FUJ00152232

Document Title:	AUDIT DATA EXTRACTION PROCESS
Document Reference:	SVM/SEC/PRO/0018
Document Type:	Process
Release:	Not applicable
Abstract:	This document establishes the process undertaken by the Post Office Account Security Litigation Support team to provide audit data for despatch to authorised requesters
Document Status:	APPROVED
Author & Dept:	Farzin Denbali
External Distribution:	Post Office Intel team
Security Risk Assessment Confirmed	Yes

Approval Authorities:

Name	Role	Signature	Date
Jason Muir	POA OSM	See Dimensions for record	

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

FUJ00152232

0 Document Control

0.1 Table of Contents

FUJ00152232

0.2 Document History

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
0.1	27-Oct-2009	Initial Draft	
0.2	25-Aug-2010	For Review	
0.3	13-SEP-2010	Revised in response to comments	
1.0	01-Mar-2011	Approval version	
1.1	14 Feb 12	For Review	
2.0	23-Apr-2012	Approval version. Includes additional section on Unauthorised Requests inserted following review.	
2.1	03 Sep 2014	Annual review, name changes only.	
3.1	01-Dec-2016	Annual Review and minor updates to names and processes	
4.0	02-Dec-2016	Approval version	

0.3 Review Details

*See HNG-X Reviewers/Approvers Matrix (PGM/DCM/ION/0001) for guidance on completing the lists below. You may include additional reviewers if necessary, but you should generally **not exclude** any of the mandatory reviewers shown in the matrix for the document type you are authoring.*

Review Comments by :	
Review Comments to :	Jason.muir GRO POADocumentManagement GRO
Mandatory Review	
Role	Name
Security Analyst/Crypto Key Manager	Andy Dunks
Security Analyst	Farzin Denbali
Security Analyst	Dharmesh Mistry
CISO	Steve Godfrey
POA Quality Manager	Bill Membery
Optional Review	
Role	Name
Issued for Information – Please restrict this distribution list to a minimum	
Position/Role	Name

(*) = Reviewers that returned comments

0.4 Associated Documents (Internal & External)

Reference	Version	Date	Title	Source
PGM/DCM/TEM/0001 (DO NOT REMOVE)			POA HNG-X Generic Document Template	Dimensions

FUJ00152232

DEV/GEN/MAN/0015			Audit Extraction Client User Manual	Dimensions
SVM/SDM/SD/0017			Service Description for the Security Management Service	Dimensions
			EMEIA Security Policy Manual	Dimensions
SVM/SEC/PRO/0017			Management of the Litigation Support Service	Dimensions
CR/FSP/006			Audit Trail Functional Specification	Dimensions
DEV/APP/SPG/0020			HNG-X Audit Server Support Guide	Dimensions
DEV/APP/SPG/0016			Audit Extraction Client Support Guide	Dimensions

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

0.5 Abbreviations

Abbreviation	Definition
ARQ	An Audit Record Query that is not a Banking Transaction Record Query and which relates to Transactions
AUW	Audit Workstation
BQ	Banking Record Query
CS	Customer Services
POL	Post Office Limited
POLIA	Post Office Limited Internal Audit
POA	Post Office Account

0.6 Glossary

Term	Definition
Audit Record Query (ARQ)	An Audit Record Query that is not a Banking Transaction Record Query and which relates to Transactions.
Audit Record Query Form	The form used by POL to request detailed transaction data.
Banking Record Query	A Record query in respect of a Banking Transaction which the Data Reconciliation Service has reconciled or has reported as an exception, the result or records of which are subsequently queried or disputed by Post Office Ltd or a third party.
Branch Code	A Post Office outlet unique identifier
Prosecution	Civil or criminal court or statutory tribunal proceedings related to transactions or fraudulent actions conducted at a Post Office Outlet

0.7 Changes Expected

Changes
None.

0.8 Accuracy

FUJ00152232

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 as a result of any error or omission in the same.

0.9 Security Risk Assessment

Security risks have been assessed and it is considered that there are no security risks relating specifically to this document.

FUJ00152232

1 Introduction

The Horizon and Horizon Online system generates transaction data that is of interest to Post Office Ltd, and other groups such as the Police and Courts. Subject to certain constraints, the audit data must be made available to Post Office or other authorised groups within timescales established in the Service Description for the Security Management Service, SVM/SDM/SD/0017.

This document establishes the process for requesting audit data extractions and subsequent activities undertaken to provide to authorised requesters.

This document is without prejudice to any of the parties and nothing contained herein shall be deemed or construed as affecting contractual obligations or creating new contractual obligations between any of the parties.

2 Scope

If future releases of Horizon Online introduce changes to the way that data is requested or extracted this process will be updated to reflect those changes.

This process applies to all audit data extraction requests, namely:

- Audit Record Queries (ARQs)
- Banking Record Queries (BQs)
- Internal Fujitsu requests

3 Audit Data

3.1 Audit Data Integrity

The integrity of audit data must be guaranteed at all times from its origination, storage and retrieval to subsequent despatch to the requester. Controls have been established to provide assurances to Post Office that this integrity is maintained.

During audit data extractions the following controls apply:

- Extractions can only be made via dedicated Audit Workstations (AUWs) which exist at Bracknell and Stevenage. The AUWs are subject to rigorous physical security controls, located in secure rooms, in secure areas, subject to proximity pass access within a secured Fujitsu (UK & Ireland) site.
- Logical access to the AUWs and their functionality is controlled by dedicated logins, 2-factor authentication password control and is in accordance with the POA Security Service Description SVM/SDM/SD/0017 and EMEIA Security Policy Manual.
- All extractions are logged on the Audit System and supported by documented ARQs, BQs or internal requests, all authorised by nominated persons within POL and Fujitsu. This log can be scrutinised on the AUWs.
- Extractions will only be undertaken by individuals previously notified to Post Office. Currently this is limited to the Post Office Account Security team, and the Post Office Account Audit Development personnel. Any additions will be notified to Post Office in advance.
- Checksum seals are calculated for audit data files when they are written to audit archive and re-calculated when the files are retrieved. The result is maintained in a check seal table.
- Windows events generated by the counters within the branch/timeframe in question are checked to ensure the counters were functioning correctly

FUJ00152232

- Agreement has been reached with Post Office regarding their rights to witness extractions without warning or to request repeat extractions that they can witness.

3.2 Archive Requirements and Support

Historic Horizon and Horizon Online transaction data is held securely on the Audit Servers in accordance with CR/FSP/006, Audit Trail Functional Specification. Audit data is archived in accordance with HNG-X Audit Server Support Guide, DEV/APP/SPG/0020 and the audit extraction client is supported in accordance with DEV/APP/SPG/0016, Audit Extraction Client Support Guide.

3.3 Retrieval of Audit Data

Archive audit data is retrieved in accordance with instructions contained in Audit Extraction Client User Manual, DEV/GEN/MAN/0015.

3.4 Audit System Audit Trail

The audit trail records the date and time of each audit request process carried out on the Horizon Audit System. The search criteria and request identifier shall be used to create the directory structure of each audit trail. An audit trail is produced only when an audit request is marked as completed on the Extractor Client. (The audit trail is not the Prosecution Support Database).

The Prosecution Support Databases hold information relating to when an ARQ, BQ or internal PEAK was received, the SLA return date (if appropriate), who completed and checked the return.

3.5 Retention of Retrieved Audit Data

Retrieved data is backed up to an external NAS drive which is located secured in the secure room on 4th floor in BRA01.

4 Authorised Requests for Audit Data

4.1 Audit Record Query

An ARQ is a request to the Post Office Account (POA) for transaction data required to support a POL investigation or litigation activity. The transaction data provided is held on the Audit Archive. The request is received from the POL Casework Manager, or his nominated representative, and/or the POL Intel team, and contains specific search criteria. The stipulated criteria and the format of the returned data are as referenced in the document Security Management Service - Service Description, SVM/SDM/SD/0017.

The agreed annual quotas and return timeframes for ARQ requests are as referenced in the document Security Management Service - Service Description, SVM/SDM/SD/0017.

4.1.1 Specific Audit Record Query Request Detail

When creating a new request for a formal ARQ on the Audit Extraction Client the 'requester' selected is 'POLIA'. This identifies the retrieval as a formal ARQ request from POL Casework Team.

4.2 Banking Record Queries (BQs)

A BQ is a request to POA for confirmation of transaction detail due to a query or dispute by POL or a third party. Requests are only received from nominated representatives of Product & Branch Accounting, Banking & Financial Services or Revenue Protection Departments.

Requests are received via e-mail.

The agreed annual quotas and return timeframes for BQ requests are as referenced in the document Security Management Service - Service Description, SVM/SDM/SD/0017.

4.2.1 Specific BQ Request Detail

FUJ00152232

When creating a new request for a BQ on the Audit Extraction Client the 'requester' selected is 'POCL Other'. This identifies the retrieval as a formal BQ request from POL Financial Departments. The stipulated criteria and the format of the returned data are as referenced in the document Security Management Service - Service Description, SVM/SDM/SD/0017.

4.3 Internal (Fujitsu) Requests for Audit Data

Other internal agencies may require copies of historic records which are held only on the Audit Archive. Requests are made via the internal PEAK system. The specific details required include outlet, branch code, timeframe, output file, etc.

4.3.1 Specific Internal (Fujitsu) Request Detail

When creating a new request for an Internal (Fujitsu) request on the Audit Extraction Client the 'requester' selected is 'Pathway SSC'. This identifies the retrieval as a formal Internal (Fujitsu) request.

4.4 Unauthorised Requests

In the event that direct contact is made with the Litigation Service from an external party, including, but not limited to, the Police, Solicitors or Defence Teams, for audit data records they shall be referred to the Post Office Limited Fraud Team at Salford or the Intel team in Chesterfield. No data will be supplied to 3rd parties without explicit written authorisation to do so from Post Office. If/when data is supplied it will be done so in a secure manner.

4.5 Finalising and Returning the Audit Data

4.5.1 Encryption of Data

It is a mandatory requirement that all sensitive data communicated either by disc or e-mail is to be encrypted. The PGP SDA Encryption tool has been selected for this use. The sender uses the functionality of PGP encryption, producing an sda.exe file, which requires only the password for access and decryption by the recipient. The recipient does not need PGP functionality.

See separate process, attached.

PGP SDA Encryption Process.doc

4.5.2 Returning ARQ Requests

ARQ requests are burnt to CD and the CD prevented from accepting further files or records. The CD is labelled and the relevant detail relating to the original request is written on it. The transaction data on the CD is checked by another member of the team to ensure completeness of the return. The CD is also checked for viruses before being sent via Royal Mail's Special Delivery Service to the notified contact as detailed in SVM/SEC/PRO/0017.

Alternatively and when requested the PGP encrypted data will be supplied to Post Office via a secure Post Office owned web based tool called Quatrix.

4.5.3 Returning BQ Requests

BQ requests are checked by another member of the team to ensure completeness of the return. The response is then returned via e-mail to approved contacts.

4.5.4 Returning Internal (Fujitsu) Requests

Files/records are returned to the requestor via the internal PEAK system.

FUJ00152232

4.6 Retention of Records

Detailed records are maintained on the Prosecution Support Databases relating to when an ARQ, BQ or internal PEAK was received, the SLA return date (if appropriate), who completed and checked the return, and when and how it was returned.