POL00105222

Security Investigations Data Handling Process

(Fujitsu Horizon Data Request)

Document Control

1 Overview

Owner:	Head Of Security	**Enquiry point:**	Head of Security
Version:	1.0	**Effective from:**	20 September 2013
Last updated:	20/09/2013	**Last review date:**	20/09/2013
Review Period	Annually or major change	**Reviewers**	Information Securityand Assurance Group
Compliance	Mandatory for Security Investigators and Case Workers staff	**Distribution**	Via Post Office National Security team

2 Revision History

Version	Date	Author	Changes
0.1	17/09/2013	Moyn Uddin	Initial Draft
0.2	19/09/2013	Moyn Uddin	Final draft and consolidation after end to end review with SIMS and CWT.
1.0	20/09/2013	Moyn Uddin	Final version after full review with SIMs/CWT and ISAG.

POL00105222

Process

When information from Horizon is required for supporting conduct of criminal investigations and prosecutions as per Post Office Conduct of Criminal Investigations Policy:

1. A request for information from Fujitsu is sent to the Case Work Team. The request is emailed to the Post Office Security email inbox (Case Work Team's email) by the Security Investigation Manager (SIM) from a Post Office email address.

   Note: The request is contained in an MS Word document, which is password protected.

2. The password is emailed to the Case Work Team in a separate email via internal Post Office email into the Post Office Security email inbox (Case Work Team's email box).

3. This email is stored in Fraud – ARQ / APOP / Statements folder, an access controlled area reserved for Case Work Team members only (currently only two people).

4. On receipt of an emailed request for credit card information from the SIM (investigators are known to the Case Work team), the Case Work team fills in an ARQ request form and attaches it to an email (from Case Work Team's email) requesting Fujitsu Horizon data (to email address cspoa.security GRO). The form is password protected using pre shared password. This document is classified STRICTLY CONFIDENTIAL.

   Note: A blank ARQ request form is held in the team drive – Security Risk Team / Fraud / Blank ARQ form V.6. Completed ARQ forms sent to Fujitsu are saved in the same location with the next ARQ number in the team drive ARQ folder. Still password protected.

5. Case Work team record details of the received request onto the ARQ database spread sheet which is in Team drive – Security Risk Team/ Fraud/ ARQ database V.1

   Note: Access to the spread sheet is controlled and available only to people in the Case Work team (2 people at the moment) No passwords are stored. (Disable Macros when opening).

6. All requests are validated and authorised by the team manager before request is sent to Fujitsu.

7. The requested data is received from Fujitsu by Case Work team via a PGP (Self-Decrypting Archive) encrypted CD ROM, using pre-shared password). The CD is sent by Special Delivery (tracking) in a padded non-marked envelope. The CD is labelled STRICTLY CONFIDENTIAL.

   Note: Separate channels are maintained. Password is never sent with the encrypted CD.
   Case workers do not open or copy the CD.

8. The encrypted CD is posted on to the SIM that made the request in Step 1 by tracked Royal Mail Special Delivery.

9. The password to decrypt the CD is emailed to the SIM's Post Office email address.

   Note: CDs are despatched to the SIM on the same day and therefore are not stored locally. Until despatch, the encrypted CDs are kept in the locker in the office. Key to the locker is only

POL00105222

available to Case Work team in the local office. New safe will become available once HR move, which can be used for longer term storage, if required.

10. The SIMs are required to acknowledge receipts of the CD. Follow-up calls are made if no response.

11. The Case Work team records date of receipt from Fujitsu on the ARQ Database spread sheet and the whole request is marked in grey to signify that it has been dealt with.

12. A monthly (previously quarterly) review of despatched disks are made at the end of the month. Security Investigation Managers are chased for updates and locations of CD is logged. An annual review by Case Work Team Manager is completed.

13. When the SIM receives the CD and email with the password. Information required for evidence is downloaded to on to the SIM's laptop. Extracts maybe printed off for use during an interview. This extract is placed in Appendix 'B' (evidence Appendix) in the Case files ("Green Jackets" (GJ)). Printing of the full data maybe required for a trial.

    Note: The laptop has full hard disk encryption and the downloaded data is deleted from the laptop after the case is concluded.

14. Encrypted CD is retained by the investigator manager and stored in their locked personal pedestals, which they only have keys for. Passwords are not written down or kept with the CDs.

15. The Green Jacket (Case File) is then sent including Appendix B – Contains evidence (possibly encrypted / not full credit card information from the CD) to the Case Work Team by RMG Special Delivery tracked.

16. Email is sent to Casework Team confirming despatch by the SIM.

    Note: Green Jackets are sent between sites and external lawyers via Royal Mail Special Delivery with tracking and are followed by an email to the recipient from the sender and confirmation of receipt required is from the recipient to the sender.

17. Case Work team log receipt of the Green Jacket in there ARQ spread sheet

18. The Green Jacket is then sent to the Post Office lawyers, Cartwright King by the Case Work team.

19. Cartwright King will review evidence and may take copy of the evidence, which may contain Credit Card information.

20. If decision is made to prosecute, the file (Green Jacket) is copied by Cartwright King (copies retained) and the original is sent back to the Case Work Team.

21. Casework team then send it to Post Office Head of Security to review and decide to whether to proceed to prosecution.

22. The Green Jacket is then sent back to Case Work Team. Will log the decision to whether prosecute or not.

POL00105222

23. The Green Jacket is then sent back to the SIM by the Case Work Team. To review advice from Legal, Lawyers and the Post Office Head of Security.

24. If the **decision is not to prosecute**, then SIM will complete a closure form and send file (Green Jacket) back to Case Work team for archiving. The ARQ database will update to reflect the decision.

25. When the green jacket comes back to Bolton to the Case Work Team, if there is no further action, the disk is to be destroyed and logged on the sheet.

26. If **decision to prosecute** then SIM will retain Green Jackets until the whole process is completed which could be months or years. CD will be retained by the SIM in their pedestal until completion or sent for storage to Chesterfield Exhibit Store.

27. If we need to retain the disks (in case of prosecution) these need to be stripped from the green jacket, logged on a sheet with the destruction date and the destruction date on the disk and these are to be stored in Bolton in a secure cupboard. These are not to be sent with the green jackets to Chesterfield.

28. If the case results in conviction, sentence being imposed, the CD is retained for minimum 6 months or the length of the sentence, whichever period is greater. CD remains with the Green Jacket.

29. The Green Jackets are archived for 3 years for non-conviction cases and 5 years for cases resulting in prosecutions.

30. The Green Jackets are destroyed after the retention period and confirmation of destruction provided to the Case Work Team to be tracked in the Case Work destruction reconciliation spread sheet.

Copies of Files Retained by Lawyers

1. Copies of files retained by the lawyers are tracked by the SIM, who have been made aware of the security to keep information secure in their possession. Cartwright King's premises are secure and alarmed and deal with other privileged and sensitive information.

2. Evidence shared with defence lawyers and the court. This is a legal requirement under the jurisdiction of the courts. Neither Post Office nor Cartwright King has control over this.

3. Cartwright King recover copies of the files as far as possible and destroy them.

4. Confirmation of destruction is provided to Post Office investigation manager via email.

Controls

Process	Responsibility	Description
	Case Work team	Record request details on ARQ database.

POL00105222

	Case Work Team	All ARQ requests to Fujitsu password protected.
	Case Work team	Update audit log
	Case Work Team Manager	Validation and authorisation of requests/transfers.
	Case Work team	Receipt Acknowledgment and Tracking
	Case Work team `	Monthly review of all disks
	Case Work team	Location and Destruction tracking
	Case Work Team Manager	Annual Review