option.
(The system displays the Transactions, Functions menu.)

SCENARIO A: If the password entered is incorrect, the system says that an invalid name or password had been supplied [Message NS_TRState_ENG:lgnInvalidLogon]:

- Select the Tick option.
(The system re-displays the Username screen.)
- Select the Password field and re-enter the password.
- This ends the procedure.

Note: if another user wishes to over-ride the current user, they may do so in the way described in *Section 6.9 Over-riding the current user*.

6.8 Session inactivity time-out (system-invoked)

A session is timed-out after a period of inactivity (that is, whereby there has been no input from any of the peripherals) of a pre-configured time (see *Section 9.5 Centrally-configurable parameters*). After this time, a user logon screen is displayed saying that the session is currently locked by that user and that the user's password needs to be entered to unlock the screen [Message NS_TRState_ENG:msgStationLockedBy].

The user can re-activate the workstation in the same way as described in *Section 6.7 Temporary lock (user-invoked).* If another user wishes to override the current user, they can do so in the way described in *Section 6.9 Over-riding the current user*.

If the user that is logged on is one who is operating via an authorised-user password (see *Section 9.3.1 Authorised-user passwords*) then, when the procedure in *Section 6.7 Temporary lock (user-invoked)* is followed, step 2 Scenario A will apply. They will need to obtain another authorised-user password, via the process in *Section 9.3.1 Authorised-user passwords*, in order to de-activate the inactivity lock.

FUJ00088005

6.9 Over-riding the current user

The facility to over-ride the current user is available to all types of user. If, whilst the user logon screen is displayed with a message saying that the session is currently locked by user *nn* [Message NS_TRState_ENG:msgStationLockedBy], another user wishes to log on, they can over-ride the current user. To do this they must delete the user name displayed and enter their own user name and password.

The system displays the Logout User screen and a message asking the new user whether they are sure that they wish to log the current user out, and telling them that any outstanding transactions will be committed [Message NS_TRState_ENG:lgnTransMayLost]. If the user selects the Tick option, the system commits any outstanding transactions using cash as the method of payment, logs the current user out and re-displays the initial screen with the Riposte logo in the centre of the screen. The new user must log in again as described in *Section 6.2 Logon*. If the user selects the Cross option, the system re-displays the Username screen with the current user's user name displayed in the username field.

If the current user is logged out, the system does not produce a receipt. When a new user logs on again after over-riding the current user, the Reprint Receipt function can be used to produce a session receipt showing the transactions committed.

6.10 User logged on at a crashed counter

If a counter crashes, the user attached to the counter cannot be attached to a new stock unit as the system believes that the user is still logged on at the crashed counter. If this happens, the user should log on and off at another counter. (The session is lost and any uncommitted transactions will have to be re-entered.)

If the user in question has left the office, their stock unit remains active as they have not logged off. This will inhibit the stock balance of a shared stock unit, and can cause other problems. In this case, the manager should change the user's password and then log on and off as that user.

6.11 Forced logout

If there is a further period of inactivity of a pre-configured time (see *Section 9.5 Centrally-configurable parameters*) after a session has timed-out and the user logon screen has appeared, the system forces a permanent logout. This results in the user being logged out, and the Riposte logo appearing in the centre of the screen.

FUJ00088005

After a forced logout, any customer session currently in progress, including a suspended session, is committed against cash. The system does not produce a receipt. When a user logs on again after a forced logout, the Reprint Receipt function can be used to produce a session receipt showing the transactions committed.

If the session is not a customer session, settlement is against the appropriate settlement product. The system produces a receipt if the session is of the type where an automatic receipt is printed (for example, remittances or transfers).

If the user leaves the Horizon system without completing a transaction, the system will progress through the following sequence of events leading to a forced logout:

- In the period prior to the inactivity timeout being invoked, the screen and system remain active allowing the user to return and progress the transaction in the normal manner.
- In the period after the inactivity timeout has been invoked and prior to the forced logout being invoked, the user will be locked out of the system under the 'Temporary Lock' condition. The user should enter their password to return to the position at which the lock-out occurred and the transaction can be progressed in the normal manner. If the user is subject to a forced password change during this process, the standard procedure should be followed (see *Section 6.4 Enforced change of password facility*) and the new password will then allow access to the transaction.
- Another user can log the original user out of the Temporary Lock at any time (see *Section 6.9 Over-riding the current user*) and the transaction will be completed as 'PAID', that is:
  - An OBCS book receipt, book issue or redirection transaction is completed; and all records for an OBCS encashment for which the value had been entered will show that the customer has received the value of one or more foils.
  - APS and EPOSS transactions will be committed.
- When the pre-configured time for forced logout has elapsed, the user will be forcibly logged out of the system and the transaction will be completed as 'PAID' automatically by the system, that is:
  - An OBCS book receipt, book issue or redirection transaction is completed; and all records for an OBCS encashment for which the value had been entered will show that the customer has received the value of one or more foils.

FUJ00088005

- APS and EPOSS transactions will be committed. The user cannot reverse the committal of the transactions. However, the transactions themselves may be reversed (providing they are defined in reference data as being reversible). See the CSR+ APS PPD [Ref. CS/PRO/091] and the CSR+ EPOSS PPD [Ref.CS/PRO/095] for information on reversing transactions.

6.12 Logout

This function is used to log out a user from a system workstation. The workstation will then be in a ready state for another user to log on or, if at the end of the day, for the daily Horizon system shutdown procedure (see *Section 6.13 Daily Horizon system shutdown)* to take place.

The procedure to log out is as follows:

Step 1. From the Desktop, select the Logout option. The system prompts you to confirm that you want to log out [Message NS_TRState_ENG:IgnLogoutCertainCaption].

Step 2. To confirm the logout, select the Tick option.
(The system displays the initial screen with the Riposte logo in the centre of the screen.)

EXCEPTION A: If you do not want to log out:

- Select the Cross option.
(The system returns to the Desktop.)
- This ends the procedure.

6.13 Daily Horizon system shutdown

At the end of day, after the users have logged out as described in *Section 6.12 Logout,* the Horizon system should be shut down as follows:

Step 1. Press the switch on the monitor to the 'off' position.

Step 2. Press the switch on the counter printer to the 'off' position.

Step 3. If the reports printer is on, press the switch to the 'off' position.

Note: the processor MUST be kept switched on overnight to enable the transfer of data.

FUJ00088005

6.14 Moveable outlets

A moveable outlet is an outlet that has no fixed counter but provides service to customers from largely private dwellings. In such outlets, the Horizon system counter position is provided on a trolley.

The trolley is operated from a location called a point of service and stored in a secure location called a point of storage. The point of service and the point of storage may be at the same or different locations. This affects the operation of the trolley as follows:

- **Single operation location trolley**: Where the points of service and storage are at the same locations, the start-up and shutdown procedures are as for a fixed counter position (see *Sections 6.1 Daily Horizon system start-up,* and *6.13 Daily Horizon system shutdown)*.
- **Dual operation location trolley**: Where the points of service and storage are at different locations, since the trolley has no electrical power supply when being moved between them, the user has to shut down the Horizon System and power off the equipment as described in *Sections 6.14.1 Moving a trolley from its point of service to its point of storage* and *6.14.2 Moving a trolley from its point of storage to its point of service* below. It should be powered on at all other times.

Business rule:

- To ensure that the end-of-day activities take place correctly, the trolley's communications cable must be connected by 19:00. This can be at either the point of service or the point of storage.

  Note: If there is a need to move the trolley between 19:00 and 20:00, this must be done as swiftly as possible.

6.14.1 Moving a trolley from its point of service to its point of storage

The procedure to move a dual operation location trolley from its point of service to its point of storage is as follows:

Step 1. Shut down and switch off the workstation's processor as described in *Section 6.15 Shutting down a processor*.

Step 2. Switch off the office printer, counter printer and monitor.

Step 3. Switch off the power outlet.

Step 4. Disconnect the trolley from its power and communications points.

Step 5. Park the power and communications cables in their docking point on the trolley.

Step 6. Release the trolley's brakes.

FUJ00088005

6.14.1 Moving a trolley from its point of service to its point of storage (contd)

Step 7. Move the trolley to its point of storage.

Step 8. Apply the trolley's brakes.

Step 9. Take the power and communications cables from their docking point.

Step 10. Connect the trolley to its power and communications points.

Step 11. Switch on the power outlet.

Step 12. Switch on the monitor and processor.

Step 13. Perform the restart procedure (see *Section 4.2.2 Regaining access to a switched-off Gateway workstation*), omitting step 16 (logging on).

Step 14. Switch off the monitor.

6.14.2 Moving a trolley from its point of storage to its point of service

The procedure to move a dual operation location trolley from its point of storage to its point of service, is as follows:

Step 1. Switch on the monitor.

Step 2. Shut down and switch off the workstation's processor as described in *Section 6.15 Shutting down a processor,* starting at step 2.

Step 3. Switch off the monitor.

Step 4. Switch off the power outlet.

Step 5. Disconnect the trolley from its power and communications points.

Step 6. Park the power and communications cables in their docking point on the trolley.

Step 7. Release the trolley's brakes.

Step 8. Move the trolley to its point of service.

Step 9. Apply the trolley's brakes.

Step 10. Take the power and communications cables from their docking point.

Step 11. Connect the trolley to its power and communications points.

Step 12. Switch on the power outlet.

Step 13. Switch on the monitor, processor, counter printer and office printer.

FUJ00088005

Step 14. Perform the restart procedure (see *Section 4.2.2 Regaining access to a switched-off Gateway workstation*).

FUJ00088005

6.15 Shutting down a processor

This procedure is performed in circumstances where a workstation's processor needs to be switched off (that is, before moving a trolley or in order to perform the lost PIN/PMMC or change PIN procedures) or under instruction from the Horizon System Helpdesk.

Step 1. Log out as described in *Section 6.12 Logout*.
(The system displays the initial screen with the Riposte logo in the centre of the screen.)

Step 2. Touch the screen or press any key.
(The system displays the agreement screen [Message DesktopInfo:LogonAcknowledgement].

Step 3. Select the Tick option.
(The system displays the Logon screen.)

Step 4. From the Logon screen, select the Off option. The system asks you whether you want to shut down or restart the computer [Message Access control and user administration hard message: workstation processor shutdown].

Step 5. To shut down the computer, select the Shutdown option. The system prompts you to confirm the shutdown [Message Access control and user administration hard message: Confirm Shutdown].

EXCEPTION A: If you want to restart the computer:

- Select the Restart option. The system prompts you to confirm the restart [Message Access control and user administration hard message: Confirm Restart].

SCENARIO A.1: To confirm the restart:

- Select the Tick option.
- The system returns to the Riposte screen.
- This ends the procedure.

SCENARIO A.2: To cancel the restart:

- Select the Cross option.
- The system returns to the Logon screen.
- This ends the procedure.

FUJ00088005

6.15 Shutting down a processor (contd)

Step 6 To confirm the shutdown, select the Tick option.

EXCEPTION A: If you do not want to shut down:

- Select the Cross option.
- The system returns to the Logon screen.
- This ends the procedure.

Step 7. When the message saying 'it's now safe to turn off your computer' is displayed, switch off the processor.

FUJ00088005

7 User administration

User administration consists of maintaining the identities of users on the system. A user identity consists of a user name, full name, password and group as follows:

- User name: This consists of six specific characters as defined in *Section 9.1 User names*.
- Full name: This consists of two fields, the user's first and last name. Standards for full names are described in *Section 9.2 Full names.*
- Password: This is specified by the user and prevents unauthorised access. Standards for passwords are described in *Section 9.3 Passwords*.
- Group: This determines the functions available to the user according to their role. Further information on groups is given in *Section 9.4 Groups.*

Business rule:

- An additional component of a user identity, called a Teller Id, is not used.

System rule:

- Only users with manager access rights are allowed to add, modify and delete users.

The following processes and procedures are described:

- Adding a user
- Modifying a user
- Deleting a user

A report function is available that lists all the users associated with the post office, together with their groups (see *Section 8.1 User Summary report*).

(To review the other components of a user identity, the user name can be identified as described in *Section 8.1.1 Printing a User Summary report* and then viewed using the Modify User function.)

7.1 Adding a user

A user needs to be added to the system in order to access system functions.

System rules:

- If a new user is being added, and has the same user name as a current user or a previously-added user, the system advises that it is unable to add that user.

FUJ00088005

7.1.1 Adding a user: procedure

The procedure to add a user is as follows:

Step 1. From the Desktop, select the Administration option, the User option, then the Add User option.
(The system displays the Add User screen.)

Step 2. Enter the user name for the user and select the Tick option. For details of the standards for user names, see *Section 9.1 User names*.

Step 3. Enter the password allocated to the user and select the Tick option. For details of the standards for passwords, see *Section 9.3 Passwords*.

Step 4. Re-enter the password and select the Tick option.

EXCEPTION A: If, when re-entering the password, you enter a password that does not match the password previously entered, the system says that the password and confirmed password do not match [Message ErrorMsgs:NoPwdMatch]:

- Select the Tick option.
- (The system re-displays the Confirm Password screen.)
- Re-enter the user's password.
- Select the Tick option.
- Proceed to step 5.

Step 5. Enter the first name of the user and select the Tick option. For details of the standards for full names, see *Section 9.2 Full names*.

Step 6. Enter the last name of the user and select the Tick option. For details of the standards for full names, see *Section 9.2 Full names.*

Step 7. The Initial Group screen is displayed. Select the relevant group for the user, then select OK. For information about groups, see *Section 9.4 Groups*.

Step 8. The system tells you that the user was successfully created [Message NS_UserMaintenance_ENG:umUserAddedCaption]. Select the Tick option.

Step 9. The system returns to the Modify User screen. Check the entered user information on the displayed details cards.

Step 10. To end the action, select the Desktop button. The system returns to the Desktop.

Step 11. Print a User History report as described in *Section 8.2.1 Printing a User History report*. Check that the user has been set up as required then destroy the report.

FUJ00088005

7.1.1 Adding a user: procedure (contd)

Step 12. Is the user available?

SCENARIO A: If the user is available:

- Give the new user their password and advise them that they will be prompted to change it the first time that they log on to the system.

SCENARIO B: If the user is not available:

- Write down the password, seal it in an envelope and store it in a secure location.

7.2 Modifying a user

This allows the following functions to be carried out from a common starting procedure:

- Modify a user's group.
- Modify a user's options.
- Modify a user's password.

Business rule:

- The system displays two additional functions, to modify a user's full name and to modify a user's Teller Id, but these must not be used.

7.2.1 Modifying a user: procedure

The procedure to modify a user is as follows:

Step 1. From the Desktop, select the Administration option, the User option, then the Modify User option.
(The system displays the User name selection screen listing all users on the system.)

Step 2. Locate the user you want to modify.
(If you cannot see the user you require, scroll through the list of user names until their name is displayed.)

Step 3. Select the name of the user whose details you wish to modify.

Step 4. The system displays the Modify User screen.
(The current settings are displayed on the details cards on the left hand side of the screen. Select tab 2 to view the group to which the user belongs.)

FUJ00088005

7.2.1 Modifying a user: procedure (contd)

SCENARIO A: If the wrong user has been selected:

- Select the Previous option.
  (The system displays the Administration User menu.)
- Select the Modify User option.
- Proceed to step 3.

Step 5. Modify the required details:

- To modify a user's group see *Section 7.2.1.1 Modifying a user's group*.
- To modify a user's options see *Section 7.2.1.2 Modifying a user's options*.
- To modify a user's password see *Section 7.2.1.3 Modifying a user's password*.

Step 6. The system displays a message to say that the user's details were successfully changed [Message NS_UserMaintenance_ENG: umUserGroupMessage, UmUserOptionsMessage or umUserChangedPasswordMessage]. Select the Tick option. The system returns to the Modify User screen.

Step 7. Proceed as follows:

SCENARIO A: To make further modifications:

- Proceed to step 5.

SCENARIO B: To end the modification of users:

- Select the Desktop button. The system returns to the Desktop.
- Proceed to step 8.

Step 8. Print a User History report as described in *Section 8.2.1 Printing a User History report*. Check that the user has been modified as required then destroy the report.

7.2.1.1 Modifying a user's group

The procedure to modify a user's group is as follows:

Step 1. From the Modify User screen (see *Section 7.2.1 Modifying a user: procedure*), select the Groups option. The system displays the Groups for User screen.

FUJ00088005

7.2.1.1 Modifying a user's group (contd)

Step 2. Deselect the unwanted group and select the relevant group to which the user is to belong (when a group is selected, it is highlighted). For information about groups, see *Section 9.4 Groups*.

Step 3. Select the Tick option and proceed to step 6 of *Section 7.2.1 Modifying a user: procedure*.

7.2.1.2 Modifying a user's options

The procedure to modify a user's options is as follows:

Step 1. From the Modify User screen (see *Section 7.2.1 Modifying a user: procedure*), select the Options option.
(The system displays the Options for User screen.)

Step 2. Select the relevant option (once selected, the option is highlighted):

- 'Must Change Password'

  Select this option if the user is to be prompted by the system to change their password at their next logon. (Note that this selection can be undone if it has been selected through the Modify User procedure but not if it has been automatically triggered through password expiry.)

- 'Password Never Expires'

  This option must not be used unless the user has been instructed to do so. If the option is selected, the password for the selected user never expires. This option cannot be selected if the Must Change Password option is selected.

- 'Account is disabled'

  Select this option if the user name and password are not to be used temporarily but it is unnecessary to delete them. The disablement takes effect the next time the user attempts to log on. If the user is already logged on, the disablement takes effect the next time the user returns to a menu. Account disablement prevents further entry into application software but allows existing open sessions to be finished.

- 'Account is locked out'

  Deselect this option if a locked user account is to be unlocked.

Step 3. Select the Tick option and proceed to step 6 of *Section 7.2.1 Modifying a user: procedure*.

FUJ00088005

7.2.1.3 Modifying a user's password

The procedure to modify a user's password is as follows:

Step 1. From the Modify User screen (see *Section 7.2.1 Modifying a user: procedure*), select the Password option.
(The system displays the New Password screen.)

Step 2. Enter the new password and select the Tick option. For details of the standards for passwords, see *Section 9.3 Passwords*.

Step 3. Re-enter the new password and select the Tick option.

EXCEPTION A: If, when re-entering the new password, you enter a password that does not match the user's new password, the system says that the password and confirmed password do not match:

- Select the Tick option.
(The system re-displays the Confirm Password screen.)
- Delete the password that you have entered.
- Re-enter the user's new password.
- Select the Tick option.
- Proceed to step 4.

Step 4. Proceed to step 6 of *Section 7.2.1 Modifying a user: procedure*.

7.3 Deleting a user

This function allows the details of a user to be deleted from the system. A user would be deleted from the system when, for example, the user has permanently left the office.

System rules:

- Deletion does not delete the user but marks the user as 'deleted' on the system, which is why the same user name cannot be used again. If a deleted user returns to the post office they must be given a different user name.
- A user who is attached to a stock unit other than the default stock unit cannot be deleted.
- The preset user names (other than ZSET01) cannot be deleted.

Note: a user's account can be disabled if the user name and password are not to be used temporarily but it is unnecessary to delete them (see *Section 7.2.1.2 Modifying a user's options*).

FUJ00088005

7.1.1 Deleting a user: procedure

The procedure to delete a user is as follows:

Step 1. From the Desktop, select the Administration option, the User option, then the Delete User option.
(The system displays the User selection screen.)

Step 2. Select the user name of the user that is to be deleted.
(The system asks you to confirm the deletion [Message NS_UserMaintenance_ENG:umAskDeleteUser].)

SCENARIO A: If you cannot see the user you require:

- Scroll through the list of user names until the relevant name is displayed.
- Proceed to step 3.

EXCEPTION A: If the user you select is attached to a stock unit that is not the default stock unit, the system tells you that you need to detach the user from the stock unit before deleting [Message Access control and user administration hard message:Delete attached user]:

- Select the Tick option. The system returns to the Desktop.
- Attach the user to the default stock unit (see the CSR+ EPOSS PPD [Ref. CS/PRO/095]) and then retry the procedure.

Step 3. To confirm the deletion, select the Tick option.
(The system marks the user as 'deleted'.)

EXCEPTION A: If you want to cancel the deletion:

- Select the Cross option. The system cancels the deletion and returns to the Desktop.

Step 4. The system displays a message to say that the user was successfully deleted [Message NS_UserMaintenance_ENG:umUserDeletedMessage]. Select the Tick option.
(The system returns to the Desktop.)

FUJ00088005

8 User reports

This section describes the following counter printer reports:

- User Summary
- User History
- User Events

8.1 User Summary report

The User Summary lists all users in a post office current to the system, and shows their group allocations. This includes deleted users.

8.1.1 Printing a User Summary report

The procedure to print the User Summary is as follows:

Step 1. From the Desktop, select the Reports option, the Event Log option, then the User Summary option.

Step 2. The system prints the User Summary report on the counter printer's tally roll and returns to the Desktop.

8.2 User History report

The User History report lists all user amendment events for the period and user name specified. These amendments include creation date, password setting/changes, group allocations, account disablements and deletions.

8.2.1 Printing a User History report

The procedure to print the User History report is as follows:

Step 1. From the Desktop, select the Reports option, the Event Log option, then the User History option.

Step 2. The system displays the User Report screen with the defaults of today's start date and your user name.

Step 3. Select the Tick option.

EXCEPTION A: If any day other then 'Today' is required:

- Select the Cross option.
- Enter the required start date of report and select the Tick option.

FUJ00088005

8.2.1 Printing a User History report (contd)

Step 4. Select the Tick option.

EXCEPTION A: If the displayed user name is not the one required:

- Use the BACKSPACE key to clear the user name.
- Enter the required user name, or leave blank to print a report for all users, and select the Tick option.

Step 5. The system prints the User History report on the counter printer's tally roll and returns to the Desktop.

8.3 User Events report

The User Events report lists all logon/logout events performed on the system for the period and user name specified. The report includes the date and times of logons, logouts, logon failures etc.

8.1.1 Printing a User Events report

The procedure to print the User Events report is as follows:

Step 1. From the Desktop, select the Reports option, the Event Log option, then the User Events option.

Step 2. The system displays the User Report screen with the defaults of today's start date and your user name.

Step 3. Select the Tick option.

EXCEPTION A: If any day other then 'Today' is required:

- Select the Cross option.
- Enter the required start date of report and select the Tick option.

Step 4. Select the Tick option.

EXCEPTION A: If the displayed user name is not the one required:

- Use the BACKSPACE key to clear the user name.
- Enter the required user name, or leave blank to print a report for all users, and select the Tick option.

Step 5. The system prints the User Events report on the counter printer's tally roll and returns to the Desktop.

FUJ00088005

9 Data input rules

This section gives the standards to which user names, full names and passwords must conform and describes the way in which groups allow access to the system.

9.1 User names

User names must conform to the following standards:

- System rules:
  - Each user name must be unique within a post office. This relates to all users added to the system, including any subsequently deleted.
  - A user name cannot contain spaces or more than two successive duplicate characters.
  - A user name must be six characters long.
- Business rules:
  - A user's user name consists of six characters in the following format: first initial, first two letters of the user's surname, three numeric characters (always 001 unless there is more then one occurrence of the user name). For example, the first Elvis Presley to be described to the system within a post office would have the user name EPR001. Ella Presley, or a second Elvis Presley, would appear as EPR002.

    If using the user's first initial and the first two letters of the user's surname gives more than two successive duplicate characters, the third duplicate character (second from the surname) should be omitted and the third character from the surname should be used instead. For example, Linda Llewellyn would appear as LLE001.

    If the next numeric character in the current sequence leads to three repeated characters, the third duplicate character should be omitted and the next number in the sequence used instead. For example, the number 111 would be omitted and the number 112 used instead.

Notes**:**

- The user name uniquely identifies the user to the system, and must be used every time the user logs on.
- It is solely for the designated person's use; users must NOT allow others to use it.
- Users must not use, or attempt to use any user name that has not been explicitly issued to themselves.

FUJ00088005

9.2 Full names

Full names must conform to the following standards:

- System rules:
  - At least one character must be entered in each of the fields.
  - The system does not allow the entry of more than one first name.
  - No spaces can be committed to the first name field.
  - The maximum number of characters that can be entered is 16. This is character dependent - wider characters (W for example) will take up more space, narrower characters (I for example) will take up less space.
- Business rules:
  - If a name is too long to fit in the displayed box, it should be truncated when it reaches the end point.
  - The names cannot be changed after the user has been set up.

9.3 Passwords

Passwords for users must conform to the following standards:

- System rules:
  - A password cannot be the same as the user name.
  - Passwords must not use the words detailed in a list of excluded words defined by POCL Product Management. This list contains obvious words such as PASSWORD and SECRET, and names.
  - A password cannot contain spaces or more than two successive duplicate characters.
  - A password must be at least 6 characters and no more than 14 characters.
  - A password must be changed immediately if it has been allocated by someone else, i.e. when the user is first introduced to the system, the password is modified or when 'Must Change Password' is set on.
  - A user cannot change their password more than once within a pre-configured duration (see *Section 9.5 Centrally-configurable parameters*).
  - Passwords will expire according to a pre-configured duration (see *Section 9.5 Centrally-configurable parameters*).

FUJ00088005

- Passwords can only be reused after a pre-configured number of password changes have elapsed (see *Section 9.5 Centrally-configurable parameters*).

- Business rules:
  - A password must contain letters and numbers, at least one of each.
  - A user's initial password is to be known only by the person creating the user and the new user. Subsequent passwords must be known only the user and must not be revealed to anybody else.

Generally users must:

- Ensure their password is private, user selected, and not revealed to anyone.
- Not write down their password.
- Change their password immediately if they believe it may be known to someone else.
- Ensure they are not observed when entering or changing their password.

Notes:

- For security, passwords are not displayed on the screen; instead each character of the password is shown as an 'X' as described in the CSR+ Operating Environment PPD [Ref. CS/PRO/0097].
- For a long password, more characters can be entered when the alphanumeric screenpad is used. However, if more characters are entered than will fit in the input field when using the keyboard, this will constrain the user to always use the alphanumeric screenpad when logging on.
- No one should ask a user for their password, not even the Horizon System Helpdesk. Any such request for information should be reported to the normal Post Office Counters Ltd security channels.

9.3.1 Authorised-user passwords

An authorised-user password is granted to verified users and allows access to the system for one session only.

The procedure to obtain an authorised-user password is detailed in the POCL 'Authorised-user Password Procedure' which describes how the user obtains authorisation from the Network Business Support Centre and how the Horizon System Helpdesk and the user interact [HSH call SEC003].

Authorised-user passwords are not linked to groups but to user names. The user names to which authorised-user passwords apply are shown in *Section 9.4.1 User names and passwords for groups*.

FUJ00088005

9.4 Groups

The rules that apply to groups are given below. Details of the user names and passwords assigned to groups are given in the following subsections.

Rules that are not enforced by the system:

- A user should be a member of not more than or less than one group.

System rules:

- A user can be a member of one or more than one group. The functions available on the menus are determined by the access rights available to the group(s) selected. The functions available to the highest level group selected will be available to the user, plus any other functions which are otherwise specific to any other particular group that is also selected.
- The system supports the following groups:
    - ENGINEER: This group will not affect counter operations; it has only diagnostic capability.
    - AUDITOR: This group has access to limited functionality which supports the auditing process.
    - AUDITOR E: This group has full manager rights plus access to final accounting facilities, and is only required in emergency situations, should another employee need to take over the post office.
    - SUPPORT: This group has only administrative functionality to create users, for instance a new manager. It is used if the manager forgets their password.
    - MANAGERS: This group allows all access to all functions. User administration is restricted to this group.
    - SUPERVISORS: This group has access to all counter and some administrative functionality.
    - CLERK: This group has access to all the counter functionality.
    - SETUP: This group operates only on initialisation of the system. The only rights this group has are administrative ones in order to create a manager user. Once this has been completed, the group must be deleted.
- Groups not appropriate to outlet users (ENGINEER, AUDITOR, AUDITOR E, SUPPORT and SETUP) cannot be allocated to new or existing users. These groups can only be assigned by the system start-up process for agreed user names.

FUJ00088005

9.4.1 User names and passwords for groups

Groups are assigned the following user names and passwords:

Group	User name	Password type
ENGINEER	'ENGR01'	Authorised-user
AUDITOR	'ZAUD01' to 'ZAUD20'	Authorised-user
AUDITOR E	'ZAUD99'	Authorised-user
SUPPORT	'ZSUP01'	Authorised-user
MANAGERS	Standard (see *Section 9.1 User names*)	Standard (see *Section 9.3 Passwords)*
SUPERVISORS	Standard (see *Section 9.1 User names*)	Standard (see *Section 9.3 Passwords)*
CLERK	Standard (see *Section 9.1 User names*)	Standard (see *Section 9.3 Passwords)*
SETUP	'ZSET01'	'FIRST1'
MIGRATION	'MIGR01'	Standard (see *Section 9.3 Passwords)*

9.4.2 Access rights

Access to menus in the menu hierarchy depends upon the user's group. For information on the sets of menus to which different groups have access, refer to the Horizon OPS Menu Hierarchy: Release 2 [Ref. SD/SPE/016].

9.5 Centrally-configurable parameters

The following parameters are configured centrally:

- Maximum number of logon attempts allowed before the user account is locked.
- Period (number of minutes) that the user account remains locked if the number of logon attempts is exceeded.
- Password expiry period (number of days).
- Number of password changes before a password can be re-used.
- Period (number of days) that must elapse before a user changes their password again.
- Session inactivity time-out period (number of minutes).
- Forced logout after time-out (number of minutes).
- Forced logout after temporary lock (number of minutes).

FUJ00088005

10 Security guidelines

The following security guidelines should be followed:

- Any misuse of the system could lead to an offence under the Computer Misuse and/or Data Protection Acts.
- Users are accountable for any actions undertaken with their user name and password.
- Users are responsible for ensuring that their password is kept private and not revealed to anybody else.
- Redundant users must be deleted from the system.
- Any breach of security into the Horizon system should be reported to the Horizon System Helpdesk [HSH call SEC007].
- All existing security checks must still be applied (the system does not do away with the need for vigilance).
- Features of the system, especially security, must be treated as business sensitive information, and not discussed outside the workplace.
- Screens should not be placed so that they can be seen by customers.
- Users must invoke the temporary lock or log out from the system if the workstation is out of their sight, or if they are not going to use it immediately.

11 Fallback procedures

The following types of equipment failure will affect administrative activities:

- If the counter printer fails:
  - A Post Office Logon PIN can be noted on paper (see *Section 4.7.1 Counter printer failure*).
  - Reports can be printed when the service is resumed or, for a multi-counter office, at another counter position.
- If the monitor or PC fails, no administrative activities will be possible until the service is resumed in a single-counter office. For a multi-counter office, another counter position can be used.
- If the monitor fails, the keyboard is still active. Touching keys on the keyboard may result in undesired activities taking place.

For the fallback procedure for keyboard or touch screen failure, see the CSR+ Operating Environment PPD [Ref. CS/PRO/097].