FUJ00234971

Document Title:	POA Operations Major Incident Procedure
Document Ref:	SVM/SDM/PRO/0001
Release:	HNG-X
Abstract:	This document details the POA Major incident processes which supplements the major incident processes defined in the Fujitsu EMEIA Business Management Systems Major Incident Procedure with the Post Office Limited specific requirements or requests.
Document Status:	APPROVED This document contains sections that have been identified to POL as comprising evidence to support the assessment of named Acceptance Criteria by Document Review. These sections must not be changed without authority from the FS Acceptance Manager.
Author & Dept:	Matthew Hatch – POA Operations
Internal Distribution:	As listed on pages 4 and 5 for Mandatory Review Optional Review Issued for information
External Distribution:	For information Martin Godbold (POL), Dionne Harvey (POL)
Security Risk Assessment Confirmed	YES

Approval Authorities:

Name	Role	Signature	Date
Steve Bansal	Senior Service Delivery Manager	See Dimensions for record of approval.	

FUJ00234971

0 Document Control

0.1 Table of Contents

FUJ00234971

FUJ00234971

0.2 Document History

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
0.1	03-Oct-06	First draft – to detail the Major Incident Escalation process. Draft taken from Horizon Document CS/PRD/122, V1.0.	
1.0	11-Oct-06	Revision following comments from Reviewers	
2.0	02-Sep-08	Changes for Acceptance by Document Review: insertion of Section (0.4) containing table of cross references for Acceptance by Document Review and addition of note to front page. No other content changes.	
2.1	24-Feb-2009	Changes made for Acceptance by Document Review by Fiona Woolfenden including the removal of references to CS/PRD/074 which has been Withdrawn and replaced by SVM/SD/PRO/0018 and other tidying up changes. Other changes to update Contact details.	
2.2	14-Apr-2009	Some Personnel Name changes and POA to POA + Abbreviations. Security Updates to sections 5.1, 6.3, 8.2.1, 9.0,	
2.3	3-June-2009	Some Personnel Changes and minor changes following review in May 2009	
3.0	7-July-2009	Following security audit 2 minor changes. Alan Simpson now on distribution and 6.3, an extra bullet entry added at end of list.	
3.0	7-July-2009	Following security audit 2 minor changes. Alan Simpson now on distribution and 6.3, an extra bullet entry added at end of list.	
3.1	14-Jan-2010	Changes following director failing to sign off v3.0, plus minor contact changes.	
4.0	26-Mar-2010	Approval version	
4.1	18-May-2010	Following team restructure, the process has been significantly reviewed.	
4.2	03-Jun-2010	Updated following minor comments provided during review cycle of version 4.1. This version will be presented for approval at v5.0	
5.0	07-Jun-2010	Approval version	
6.0	14-Sep-2010	Approved version following updates to personnel and table in 10.4 and section 10.8	
6.1	15 July-2011	Updates to personnel and changes from 'Process' to Procedure'	
6.2	05-Sept-2011	Updates following changes requested by Bill Membery from 6.1, plus clarification of TRM role	
6.3	14- Oct- 2011	Cosmetic changes mainly changing RMGA with POA and also updating abbreviations	
6.4	21-Dec-2011	Updating of details for a Service Bridge. Also some POL requests. Despite this being an internal POA document, all external comments that can improve the document are considered.	
6.5	16-Jan-2012	Updated, following review and cosmetic changes in relation to version 6.4	

FUJ00234971

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
7.0	02-Jan-2013	Changes in relation to Personnel and also Tower Leads and other cosmetic changes	
7.1	04-Feb-2013	Changes in relation to Personnel and revisions around Communications	
7.2	17-Sep-2013	Major update to align with Business Assurance Management procedures and for organisational changes. (This version was originally identified as version 8.1)	
8.0	18-Oct-2013	Updated for minor changes from Nana Parry.	
8.1	10-Jun-2014	Amended to replace the HSD function with the Atos Service Desk and replaced IMT references with the MAC team. Also updated to reflect the introduction of Atos as POL's Service Integrator.	
9.0	14-Aug-2014	Implemented minor changes following 8.1 review cycle.	
9.1	22-Jan-2015	Optional Reviewers amended to include Chris Harrison & Shaun Stewart. Section 3.3.5 POLSAP Service Triggers added Section 10.1 amended to refer to the Major Incident Report and Post Incident Review Report templates which are now held in Dimensions.	
10.0	12-Feb-2015	Minor update to section 9.1 and issued for approval.	
10.1	10-Sep-2015	Note added to Section 1.1 General revision to reflect recent organisational changes, the removal of the Engineering service. Created table entry 6.13 and section 8.2 to cover the production and management of multiple versions of the Major Incident Report	
10.2	22-Sep-2015	Minor changes for comments received from informal review and issued for formal review.	
11.0	12-Jan-2016	Section 4.0 updated, table entry 6.12 amended, other minor updates and issued for approval. – This Version was REJECTED in Dimensions.	
11.1	23-Jun-2016	Section 4, Security Major Incidents deleted. Re-aligned cross references to section numbering from 5 onwards	
11.2	19-Jul-2016	Revised to include feedback from Steve Bansal replacing Tower Lead with Senior SDM and/or Service Lead and incorporated changes requested by Bill Membery.	
12.0	19-Jul-2016	Approval version	
12.1	14-Dec-2016	Section 3.3.5 POLSAP Service Triggers modified to reflect 5th October 2016 migration of POLSAP application support to Accenture. Section 7.1 modified to include recommendations to share lessons learnt across Fujitsu, as per the Fujitsu EMEIA Business Management System Major Incident Procedure issued on 28th July 2016.	
12.2	09-Jan-2017	Removed Sandie's name from optional review –appeared twice	
13.0	12-Jan-2017	Approval version	
13.1	20-Jul-2017	The procedure was checked and updated for CCN1602 (section 3.3.5 amended to remove reference to Credence), CCN1609 (no change) and CCN1614 (section 3.3.1 amended	CCN1602; CCN1609; CCN1614

FUJ00234971

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
		to remove reference to the VSAT service). Revised section 0.5.	
13.2	12-Sep-2017	Revised section 9.3, Out of Hours Duty Manager Contact Details.	
14.0	12-Sep-2017	Approval version. Updated link to Dimensions web service, section 9.1.	
14.1	31-May-2018	Major re-write so that the Fujitsu EMEIA Major Incident Procedure is used as the primary process and this document contains customer specific process requirements in managing a major incident. It also contains changes for HDCR changes and amendment in the Acceptance by Document Review, section 0.4. Requested internal Fujitsu Document Review	
14.2	26-Oct-2108	Section 3.3.6, Security Triggers, updated to include breaches of Data Protection Legislation	
15.0	24-Jan-2019	Incorporated changes for comments raised by Steve Bansal and Sandie Bothick.	
15.1	09-May-2019	Section 6.1 Technical Bridge enhanced for the actions managed by the Major Incident Communications Manager.	
15.2	03-August-2019	Following the Major Incident Walkthrough, Section 6.1 Service Bridge has been reviewed and amended. 1) Timings for IN/OOH. 2) The part of this section covering TRM (Technical Recovery Manager. Additionally, Section 6.2 Service Bridge has been amended in line with comments from Steve Bansal during the Major Incident Walkthrough	
15.3	25-September-2019	Following a communication from Phil Boardman and review meeting added section 6.7 to cover Requests to Disable Training Controls and to Re-Enable Training Controls. This new section was required following Post Office Limited signing CCN1641c	
15.4	28-January 2020	Following review meetings with Bill Membery, Sarah Selwyn, Andrew Hemingway, Steve Evans and Phil Boardman, added sections 3.3.7 GDPR Triggers, 3.3.7.1 Breach Notification to POL controller and EMEIA, 3.3.7.2 Recognising a data breach and collecting evidence, 3.3.7.3 Who decides if it is a data breach and 3.3.7.4 Supporting a GDPR audit resulting from a breach. Additionally, following receipt of an update from Bill Membery and Sarah Selwyn made further amendments.	
15.5	23-March 2020	This review was purely for the GDPR section of the document following the AMEX EPA SSK file incident. Following being sent out for internal review, made the low level changes suggested by Matthew Lenton, Steven Browell and Steve Bansal to section 3.3.7 and sub-sections. Additionally, added comments made to me by Bill Membery if the DPO does not come back or advises not to inform POL to section 3.3.7.1. Following the AMEX SSK EPA file issue added a comments to sections 3.3.6 Security Triggers and 3.3.7 GDPR Triggers and 8.4 role of Problem Manager.	
16.0	01-April 2020	This review is purely for the section 6.7 Requests to Disable Training Controls and to Re-Enable Training Controls, which relates to CCN1641c. Following a review of the list of authorised Fujitsu people by Phil Boardman (Fujitsu) the list has been amended in order to reflect the current people who can authorise this activity, from a Fujitsu perspective. Currently awaiting an update from Stuart Banfield (POL), following a review of the list of POL people who can request	

FUJ00234971

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
		this activity to be performed. Once received, further amendments will be made to the document.	
16.0	02-Apr-2020	Approval version	
16.1	07-Apr-2020	Following a review by Stuart Banfield (POL) in regards to the POL requestors for section 6.7.1.1 Requests to Disable Training Controls and to Re-Enable Training Controls, which relates to CCN1641c, the required changes have been made. No other changes have been made to the document and the changes made relate purely to what has been detailed above	
17.0	07-Apr-2020	For Approval	
17.1	20-Apr-2020	Following a Major Incident Management – Transition to Post Office Meeting held on the 15th April 2020, conducting a review of the document in order to replace any reference to Atos with Post Office as of 1st May 2020. This included the removal of Atos and the adding of Post Office to sections 6.4 Major Incident Communication Flow Diagram and 6.5 Post Office Major Incident Report Requirements Additionally, from section 0.5 Associated Documents (Internal & External) removed ISSC 11A Information Security Incident Management Procedure (ATOS) from the list.	
17.2	02-June-2020	Following a review by Steven Browell made the changes to section 0.3 Review Details and section 6.7.1. Handling Requests to Disable Training Controls in line with his comments. Following a review by Sarah Selwyn made changes to section 3.3.7.2 Recognising a Data Breach and Collecting Evidence, in line with her comments. Additionally, with the decommissioning of POLSAP removed any references and sections related to POLSAP. 3.3.5 POLSAP Service Triggers. Updated reference to Fujitsu Major Incident Process at 7.1. No other changes have been made to the document and the changes made relate purely to what has been detailed above.	
18.0	03-Jun-2020	Approval version	
18.1	16-Jun-2020	Following completing a Pluralsight training course "The State of GDPR: Common Questions and Misperceptions" made some minor changes to the section 3.3.8 Recognising a data breach and collecting evidence. Reviewed with Sarah Selwyn and agreed changes. No other changes have been made to the document and the changes relate purely to what has been detailed above.	
19.0	17-Jun-2020	Approval version	
19.1	14-July-2020	Added a minor change to section 3.3.5 Security Triggers in relation to using the configuration items to indicate if there are GDPR, PCI or PCI and GDPR implications Amended Steve Bansal's job title No other changes have been made to this document other than what has been highlighted above.	
19.2	01-Sep-2020	Following a discussion with the GDPR team with reference to communicating to the account about the configuration items related to PCI & GDPR, added a new configuration to TfSNow. This has resulted in section 3.3.5 Security Triggers in relation	

FUJ00234971

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
		to using the configuration items to indicate if there are GDPR, PCI or PCI and GDPR implications being updated No other changes have been made to this document other than what has been highlighted above.	
20.0	01-Sep-2020	Approval version	

0.3 Review Details

Review Comments by :	
Review Comments to :	Matthew Hatch
Mandatory Review	
Role	Name
POA Account Service Director	Steve Bansal
Service Architect	Phil Boardman
Head of Quality and Compliance	Bill Membery
POA Acceptance Manager	Steve Evans
POA Information Security Manager	Jason Muir
POA Senior Ops Manager HNS	Alex Kemp
Optional Review	
Role	Name
POA Infrastructure Operations Manager	Andrew Hemingway
POA Business Continuity Manager	Almizan Khan
POA Problem Manager	Matthew Hatch
POA Service Architecture Lead	Alex Kemp
POA MAC & OBC Manager	Sandie Bothick
POA Operations Manager, Systems Management	Jerry Acton
POA Head of Online Services	Sonia Hussain
Solution Design Architect, Web Services	Sarah Selwyn
POA Network Infrastructure SDM	Chris Harrison
POA Service Delivery Associate	Piotr Nagajek
POA Service Delivery Manager	Kelly Nash
POA Document Manager	Matthew Lenton
Issued for Information – Please restrict this distribution list to a minimum	
Position/Role	Name

(*) = Reviewers that returned comments

0.4 Acceptance by Document Review

FUJ00234971

The sections in this document that have been identified to POL as comprising evidence to support Acceptance by Document review (DR) are listed below for the relevant Requirements:

POL NFR DR Acceptance Ref	Internal FS POL NFR Reference	Document Section Number	Document Section Heading
SER-2200	SER-2178		Whole Document
SER-2202	SER-2179		Whole Document
SEC-3095	SEC-3266	3.3.6	Security Triggers
SEC-3095	SEC-3266	SVM/SDM/PRO/0018 section 8.5	Security Major Incidents

0.5 Associated Documents (Internal & External)

Reference	Version	Date	Title	Source
ARC/SEC/ARC/0001			Security Constraints	Dimensions
CS/IFS/008			POA/POL Interface Agreement for the Problem Management Interface	Dimensions
CS/QMS/001			Customer Service Policy Manual	Dimensions
EMEIA Incident Management Process			EMEIA Incident Management Process	EBMS
EMEIA Major Incident Process			EMEIA Major Incident Process	EBMS
EMEIA Root Cause Analysis (RCA) Process			EMEIA Root Cause Analysis (RCA) Process	EBMS
PA/PRO/001			Change Control Process	Dimensions
PGM/DCM/TEM/0001 (DO NOT REMOVE)			Fujitsu Services Post Office Account HNG-X Document Template	Dimensions
SVM/SDM/INR/2693			Major Incident Report Template	Dimensions
SVM/SDM/PLA/0001			HNG-X Support Services Business Continuity Plan	Dimensions
SVM/SDM/PLA/0002			HNG-X Services Business Continuity Plan	Dimensions
SVM/SDM/PLA/0031			HNG-X Security Business Continuity Plan	Dimensions
SVM/SDM/PRO/0018			POA Operations Incident Management Procedure	Dimensions
SVM/SDM/PRO/0025			POA Problem Management Procedure	Dimensions
SVM/SDM/SD/0011			Branch Network Services Service Description	Dimensions
SVM/SDM/SD/0023			POA Incident Enquiry Matrix	Dimensions
SVM/SDM/TEM/2531			Post Incident Report Template	Dimensions
SVM/SEC/MAN/3807			Post Office Account HNG-X GDPR Directory	Dimensions
DES/GEN/SPE/2756			Horizon Business Data Flows and Interfaces	Dimensions

FUJ00234971

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

0.6 Abbreviations

Abbreviation	Definition
BCP	Business Continuity Plan
BMS	Business Management System
EMEIA	Europe, Middle East, India and Africa
ITIL	Information Technology Infrastructure Library
MAC	Major Account Controllers
MBCI	Major Business Continuity Incident
MICM	Major Incident Communications Manager
MIM	Major Incident Manager
MIR	Major Incident Report
OOH	Out Of Hours
PCI	Payment Card Industry (as per Security Standards Council)
POA	Fujitsu Post Office Account
POL	Post Office Limited
POL ITSD	Post Office IT Service Desk
SDM(s)	Service Delivery Manager(s) (NB: Throughout this document SDM refers to a person responsible for the Service, and the SDM could work in, but not limited to, the Service Delivery, Service Support, and Release Management or Security teams).
SDU	Service Delivery Unit
SLT	Service Level Targets
SMC	System Management Centre
SMS	Short Message Service (as known globally within Mobile Telephone Networks)
SSC	Software Support Centre
TB	Technical Bridge
TfS (TfSNow)	Triole for Service – Hosts Incident, Problem and Change databases
TRM	Technical Recovery Manager

0.7 Glossary

Term	Definition
EMEIA Business Management System	The EMEIA Business Management System (EBMS) is the central library for all Policy, Process and associated assets which provides Fujitsu with the responsible way of working that keeps the company, its employees and the services we deliver efficient, effective and compliant
Fujitsu EMEIA	Refers to Fujitsu Services Holdings PLC, Fujitsu Technology Solutions (Holding) BV and their subsidiaries, whether they be incorporated within the EMEIA Region or not, and any other company or organization that is managed by the EVP, Head of EMEIA Region.

FUJ00234971

Term	Definition
T	Time of incident occurring
T+3	Time Incident Occurred plus 3 minutes

0.8 Changes Expected

Changes

0.9 Accuracy

Fujitsu Services endeavours to ensure that the information contained in this document is correct but, whilst every effort is made to ensure the accuracy of such information, it accepts no liability for any loss (however caused) sustained as a result of any error or omission in the same.

0.10 Security Risk Assessment

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

FUJ00234971

1 Introduction

1.1 Purpose

The purpose of this Post Office Account major incident procedural document is solely to supplement the major incident processes defined in the Fujitsu EMEIA Business Management Systems Major Incident Procedure with any Post Office Limited specific requirements or requests.

This document outlines the management guidelines to be used for Major Incidents impacting the live estate in communicating with Post Office Limited.

1.2 Owner

The owner of the Major Incident Management process at the local POA level is the Fujitsu POA Senior SDM, Problem and Major Incident.

2 Guidelines and Interfacing to Post Office

2.1 Guidelines

It is important to maintain a balance between:

a) Allowing the technical teams the right amount of time to diagnose and impact an incident

b) Avoiding unnecessary alerting of the customer

c) Assessing which incidents are major

2.2 Interfacing to Post Office

- During the MAC Core Hours (Monday – Friday 08:00 – 20:00, Saturday 08:00 – 17:00) and Bank Holidays 0800 – 1400 excluding Christmas Day. The MAC should be the first point of operational contact between Fujitsu and the Post Office Service Desk. The SMC are responsible for escalation of incidents to the POA OOH Duty Manager. The POA OOH Duty Manager may initiate communications with the Post Office OOH Duty Manger. The SMC operate on a 24 x 7 x 365 basis.
- Any activity detailed in this document which is assigned to the MAC team is handed over to the SMC outside the MAC Core Hours, with the exception of the above.
- The relevant technical teams who are aware of and monitoring a potential major incident must call the appropriate Major Incident Manager (Duty Manager out of hours) as ***soon as possible.*** This is not limited to major incidents alone, but applies wherever a state other than Business as Usual has been detected. The Major Incident Manager must in turn communicate the potential incident, to the POL Service Desk for awareness and monitoring in POL Post Office. This is usually done via the MAC team in core hours.
- The Major Incident Manager (or Duty Manager out of hours) is responsible for communicating both *up* the Fujitsu organisation and *across* (see appendix 9.3) to their counterpart in Atos. Where this is impractical (e.g. leave, out of hours, unavailable), the initiative should be taken to jump up the organisation. Of prime importance is that the customer is informed in a timely manner and at the correct touch point. This communication should be by voice or direct SMS. The communication should include the date, time, name, nature of the incident, priority, if service affecting, likely impact, and the Fujitsu owner to contact.

FUJ00234971

- The Major Incident Manager (Duty Manager OOH, who covers Monday to Friday 17:30 to 09:00 and from 17:00 Friday though to 09:00 Monday) should also initiate communication using SMS via the MAC team (see operational hours above.). Outside of these hours the SMS should be via the SMC. The SMS distribution list used is titled 'SMS Internal' and amongst others includes the appropriate members of the POA Operations Management Team.

3 Post Office Account defining a Major Incident

3.1 Incident Classification

As a general rule a Major Incident will be an incident rated as a Business Critical Incident as shown in the following

- The 'CONTRACT'
- Sections 3.2 and 3.3 below.
- POA Operations Incident Management Procedure document (SVM/SDM/PRO/0018).
- A series of connected lower priority incidents which combine to have a significant business impact.

However not all incidents rated as priority 1 qualify as a Major Incident as the priority levels do not always reflect the overall business impact to POL. For example a single counter post office which is unable to trade, regardless of its business volumes, is rated as a priority 1 incident.

For incident classification on Post Office Account refer to the POA Incident Enquiry Matrix SVM/SDM/SD/0023.

3.2 Influencing Factors in calling a Major Incident

It is important that a Major Incident is defined in accordance with section 3.3 Major Incident Triggers, as such, because of its business impact on the day when it occurs, rather than simply being defined as a Major Incident because it appears on a list. However the following parameters will also feed into the consideration of whether a major incident should be called:

- Duration, i.e. how long has the vulnerability to service already existed?
- Impact across the estate, including consideration of whether a service is merely degraded or actually stopped
- Time at which the event occurs in relation to the 24 hour business day
- Time of year – e.g. Peak Trading Period, Christmas / Easter / End of month / quarter
- Anticipated time before service can be resumed
- Impact to POL branches, customers, clients or brand image
- Business initiatives e.g. product launches

3.3 Major Incident Triggers

The following criteria could trigger a major incident, however as detailed in 3.2, the influencing factors must also be considered. As such the list below is not exhaustive, whilst if an incident occurs which is not detailed below, e.g., legislative, it should not necessarily be precluded from being declared a major incident.

FUJ00234971

It should be noted that any call trends in relation to the following, should be reported to the POA Duty Manager as soon as the agreed threshold levels have been breached.

3.3.1 Network Triggers

Network Major Incident triggers are as follows:

- Complete or significant outage of the Central network, e.g. failure of both 3750 stack Catalyst switches in totality for the Core layer in IRE11.

3.3.2 Infrastructure Components Triggers

Infrastructure component Major Incident Triggers are as follows:

- Total loss of environments providing individual online service capability
- Breach of access to data centres
- Breach of security
- Virus outbreak.

3.3.3 Data Centre Triggers

Data Centre Major Incident triggers are as follows:

- Network / LAN outage
- Loss of Data Centre, or significant loss of Data Centre Components
- Breach of security.

3.3.4 Online Service Triggers

Online services Major Incident Triggers are as follows:

- Online service unavailable within the Data Centre (not counter level)
- Third party provided service failure – e.g. DVLA, Link, Moneygram, Santander etc.

  N.B Once the third party service provider has been deemed to be the source of the Major Incident; it will be managed by either POA or POL Service Desk in accordance with whichever organisation manages that supplier relationship.

3.3.5 Security Triggers

Security major incident trigger examples are as follows:

- Actual or suspected attacks on the Fujitsu Services Buildings and its resources, POA Network or Information Systems
- Theft of IT equipment / property
- Theft of software
- Either Cardholder Data or Sensitive Authentication Data not being handled as described in the CCD entitled "Security Constraints" (ARC/SEC/ARC/0001) or as required by PCI –DSS. For example (AMEX) American Express sending EPA files such as the SSK file that does not conform to the AIS (Application Interface Specification)
- Breach of Data Protection Legislation – inclusive of the GDPR, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and all other Applicable Law in respect of data

FUJ00234971

protection and data privacy including any applicable guidance or codes of practice that are issued by the Information Commissioner, Working Party 29 and/or the European Data Protection Board (and each of their successors);

In the event of a Security Incident, minor or major (which also include GDPR and PCI Incidents), the POA Operational Security Manager MUST be informed.

The POA Incident Management procedure SVM/SDM/PRO/0018 Appendix A provides further guidance on security incidents and the contact details for the POA Operational Security Manager is contained in Appendix B.

From a corporate perspective the Fujitsu EMEIA SECURITY INCIDENT REPORTING PROCEDURE is to be followed.

If the Security Incident has been confirmed to be a GDPR Incident, minor or major please follow the GDPR process. Also, please add the appropriate configuration item to the incident i.e. GDPR, PCI or PCI and GDPR. This will allow us to report against any incident where GDPR and/or PCI breaches have been identified. Additionally, added the configuration of No PCI/GDPR impact, so we have the ability to highlight and report against this.

3.3.6 GDPR Triggers

If anybody on the Post Office Account suspect that a GDPR incident has occurred, then the Fujitsu Security Operations (CSPOA) team need to be engaged immediately, even out of hours.

When the Fujitsu Security Operations (CSPOA) team have determined or suspect that a GDPR issue has occurred and that the Major Incident Process needs to be followed:

GDPR major incident triggers\considerations are as follows:

- Is this personal data
- What type of personal data
  - Normal data
  - Sensitive data
- What is the data shared on, processed on or transmitted through
- Has the data come from a 3rd Party or the Customer. For example (AMEX) American Express sending EPA files such as the SSK file that does not conform to the AIS (Application Interface Specification)
- Has data been lost in the Fujitsu domain that can't be explained

If the answer to the above questions has confirmed that there has been a GDPR incident, then the process that should be adhered to is as follows:

- POA Duty Manager has identified a GDPR incident (suspected GDPR breach), during the management of an incident.
- In Hours there is a requirement to inform the Fujitsu Security Operations (CSPOA) team, and the Fujitsu GDPR team that currently consists of (Bill Membery, Steven Evans and Sarah Selwyn)
- Out of Hours there is a requirement to inform the OOH Contact for the Fujitsu Security Operations (CSPOA) team
- In hours Fujitsu Security Operations (CSPOA) team, Fujitsu GDPR team that currently consists of (Bill Membery, Steve Evans or Sarah Selwyn) in conjunction with the relevant SME, are required to raise an incident via the EMEIA Connect Security page

IRRELEVANT

FUJ00234971

- Out of Hours the CSPOA team are required to raise an incident via the EMEIA Connect Security page

  IRRELEVANT

- In hours a call to the EMEIA Alerts and Crisis Management team using the telephone number GRO is required. This is performed by a member of the GDPR team (Bill Membery, Steven Evans and Sarah Selwyn)
- Fujitsu GDPR team that currently consists of (Bill Membery, Steven Evans and Sarah Selwyn) in conjunction with the EMEIA DPO team investigate the root cause analysis of a GDPR suspected breach within 24 hours so Post Office Limited can be informed.
- Post Office Limited have 72 hours from being informed of a suspected GDPR breach to notify the ICO.

Please see below sections for information on Breach Notification to POL controller and EMEIA

3.3.7 Breach Notification to POL controller and EMEIA

If the Fujitsu Problem and Major Incident team require to contact the Post Office data protection team, particularly where root cause analysis of a suspected breach is being undertaken, the email address GRO can be used as a point of escalation as this mailbox is continually monitored.

Data processors (POA and POA sub-processors) must understand what personal data is contained within any data that has been lost, stolen, altered without permission, been subject to unauthorised access or is unavailable to the data subject that requires access to it etc.

POL have confirmed that the current Horizon Incident Management Process is to be used in the case of a suspected GDPR data breach and POL will determine if the incident is a GDPR breach.

In the event of a breach POA are to:

1. Follow the Major Incident Management process as below
2. Make sure if it is deemed a GDPR incident that the Fujitsu EMEIA Security Process is invoked via this link: EMEIA Breach Notification Policy Link and ensure that the EMEIA DPO has authorised a decision to notify POL of a breach before notify POL
3. If instruction to not notify POL by the EMEIA DPO, then do not proceed with notifying POL and leave as an internal incident.
4. If EMEIA DPO does not provide feedback within the 24 hour window, then proceed with notifying POL.
5. Immediately (within than 24 hours from discovery) inform POL in order that they can determine if it is a GDPR breach. POL will notify the ICO and, if appropriate, the impacted data subjects (under article 33 of GDPR legislation POL have 72 hours from becoming aware of the breach to notify the ICO of the nature of the breach and the containment plan).

SVM/SDM/PRO/0018 Appendix A provides further guidance on security incidents and the contact details for the POA Operational Security Manager are contained in Appendix B.

The POA Security Management team will follow:
SVM/SEC/WKI/3119 - POA Security Incident Management Work Instruction

- Suspected data breaches must be notified to POL within 24 hours (GDPR article 33(2) processor to inform controller of breach without delay). During business hours please contact the Post Office via the email address:

POLITD GRO who will triage the incident and forward onto the data protection team GRO in Hours if required.

- For OOH please contact the Post Office via the email address POLITD GRO as well as the Post Office OOH contact in order for the Post Office data protection team GRO) to be informed if required after being triaged. OOH the Post Office

FUJ00234971

Duty Manager's will add the data.protection GRO email address into any relevant communications.

NB: data.protection GRO can be used as a point of escalation as this mailbox is continually monitored.

3.3.8 Recognising a data breach and collecting evidence

How do you decide if it is a suspected data breach? There is a set of criteria defined by the Working Party 29.

As per the Working Party 29 (Independent European working party that deals with issues related to protection of privacy and personal data) Guidelines on personal data breach notification, **a security incident falling within one or more of the following categories should be considered a personal data breach**:

1. unauthorised or accidental disclosure of, or access to, personal data (a "Confidentiality Breach")
2. unauthorised or accidental alteration of personal data (an "Integrity Breach");
3. accidental or unauthorised loss of access to, or destruction of, personal data (an "Availability Breach").

As above the Working Party 29 is now known as the European Data Protection Board.

NB: Please refer to the SVM/SEC/MAN/3807 GDPR Directory (Post Office HNG-X Account GDPR Directory) held in Dimensions, for details of the Working Party 29 Guidelines. Please refer to sections 2.1.2 and 2.1.3 of the GDPR directory.

Additionally, please use the following link IRRELEVANT and refer to the document "Definition of Personal Data Breach.

The following information sources identify personal data content:

- See **'GDPR Capability Statements'** for high level information on personal data content defined for each Business Stream type in POA SharePoint: GDPR Capability Statements
- See '**GDPR Account Data Mapping'** and filter on the personal data and special category data columns in POA SharePoint. Use this spreadsheet in combination with DES/GEN/SPE/2756 'Horizon Business Data flows and Interfaces' in order to see the business flows in context and understand the interface numbering used in the spreadsheet. This spreadsheet also contains the names of the interface specifications that hold in detail the data elements within files (POL is yet to highlight personal data in these POL documents)
- See Section 5 of SVM/SEC/MAN/3807 'Personal Data Summary'.

Post Office are likely to ask POA for technical support in their report of the suspected breach to the ICO in at least the following areas:

- The nature of the suspected breach – what personal data has been impacted and how
  - Who accessed what data (content and artefact e.g. log, data file, device etc.) and when
  - What category is the suspected data breached
  - How many data subjects are suspected to be impacted and what category are these data subjects (since Horizon is transaction based it may be difficult to supply the number and category of data subjects but by inspection of data, where available, a best guess should

FUJ00234971

be attempted. This may involve ATOS where the data has been collected via AP-ADC at the counter)

- ○How many records are suspected to be involved
- ○Who are the suspected impacted data subjects
- ○ Whether the data has been replicated elsewhere e.g. Skype, e-mail, TFS Now, Peak

- •What is the estimated impact of the suspected breach on data subjects (i.e. what is the risk to data subjects whose data is breached)
- •Containment plan
- •Remediation Plan
- •What was done to prevent the suspected breach (security controls in place)

POA Operational Security will guide POA technical teams on gathering the above evidence.

Ensure suspected breaches and evidence collected is recorded (even if POL don't deem the incident as a GDPR breach). This evidence must be securely stored (encrypted) under the control of POA Operational Security and must reference the original TfSNow incident.

A useful webpage is the Information Commissioners Office, provides checklists that are useful. Please use the following link: https://ico.org.uk/for-organisations/guide-to-data-protection/

For additional information and guidelines for areas such as breach notifications a useful link is: https://ec.europa.eu/newsroom/article29/news.cfm?item_type=1390

3.3.9 Who decides if it is a data breach?

Post Office will ultimately determine using the evidence POA supply whether the incident is a GDPR data breach. Prior to notifying POL and passing POL the evidence POA and EMEIA DPO will analyse the evidence to determine if a breach has occurred.

See the EMEIA definition of data breach document link below. This document states that 'only the EMEIA DPO can authorise a decision to notify' the controller of a breach

The EMEIA Definition of Personal Data Breach and Legal DPO Personal Data Breach Guidance documents can be accessed via the link:

IRRELEVANT

3.3.10 Supporting a GDPR audit resulting from a breach

Please see section 2.6 of the document GDPR Directory (SVM/SEC/MAN/3807).

3.4 Major Business Continuity Incidents (MBCI)

For HNG-X the MBCI triggers are listed in:

- HNG-X Support Services Business Continuity Plan (SVM/SDM/PLA/0001)
- HNG-X Services Business Continuity Plan (SVM/SDM/PLA/0002)
- HNG-X Security Business Continuity Plan (SVM/SDM/PLA/0031)

These documents should be referred to as appropriate in the event of Major Incident to determine if Business Continuity needs to be invoked.

4 Calling the Major Incident

FUJ00234971

During business hours the Major Incident Manager declares and manages the Major Incident (with handovers to the POA OOH Duty Manager where applicable.)

Where the impact of the incident is not immediately obvious, and it is not clear if a Major Incident should be called, escalation and discussion with the POA Operations Management Team should occur, and a collective decision made. If a Major Incident is not called, the incident should be monitored until closure, to ensure that the impact does not increase to that of a Major Incident.

In the event that multiple services are impacted, multiple Major Incident Managers may be appointed by any Service Lead or Senior SDM and will remain in their roles until incident closure.

Out of hours the POA OOH Duty Manager is responsible for declaring a Major Incident.

Section 8 of this document specifies the roles and responsibilities during a major incident. The Major Incident Manager, see section 8.2, is referred to the Manage Major Incident Procedure and must endeavour throughout the life of a major incident to adhere to the principles of that procedure.

5 Process Flow

As stated in section 1.2 Purpose, this Post Office Account Major Incident Procedural document is solely to supplement the major incident processes defined in the Fujitsu EMEIA Business Management Systems Major Incident Procedure so please refer to the EMEIA procedure and utilise the templates provided within that procedure. These include the Major Incident Report and e-mail templates.

Section 6.4 of this Post Office Account process details the normal Major Incident Communication Flow agreed with Post Office

When initiating the Major Incident Report, as required by the Fujitsu EMEIA Business Management Systems Major Incident Procedure, take into consideration the Post Office specific reporting requirements detailed in the Post Office Major Incident Report Requirements contained in section 6.5 below.

6 Communications

6.1 Technical Bridge

This is a Fujitsu technical conference for Technical experts and SDU's to discuss and analyse the incident and to formulate an action plan to restore the service to POL without delay. It should enable the Technical Recovery Manager to baseline the anticipated response, covering resolution, time and resources required. This will also include the appropriate owning SDU of the service affected by the Major Incident.

The Technical Bridge will be set up as required by the Major Incident Manager.

Invitations to the Technical Bridge will be via SMS, email or voice. The SMS will be sent to the distribution list titled '**SMS Technical Bridge**'. The SMS text will be sent to technical experts on the POA and will include outline details of the Major Incident. Also dial in details and the start time will be provided as part of the meeting invitation.

The Technical Bridge will be started at T + 15 from the trigger, and reconvened at regular intervals during the Major Incident; the exact scheduling will be discussed and agreed at each preceding Major Incident Call. The timing of "T+15" for calling a Tech Bridge is for IN Hours only. For OOH the Duty Manager will be contacted (1 hour reasonable endeavours for response).

The Technical Bridge is chaired by the Major Incident Manager with the recovery managed by the Technical Recovery Manager.

FUJ00234971

The Major Incident Communications Manager (MICM) is responsible for ensuring that updates, e.g., internal POA or SMS messages to a wider audience are provided at regular intervals, ideally every 30 minutes or longer if an appropriate ETA for the next update relevant to the recovery actions is given.

The MICM is also responsible for ensuring that the Major Incident within TfSNOW is updated at regular intervals throughout the major incident, including relevant Technical Bridge updates, for audit trail and report writing purposes.

A request for a Technical Recovery Manager (TRM) will be made to the appropriate Service Delivery Unit or Development Leads, who will appoint the appropriate resource to be the TRM. Ideally this nomination is made at the start of the Technical Bridge and will be a SME and a person who is expected to drive to the resolution. Throughout the Technical Bridge and resolution of the incident, the individual may change during the bridge and evolvement. Also, there is a possibility that the role could be reassigned to different individuals.

Following each Technical Bridge, it is the responsibility of the TRM to agree any actions as follows

-Recovery / restoration actions (which should normally include the TfSNow Change numbers),

-Service Improvement Plan recommendations

-Risk Register recommendations

-Recommendations for any improvements to KELS / Alerting / Configuration changes

The above will be documented in the Major Incident Report which is produced using the MIR Report template contained within the Fujitsu EMEIA Business Management Systems Major Incident Procedure

6.2 Service Bridge

This is a service focussed call for Service Management (including the Technical Recovery Manager if appropriate) and POL to discuss the service impact of the Major Incident and to receive updates on the progress towards resolution. Post Office Major Incident Management may also be the initiators of a Service Bridge.

The purpose of the Service Bridge is to provide a focussed area from which strategic decisions can be made regarding a Major Incident.

As a guide the attendance could be made up of the following or their designated representative depending upon if the incident occurs IN/OOH:

- Post Office (Personnel as instructed by Post Office Major Incident Management or Live Systems Service Manager)
- The Senior SDM (Chair Person)
- POA Duty Manager IN/OOH
- POA other Service Leads or Senior SDMs
- POA Lead SDM, Problem and Major Incident
- POA Security Manager (If required)
- POA SDM owning the affected service
- Third Party Executives (if appropriate)

Service Bridge responsibilities include:

- Agreement of a containment plan
- Documentation of all agreed actions and timescales with owners
- Consistent management of the Major Incident across all the locations involved

FUJ00234971

- Management of potential Major Business Continuity Incidents (MBCI's) within Post Office and the POA
- Co-ordinate meeting times and locations

In the event of a Major Incident requiring a Fujitsu Service Bridge, it is envisaged that this will be in place at T+60 (or earlier if required by Post Office MIM). Participants required in the Service Bridge will be contacted via SMS as appropriate.

The Senior SDM will send out a text via the MAC team or SMC in order to organise a Service Bridge.

Invitations to the Service Bridge will be via SMS, email, voice or Skype Meeting.

The SMS text should state such details as;

- An outline of the ongoing incident,
- Dial in details
- Start time.

The chairperson's code is held by the POA Senior SDM and the Problem and Major Incident Managers. The chairperson, normally the Senior SDM will initiate the call.

The TRM will attend meetings as required and provide appropriate root cause analysis and corrective action detail.

In the event that Post Office MIM initiate the Service Bridge, they should provide the contact details via the POA Duty Manager for internal distribution.

6.3 Communication Process Flow

- On suspicion or confirmation of a Major Incident, the MIM will escalate to the Senior SDM for the area, Problem and Major Incident Management SDM, and to the POA Service Leads.
- The MIM will inform the Post Office Service Desk, via the MAC team, of the start of the service incident alerting of potential issues – including date, time, nature of the incident, priority and impact if known and then directly inform the Post Office Live Service Manager
- All updates to the Service Desk are via the MAC team, within agreed timescales controlled by the MICM
- The MICM will issue an SMS text to the POA via the MAC team, alerting of potential issues – including date, time, nature of the incident, priority, impact and name
- A POA Service Lead or Senior SDM will inform the following within 10 minutes of start of the service incident
  - POA Delivery Executive
  - POL Senior Service Delivery Managers

  And will coordinate and ensure consistency of response to Post Office and POA Senior Management via The Service Bridge
- Periodic (interval to be determined depending on the nature of the issue but not more than 30 minutes for Major Incidents) SMS updates to be sent to the original SMS Distribution list
- On final service restoration, an SMS text message must be sent to the original SMS Distribution list
- The POA Senior SDM, will confirm understanding of Major Incident closure with Post Office management and POA senior management, and agree next steps.

FUJ00234971

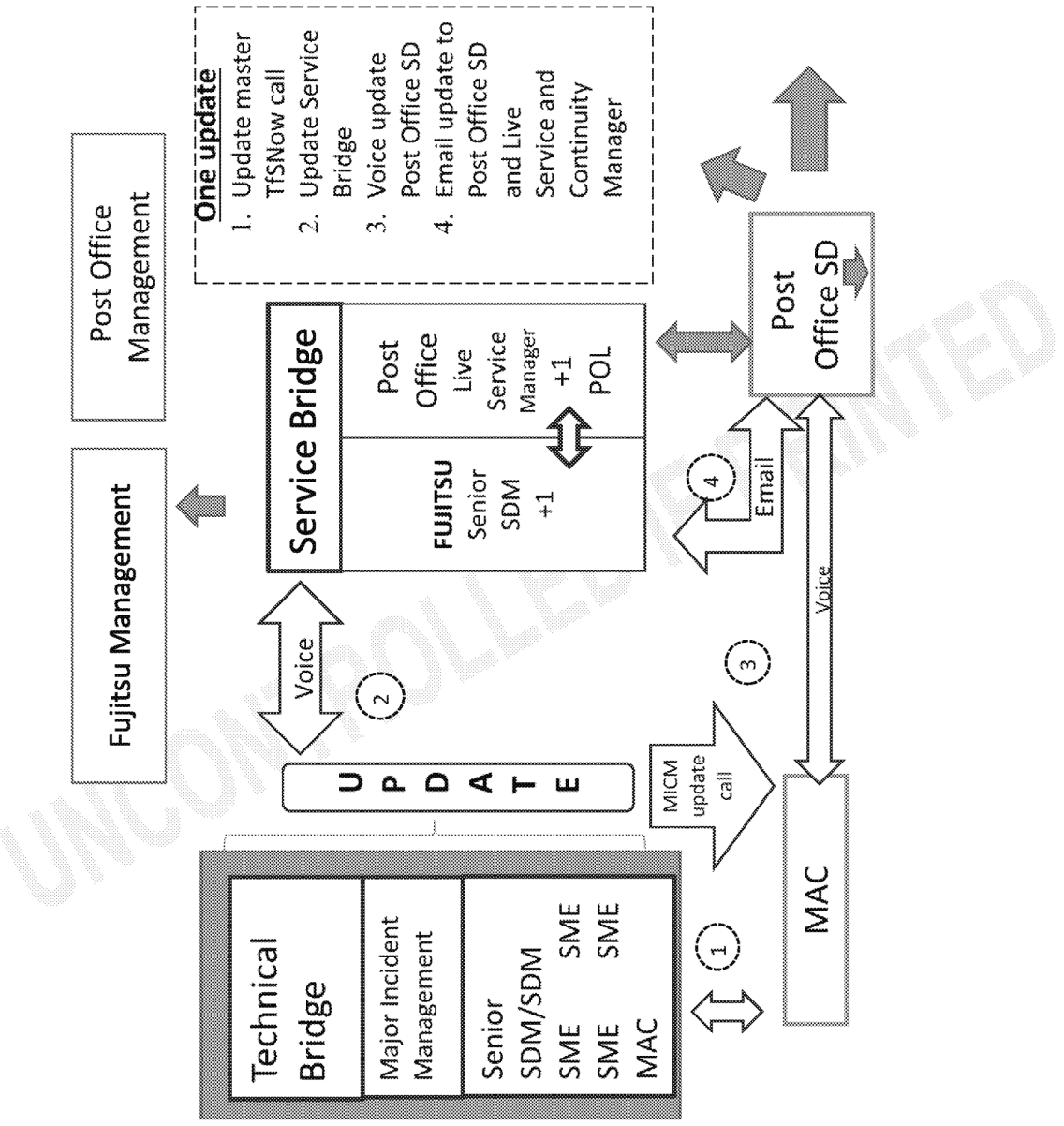

Figure 1: Major Incident Communication Flow Diagram

FUJ00234971

6.4 Post Office Major Incident Report Requirements

POL agreed template to base MI updates on.

Questions POL need to understand
What is the impact to POL? (Who/What is affected?) *Have there been calls to the Post Office Service Desk?* *Can branches trade?*
Which Means? (Expand impact)
What has happened? *Where in the system has a fault occurred?* *Is this in the Fujitsu domain or third party (ie.TTB)?*
When did it occur? *When did we become aware?* *When were Post Office first notified?*
What are we currently doing to resolve? *Tech Bridge / Who's investigating?* *Who have we escalated to?* *Are third parties involved?* *Have Post Office introduced an IVR or requested an MBS*
When is it expected to be fixed? *Do we require third party assistance to resolve?*
Why did it occur? *Has it been linked to a TfSNow Change?*

FUJ00234971

6.5 Escalation Communication Protocol

The primary principle:

"Up and Across"

Example:

The Major Incident Manager would escalate up to POA Lead SDM, Problem and Major Incident Management, and across to the Post Office Service Desk.

6.6 Requests to Disable/Re-Enable Training Controls

Training Controls have been added to the HNG-A/X Applications, which control the roles that Counter Users are able to logon with and the products that they can trade when logged on. Training Controls manage access in accordance with training curricula data provided by POL's identity management system. POL have expressed concerns that the training curricula data that they provide could be mis-entered or corrupted by the systems providing it (supplied by Accenture) so as to cause a catastrophic/wide-spread loss of access to HNG-A/X Users.

One approach to resolving such a situation would be for POL to Request that POA disabled Training Controls, completely, and then re-enable the Controls once the training curricula data had been corrected. Should such a situation arise, it is likely that it would be recognised during a Major Incident Service Bridge call. Similarly, it would be during a Major Incident Service Bridge call that POL would decide on Training Controls disablement, over any other courses of action to resolve (e.g. correcting the data in their identity management system or continuing with limited trading).

N.B. POL requesting us to disable Training Controls during a Major Incident Service Bridge call is **NOT** sufficient authorisation to action that request (see below)

6.6.1 Handling Requests to Disable Training Controls

Whilst discussions for requesting disablement of Training Controls might have occurred during a Major Incident Service Bridge, disablement should not be carried out until a formal authorised request has been received.

During the Major Incident service bridge call, should the decision be made to disable Training Controls, the Post Office signatory who will issue the request to disable Training Controls will be identified to Fujitsu Services. To enable the Post Office signatory to make the request, after the Service Bridge call POA Duty Manager will send an email to the identified Post Office signatory requiring Post Office to issue Fujitsu Services with instructions to make a Request to Disable Training Controls and subsequently a Request to Re-Enable Training Controls.

The email will contain the text below:

FUJ00234971

On the recent Service Bridge Call, it was indicated that Post Office Ltd. would wish to request disablement of Training Controls in HNG-X Systems and you were identified as the authorised Post Office signatory who would raise the request. The instructions for requesting disablement **and** re-enablement of Training Controls are shown below.

N.B. Please **retain** this email until after any Request to Re-Enable Training Controls has been issued.

To Request to Disable Training Controls

"Reply All" to this email, copying and pasting the text in the paragraph below into your reply;

> Post Office hereby request that Fujitsu Services temporarily disable Training Controls in HNG-X Systems with immediate effect until such time as Fujitsu Services receives a written Request to Re-Enable Training Controls from Post Office.

To Request to Re-Enable Training Controls

Whenever the decision is made to re-enable Training Controls, "Reply All" to this email, copying and pasting the text in the paragraph below into your reply;

> Post Office hereby request that Fujitsu Services re-enable with immediate effect Training Controls in HNG-X Systems, previously disabled.

Regards, Fujitsu Post Office Account Duty Manager

6.6.1.1 Recognising Requests to Disable Training Controls

In order to be an acceptable Request to Disable Training Controls, all of the following must be true;

- The expectation that POL would issue a Request to Disable Training Controls must have been expressed during a Major Incident Service Bridge Call. We should not accept "unexpected" requests to disable Training Controls. Any such requests received should be returned to the Post Office Limited IT Service Managers during normal working hours and not processed further. OOH please refer to the OOH Rota supplied by Post Office Limited for the Post Office IT and Post Office contact details and communicate with them and do not proceed any further.
- The request should be communicated on email to:
  - POA Duty Manager - GRO
  - Steve Bansal - GRO
  - Sonia Hussain - GRO

FUJ00234971

- The emailed request should be received from one of the Post Office Limited IT Service Managers;
    - Head of IT Service – Finance, Ops and Central - Paula Jenner
    - Heads of Service – Retail – Martin Godbold
    - Head of IT Service – Financial Services and Telecoms - Mark Nash
- The following deputies can also provide authorisation in a case where none of the above 3 were available:
    - Head of IT Service – FS & NS - Nick Baker
    - IT Service Design and Assurance - Stuart Banfield
    - IT Service Transformation Lead - Andy Jacques
    - IT Security & Service Director - Ben Cooke
    - IT Change Manager - Cherise Osei
    - Senior Service Manager (Retail) - Lorna Owens
    - Senior Service Manager - Matt Quincey
- The emailed request should include the following text:

> "Post Office hereby request that Fujitsu Services temporarily disables Training Controls in HNG-X Systems with immediate effect until such time as Fujitsu Services receives a written Request to Re-Enable Training Controls from Post Office."

On receipt of an acceptable Request to Disable Training Controls, the MIM/Duty Manager should;

- Reply to the Request email to confirm receipt
- Request to the POA Unix Duty Manager to Disable Training Controls reminding them that in order to do this they would need to arrange for someone to;

1. Logon to the BRDB (assuming node 1) as Unix user 'brdbblv1'
2. Invoke the command to disable the controls (where 'SOMEREF' is an Operational Change Emergency Operational Change or P1/P2 Incident reference):

```
$BRDB_SH/BRDBX011.sh -n BRDB_EUM_CONTROLS_ENABLED -t T -v N -r SOMEREF
```

- On confirmation that this action has been performed the MIM/Duty Manager should reply to the Request email confirming fulfilment.

If there was sufficient time to have raised an Operational Change between the Major Incident Service Bridge call and receipt of the acceptable Request to Disable Training Controls then the Operational Change reference should be provided, if not an Emergency Operational Change code should be used, but a follow up Operational Change should be raised.

6.6.2 Handling Requests to Re-Enable Training Controls

6.6.2.1 Recognising Requests to Re-Enable Training Controls

In order to be an acceptable Request to Re-Enable Training Controls, all of the following must be true;

- POL should have previously requested that we Disable Training Controls. We should not accept "unexpected" Requests to Re-Enable Training Controls. Any such requests received should be returned to the Post Office Limited IT Service Managers during normal working hours and not processed further. OOH please refer to the OOH Rota supplied by Post Office Limited for the Post Office IT and Post Office contact details and return the request to the specified Post Office Limited staff and do not proceed any further.

FUJ00234971

- The request must be communicated on email to;
  - POA Duty Manager - GRO >
  - Steve Bansal - GRO
  - Sonia Hussain - GRO
- The emailed request should be received from one of the Post Office Limited IT Service Managers:
  - Head of IT Service – Finance, Ops and Central - Paula Jenner
  - Heads of Service – Retail – Martin Godbold
  - Head of IT Service – Financial Services and Telecoms - Mark Nash
- The following deputies can also provide authorisation in a case where none of the above 3 were available;
  - Head of IT Service – FS & NS - Nick Baker
  - IT Service Design and Assurance - Stuart Banfield
  - IT Service Transformation Lead - Andy Jacques
  - IT Security & Service Director - Ben Cooke
  - IT Change Manager - Cherise Osei
  - Senior Service Manager (Retail) - Lorna Owens
  - Senior Service Manager - Matt Quincey
  - Service Design & Transition Lead - Financial Services & Telecoms - Darryl Inch
- The emailed request must contain the following text;

  "Post Office Ltd. hereby request that Fujitsu Services Re-Enable the Training Controls Support Facility in HNG-X Systems, previously Disabled"

On receipt of an acceptable Request to Re-Enable Training Controls, the MIM/Duty Manager should;

- Reply to the Request email to confirm receipt
- Request to the POA Unix Duty Manager to Re-enable Training Controls reminding them that in order to do this they would need to arrange for someone to;

  1. Logon to the BRDB (assuming node 1) as Unix user 'brdbblv1'
  2. Invoke the command to re-enable the controls (where 'SOMEREF' is an Operational Change, Emergency Operational Change or P1/P2 Incident reference):

     $BRDB_SH/BRDBX011.sh -n BRDB_EUM_CONTROLS_ENABLED -t T -v Y -r SOMEREF

- On confirmation that this action has been performed the MIM/Duty Manager should reply to the Request email confirming fulfilment.

If there was sufficient time to have raised an Operational Change between the Major Incident Service Bridge call, fulfilment of a Request to Disable Training Controls and receipt of an acceptable Request to Re-Enable Training Controls then the Operational Change reference should be provided; if not an Emergency Operational Change code should be used, but a follow up Operational Change should be raised.

6.6.3 Carrying out requests for Disabling and Re-Enabling Training Controls

There is no SLA to action these requests. Fujitsu will aim to action the request within 30 minutes of being received from one of the Post Office authorised staff if received between Monday to Thursday between

FUJ00234971

09:00 and 17:30 and 09:00 to 17:00 on Friday. For any other times such as OOH, weekends and Bank Holiday's Fujitsu will aim to action the request within 90 minutes.

The activity will be completed under a change raised in TfSNow by the Fujitsu UNIX Support team. Post Office Limited have agreed that this can be raised as an Emergency Operational Change Request during normal working hours and RETRO Operational Change Request for activity OOH.

6.6.4 Charging the Customer for Disabling and Re-enabling of Training Controls

Within the contract (Schedule D1) paragraph 7.14 specifies if and when the Disabling and Re-enabling of Training Controls is requested by Post Office Limited, it is a chargeable activity. Please engage finance that this charge needs to be invoiced against the appropriate month.

7 Formal Incident Closure & Post Incident Review

7.1 Post Incident Review

The Post Incident Review is chaired by the Major Incident Manager and follows a set agenda which is distributed with the Post Incident Review meeting invitation, along with the draft copy of the Major Incident Report (if available).

The template for writing a Post Incident Review Report is stored in Dimension (hyperlink below) under SVM/SDM/TEM/2531.

IRRELEVANT

The purpose of a Post Incident Review is:

- To understand the incident that prevented a Service or Services from being delivered.
- To confirm the impact to the business during and after the Incident and agree the number of branches impacted and duration of Major Incident.
- To confirm the end-to-end recovery process and timeline, and identify that all documented processes were followed.
- To analyse the management of the incident and the effectiveness of the governance process.
- To identify corrective actions, including agreed Third Party actions, to:
  - prevent recurrence of the incident
  - minimise future business impact
  - improve the procedure for the management of incidents

Output: To confirm details provided in the draft MIR provided to POL update with corrective actions and redistribute. To also include any of the following as appropriate

- any activities for a Service Improvement Plan
- any Changes and associated TfSNow Change reference.
- any follow up that requires to be progressed via Problem Management
- any improvements to KELS, alerting and /or event management

FUJ00234971

The agreed impact of the Major Incident must be provided for inclusion in the Counter Availability SLT Figures.

If this review highlights areas where improvements can be made, an agreed Service Improvement Plan will be produced, using the EMEIA SIP template, with appropriate actions, owners and timescales. It will also identify any ongoing risks to the service, together with any changes. Service Management will track all actions to resolution. Third party actions will be reviewed at Service Review meetings.

Consideration should be given as to whether the improvements can be shared across Fujitsu as lessons learnt, in accordance with Fujitsu EMEIA Business Management System document: Major Incident Process (29/09/2017). These are to be documented on the Lessons Learnt portal to help other Accounts to learn from the failures or success of the major incident activities. As stipulated in the document, there may be situations when the lessons cannot be shared due to confidentiality reasons.

It is important that the number of branches impacted and the duration of the Major Incident is agreed at the Major Incident Review. This information is required to calculate the impact on Branch and Counter Availability and any associated Liquidated Damages (LD) liabilities

7.2 The Major Incident Report

A first draft of the Major Incident Report is to be produced within 24 hours and on the approval of the POA Senior Service Delivery Manager sent to Post Office Service Management.

The first formal version of the Major Incident Report is to be produced within five working days and on the approval of the POA Senior Service Delivery Manager is sent to Post Office Service Management. Generally this report will be produced after a Post Incident Review is held and the actions for the Major Incident Report identified.

If applicable a Problem Record is to be opened for tracking the corrective actions and managed through the POA Problem Management Process. The formal Major Incident Report version 1.0 is to be attached to the TfSNow problem record and sent formally for storing in Dimension.

One or more formal versions of the Major Incident Report is to be produced which will also be sent to either Post Office Service or Problem Management, after the approval of the POA Senior Service Delivery Manager, providing feedback on the corrective actions. These major incident reports are also to be attached to the TfSNow problem record and sent formally for storing within Dimensions.

FUJ00234971

7.3 Calculating potential LD liability for Major Incidents

Major Incidents which qualify as Failure Events are detailed in the Branch Network Service Description (SVM/SDM/SD/0011). A Failure Event is defined in this document as an event or series of connected events which causes one or more Counter Positions to be deemed to be Unavailable due to a Network Wide Failure or a Local Failure. Ongoing failures will be deemed to be part of such a Failure Event until the Failure Event is closed in accordance with the Incident closure and Major Incident Review process as detailed in section 6.0.

For a Failure Event the Incident Closure & Major Incident Review Process will require Post Office and Fujitsu to agree the number of branches and counter positions affected and the duration of the outage (rounded to the nearest 30 minutes as detailed in the Network Wide Rounding Table).

Network Wide Rounding Table

Duration of Incident	Deemed duration for the purposes of LD calculations
30 minutes or less	30 minutes
More than 30 minutes but less than 1 hour	1 hour
1 hour or more but less than 1 hour 30 minutes	1 hour
1 hour 30 minutes or more but less than 2 hours	2 hours
N hours or more but less than N hours 30 minutes	N hours
N hours 30 minutes or more but less than (N+1) hours	(N+1) hours

FUJ00234971

8 Fujitsu Roles and Responsibilities during a Major Incident

This section defines the roles and responsibilities individuals and teams have as part of the Major Incident Escalation Procedure. The following roles will be laminated and available for the MIM to assign during a Major Incident.

8.1 Role of the MAC Team

The role of the Major Account Controllers team in the event of a Major Incident is as follows:

- Receive phone calls and log incidents from Post Office Service Desk, and communicate the progress of investigations to the Post Office Service Desk.

  Notes:

  1, There is also a HDI interface between Post Office SDM12 and Fujitsu TfSNow systems so incidents and updates may be automatically transferred as well

  2, These incidents are generally considered 'software' incidents as branch engineering incidents are no longer managed by Fujitsu.
- Escalation of any Call Threshold Breaches to the POA Duty Manager
- Confirming times and details to Major Incident Manager (MIM)
- Send/update service impact details from the Post Office Service Desk (e.g., trend analysis, which the MAC is dependent upon Atos supplying) to the Major Incident Manager. These details will be fed into the Technical Bridge in real time as requested, whilst details for the overall Major Incident will be provided to the Major Incident Manager post the incident.
- Be responsible for sending communications as provided by the Major Incident Communications Manager for the following:-

  To send out SMS text messages and attend all Technical Bridges

  -SMS to SMS Technical Bridge

  To inform of new Major Incidents and provide MI updates of progress to the following

  - E Mail Post Office Service Desk

  - Voice Post Office Service Desk

  -SMS to SMSInternal – POA Internal

  -SMS to POASeniors – POA Senior Management

  NB

  The above communications will be as per instructed by the Major Incident Communications Manager

  ALL should be identical, in order to avoid any misunderstandings.

  This also of course includes notification to Post Office Service Desk and POA Management of the restoration of service.

FUJ00234971

8.2 Role of the Major Incident Manager

Major Incident Manager (MIM). This will by default be either the Day Time Duty Manager or OOH Duty Manager (hours shown in 9.3). However a separate member of the Service Management team may be appointed as the MIM depending on the situation. The primary role of the MIM in a Major Incident is to facilitate the management of the Incident through investigation and diagnosis to resolution, with the aim of making the process as efficient and effective as possible. Upon determining that a Major Incident has been called, a request for a Technical Recovery Manager (TRM) will be made to the appropriate POA Service Lead or Senior SDM who will appoint one of his team to be the TRM. The Major Incident Manager acts as the central point for communication and non-technical information flow, allowing the TRM to focus on the technical situation and the resolution of the Incident. The Major Incident Manager is also responsible for creating and maintaining all the associated documentation. For the process to be effective, all updates and information regarding the incident must be fed to the MIM to update the timelines and report.

The Major Incident Manager:

- Calls and chairs the Technical Bridge
- Has responsibility for creating the Major Incident Report, using the template defined in section9.1 and ensuring that the applicable information is captured.
- Records the Technical Bridge attendees names so they can be documented in the Major Incident Report.
- Identifies Business and Service impact though discussions with the users, the Post Office Service Desk and the MAC team – providing this input into the Tech Bridge.
- Distributes the Technical Bridge actions provided by the TRM (if appropriate).
- In conjunction with the TRM considers if escalation into the Corporate Alert process is desirable and recommends this when required, see section 6.8 above.
- Assists with communication internally within the POA
- Track time lines
- Along with the POA Problem Manager, ensures that the TRM provides regular updates on any longer term corrective actions
- Following the resolution of the Incident, schedules and chairs the PIR.

FUJ00234971

8.3 Role of the Technical Recovery Manager

The primary functions of the Technical Recovery Manager are to co-ordinate and manage the restoration of service, manage the technical teams, and act as the communication point for the technical teams and third parties. The function will also include managing all longer term technical corrective actions, e.g. recommendations for improvements to KELs, eventing and configuration.

The Technical Recovery Manager:

- Manages the technical recovery of the Incident – liaising with SDUs and third parties.
- Provides updates on the recovery, when technicians / representatives of technical teams are unable to attend the Technical Bridge.
- Is the only person to liaise directly with the technical teams, including technical third parties.
- Provides summarised actions from Technical Bridge to the Major Incident Manager, including:
    - Current status including impact and risk
    - Advising on potential workarounds.
    - Planned recovery activities including timelines
    - Root Cause Analysis*, corrective actions, and their corresponding action owners and timelines (where known)

The TRM will be responsible for attending any meetings and providing appropriate root cause analysis and corrective action detail. This will also include managing any longer term technical corrective actions that are documented in the Major Incident Report and will include where appropriate:

- Any activities for a Service Improvement Plan
- Any Changes / TfSNow Change references
- Any Risks
- Any Configuration changes
- Any improvements to KELS, alerting and /or events
- Any associated Peak or TfSNow calls

* For Root Cause Analysis refer to the Fujitsu EMEIA Conduct Root Cause Analysis Procedure.

8.4 Role of the Problem Manager

The Problem Manager ensures that corrective actions / investigations are tracked and completed following the major incident.

Any corrective actions arising from the Major Incident Review will be added to the Major Incident Report and also a Problem Record if appropriate, and tracked with POL through to completion. The updates will be distributed to Atos as required, and in the case of a Security Major Incident associated with PCI failures, the POL Security team will also receive a copy of the report.

As Fujitsu have interfaces with 3rd parties such as American Express, then liaising with Post Office representatives from Service and support teams such as the Payments team as well as 3rd party representatives will be required, in order to contain, remove data etc, so the potential PCI\GDPR data breaches are resolved in a timely manner and with the required authorisations.

8.5 Role of the Communications Manager

FUJ00234971

The Major Incident Communications Manager (MICM) will attend the Technical Bridge and produce each update, where possible trying to ensure that updates are provided on time and following the agreed Major Incident Progress Template. This will reduce any miscommunication and ensure all parties follow process.

- Above all ensuring only one update is circulated
- Will ensure that updates are provided within the agreed times
- Updates will adhere to the agreed Major Incident Progress Template
- Update the master TfSNow call with all updates
- Ensure update is provided to MAC to circulate through to Post Office SD
- Supply update to Service Bridge
- Manages all communication internally within the POA
- Communicate to Fujitsu Core Major Incident Management team
- Manages via MAC, the communication with the Post Office Service Desk on the progression of the incident

8.6 Role of the SDUs: (Technical Teams /SMC/MAC & Third Parties)

The role is to investigate the Incident, monitor the progress and feed into the Technical Bridge. Also in the event of no pre-determined recovery options, suggest and evaluate potential recovery options to resolve the Incident.

The technical teams should not be contacted by any party other than the Technical Recovery Manager.

The Technical Teams / SMC/ MAC team & Third Parties should send an attendee to the Tech Bridge and the associated Major Incident Review meeting. Where attendance on the Tech Bridge is not possible, a suitable alternative resource should attend. If neither is possible then a full update MUST be provided to the TRM to ensure that the Bridge can be updated.

8.7 Role of the Service Delivery Manager owning the affected service

- Attends Technical Bridge
- Attends PIR
- Responsible for any further action proposed by the Problem Manager that falls outside the Major Incident closure criteria.
- Responsible for any Service Improvement Plan actions.

8.8 Role of the Service Lead/Senior SDM

- Appoint a Technical Recovery Manager
- POA Service Lead or Senior SDM will inform within 10 minutes of the start of the service incident the following-
  - POA Delivery Executive
  - POL Senior Service Delivery Managers

FUJ00234971

- Will coordinate and ensure consistency of response to Post Office and POA Senior Management via the Service Bridge.

9 Appendices

9.1 Daytime Duty Manager Contact Details

- Steve Bansal – GRO
- Matthew Hatch – GRO
- Sonia Hussain – GRO
- Piotr Nagajek – GRO
- Kelly Nash – GRO

9.2 Out of Hours Duty Manager Contact Details

The OOH Duty Manager provides cover between 17.30 - 09.00 Monday PM to Thursday AM and 17.00 - 09.00 Friday PM to Monday AM. The OOH Duty Manager can be contacted on the phone number detailed in the *Post Office Account Service Delivery Contact Details* on Share Point (see 9.4 below) or on the date relevant POA OOH Duty Manager rota.

Outside these times, please contact the POA Duty Manager

Note: Names and phone numbers are correct at the time of document issue and subject to change. In the event of difficulties refer to the Fujitsu Services Global Address List for the latest details.

9.3 POA Service Delivery Contact Details

The Post Office Account service delivery contact details can be found on the Post Office Account Share Point under *Operations* > *BCP* in a folder named *Post Office Account Service Delivery Contact Details.*

9.4 Special Situations

9.4.1 Personnel Absence

- In the absence of a POA Service Lead or Senior SDM, an alternative Lead will be appointed.
- Role cards have been produced and will be available to expedite the process.

9.4.2 OOH

- The OOH Duty Manager will act as the Major Incident Manager.

9.4.3 Duty Manager Change Over

- The Duty Manager at the beginning of the incident will be by default responsible for all MIM communications responsibilities unless a different arrangement is made between the outgoing and incoming Duty Managers.