FUJ00080222

Document Title:	POA Operations Major Incident Procedure
Document Type:	Procedure Definition
Release:	HNG-X
Abstract:	This document describes the POA Operations Major Incident Management Procedure.
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:	Mike Woolgar – POA Operations
Internal Distribution:	As listed on pages 4 and 5 for Mandatory Review Optional Review Issued for information
External Distribution:	For information Dave Hulbert (POL), Mark Weaver (POL), Gary Blackburn (POL) Richard Barber POL) Antonio Jamasb(POL)
Security Risk Assessment Confirmed	YES

Approval Authorities:

Name	Role	Signature	Date
Tony Atkinson	POA Head of Service Management	See Dimensions for record of approval.	

FUJ00080222

0 Document Control

0.1 Table of Contents

FUJ00080222

FUJ00080222

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for Acceptance by Document Review by Fiona Woolfenden including the removal of references to CS/PRD/074 which has been Withdrawn and replaced by SVM/SD/PRO/0018 and other tidying up changes.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	
7.0	18-Jan-2012	Approval version	

FUJ00080222

0.3 Review Details

Review Comments by :	
Review Comments to :	Mike Woolgar
Mandatory Review	
Role	Name
POA Head of Service Management	Tony Atkinson
POA Acceptance Manager	David Cooke
Optional Review	
Role	Name
POA Business Continuity Manager	Adam Parker
POA SAP and Credence SDM	Gaby Reynolds
POA Lead SDM, Problem and Major Incident	Steve Bansal
POA Lead SDM End User Services	Leighton Machin
POA Lead SDM Online Services	Elizabeth Bailey
POA Head Of Service Operations	Pete Thompson
Fujitsu HSD Operations Manager	Mike Clive (acting)
POA SMC Manager	Saha Saptarshi
POA Security Manager	Donna Munro
POA SDM HSD	Sandie Bothick
POA Quality Compliance and Risk Manager	Bill Membery
POA SDM Networks	Andy Hemingway
Issued for Information – Please restrict this distribution list to a minimum	
Position/Role	Name
POA CISO	Howard Pritchard
Fujitsu Unix Team Leader	Andy Gibson
Fujitsu NT Team Leader	Adrienne Thompson
Fujitsu DC Operations Manager	John Hill
POA Infrastructure Manager	Alex Kemp

(*) = Reviewers that returned comments

0.4 Acceptance by Document Review

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

FUJ00080222

SEC-3095	SEC-3266	3.3.5	Security Triggers
SEC-3095	SEC-3266	10.5	Security Major Incidents

0.5 Associated Documents (Internal & External)

Reference	Version	Date	Title	Source
PGM/DCM/TEM/0001 (DO NOT REMOVE)			Fujitsu Services Royal Mail Group Account HNG-X Document Template	Dimensions
CS/IFS/008			POA/POL Interface Agreement for the Problem Management Interface	Dimensions
SVM/SDM/SD/0025			POA Problem Management Procedure	Dimensions
PA/PRO/001			Change Control Process	Dimensions
CS/QMS/001			Customer Service Policy Manual	Dimensions
SVM/SDM/SD/0001			Service Desk – Service Description	Dimensions
266/FRM/HSD/001			HSD Business Continuity Activities Plan	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/0030			HNG-X Engineering Service Business Continuity Plan	Dimensions
SVM/SDM/PLA/0031			HNG-X Security Business Continuity Plan	Dimensions
SVM/SDM/SD/0011			Branch Network Services Service Description	Dimensions
SVM/SDM/PRO/0018			CS Incident Management Procedure	Dimensions
C-MSv1.3			Manage Incidents Process	BMS
C-MSv_roles			Service Management Process Roles and Responsibilities	BMS
SVM/SEC/STD/1823			LINK information security standard issued January 2001 (subject to such dispensations from that standard as LINK may grant from time to time).	Dimensions

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
A+G	Advice & Guidance
BCP	Business Continuity Plan
BMS	Business Management System

FUJ00080222

HSD	Horizon Service Desk
IMT	Incident Management Team
ISO	International Standards Organisation
ITIL	Information Technology Infrastructure Library
KEDB	Known Error Database
KEL	Known Error Log
MBCI	Major Business Continuity Incident
MIM	Major Incident Manager
MIR	Major Incident Report
MSC	Managed Service Change
MSU	Management Support Unit
OCP	Operational Change Proposal
PCI	Payment Card Industry (as per Security Standards Council)
PO	Post Office
POA	Fujitsu Post Office Account
POA	Fujitsu Post Office Account Business Unit
POL	Post Office Limited
RFC	Request For Change
SCT	Service Continuity Team
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, Release Management or Security teams).
SDU	Service Delivery Unit
SLT	Service Level Targets
SMC	Systems Management Centre
SMS	Short Message Service (as known globally within Mobile Telephone Networks)
SRRC	Service Resilience & Recovery Catalogue
SSC	System Support Centre
TB	Technical Bridge
TRM	Technical Recovery Manager
VIP	VIP Post Office, High Profile Outlet

0.7 Glossary

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

FUJ00080222

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.

FUJ00080222

1 Introduction

1.1 Owner

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

Objective

The key objective of the procedure is to ensure effective and efficient management of Major Incidents, through:

- Improvement of communication channels
- Clarification of the need to communicate awareness of potential incidents
- Improved accuracy of reporting of incident status
- Allowing technical teams the right amount of time to diagnose and impact an incident
- Avoiding unnecessary alerting of the customer
- Demonstrating a professional approach to the Post Office
- Provision of clearly defined roles and responsibilities
- Defined reporting and updating timelines throughout a major incident.
- Improved governance
- Assessing which incidents are major and which are 'Business as Usual'

1.2 Rationale

This document outlines the communication and management procedure and guidelines to be used for Major Incidents impacting the live estate.

The methodology defined within this document augments the existing SMS framework procedure presently deployed within the live estate.

The aim of the document is to provide a pre-defined procedure for future major incident communication and management.

FUJ00080222

2 Mandatory 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

The following guidelines should be adhered to.

- During the HSD IMT Core Hours (Monday – Friday 08:00 – 18:00 and Saturday 08:00 – 14:00) the HSD IMT should be the first point of operational contact between Fujitsu and the end user. Outside these hours the SMC acts as the first point of contact.
- Any activity detailed in this document which is assigned to the HSD IMT is handed over to the SMC outside the HSD IMT Core Hours.
- The relevant technical teams who are aware of and monitoring a potential major incident must page / 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. This is usually done via the HSD IMT 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 10.3) to their counterpart in POL. 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 problem, severity, if service affecting, likely impact, and the Fujitsu owner to contact.
- The Major Incident Manager (Duty Manager OOH) should also initiate communication using SMS via the HSD IMT (08.00 to 18.00 Monday to Friday, and Saturday 08.00 to 14.00). 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.

FUJ00080222

3 Definition of a Major Incident

3.1 Incident Classification

As a general rule a Major Incident will be an incident rated as severity level A (critical) in the POA Operations Incident Management Procedure document (SVM/SDM/PRO/0018), or a series of connected lower severity incidents which combine to have a significant business impact. However not all incidents rated at severity level A qualify as a Major Incident as the severity 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 severity A incident.

For simplicity, incidents are classified into three impact levels: High, Medium and Low.

High – An Incident that has occurred with a significant and potentially prolonged adverse impact on POL business. Typically these incidents will initially require a significant amount of reactive management before they can be controlled and resolved.

Medium – An incident that has the potential to cause significant impact to POL business but can be controlled and contained through effective management.

Low – An Incident that requires business attention but if managed effectively will not have significant impact on POL business.

3.2 Influencing Factors in calling a Major Incident

It is important that a major incident is defined 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. 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 criteria below 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 it should not necessarily be precluded from being declared a major incident.

FUJ00080222

3.3.1 Network Triggers

Network Major Incident triggers are as follows:

- Complete or significant outage of the Central network
- Complete or significant outage of the Talk Talk network
- Complete or significant outage of VSAT sites
- Complete or significant outage of the ISDN network (whether C&W, BT or Kingston Comms)

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)
- Number of Branches not able to provide online services – as defined by POL
- Third party provided service failure – e.g.DVLA, Link, Fujitsu Group

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 POSD in accordance with whichever organisation manages that supplier relationship.

FUJ00080222

3.1.5 Security Triggers

Security major incident triggers 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, and in particular PIN Pads
- Theft of software
- Any PIN Pad Issues that are in breach of FIPS 140-1 level 3 and ISO 9564 1st Edition 1991 section 6.3.1 as specified in the LINK information security standard issued January 2001 (subject to such dispensations from that standard as LINK may grant from time to time). The main criteria being as follows:

> *The purpose of this Standard is to protect the LINK Network, its Members and their cardholders and ATM owners from attacks designed to compromise sensitive data or defraud financial institutions and their cardholders. This protection takes into account not just the direct financial losses that may be incurred but also the potential reputational damage to the LINK ATM Scheme and its Members and its impact on customer confidence in LINK and ATMs in general. It is intended to protect the Link Brand:*
>
> *• the interests of the Members*
> *• the interests of the Members' customers*
> *• the reputation and integrity of the UK cash handling infrastructure*

In the event of a Security Major Incident (which may also include PCI Incidents), the POA Security Manager MUST be alerted who will then follow the Security Incident Management processes, as detailed in both:

SVM/SDM/PRO/0018 Appendix A

SVM/SDM/PLA/0031 HNG-X Security Business Continuity Plan (defines the actions to be taken if security violations are identified).

In the event of a Major Incident Security trigger for Fujitsu Services Buildings and its resources, the POA Security Manager MUST inform the Group Property Security Team who will be alerted either by telephone on a 24/7 basis or the next working day via our Incident Reporting process and the actual or potential impact of the incident dictates which route is followed.

The Group Property Security Team then take responsibility for interfacing into the corporate process by entering reports on to the corporate system

FUJ00080222

4 Calling the Major Incident

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

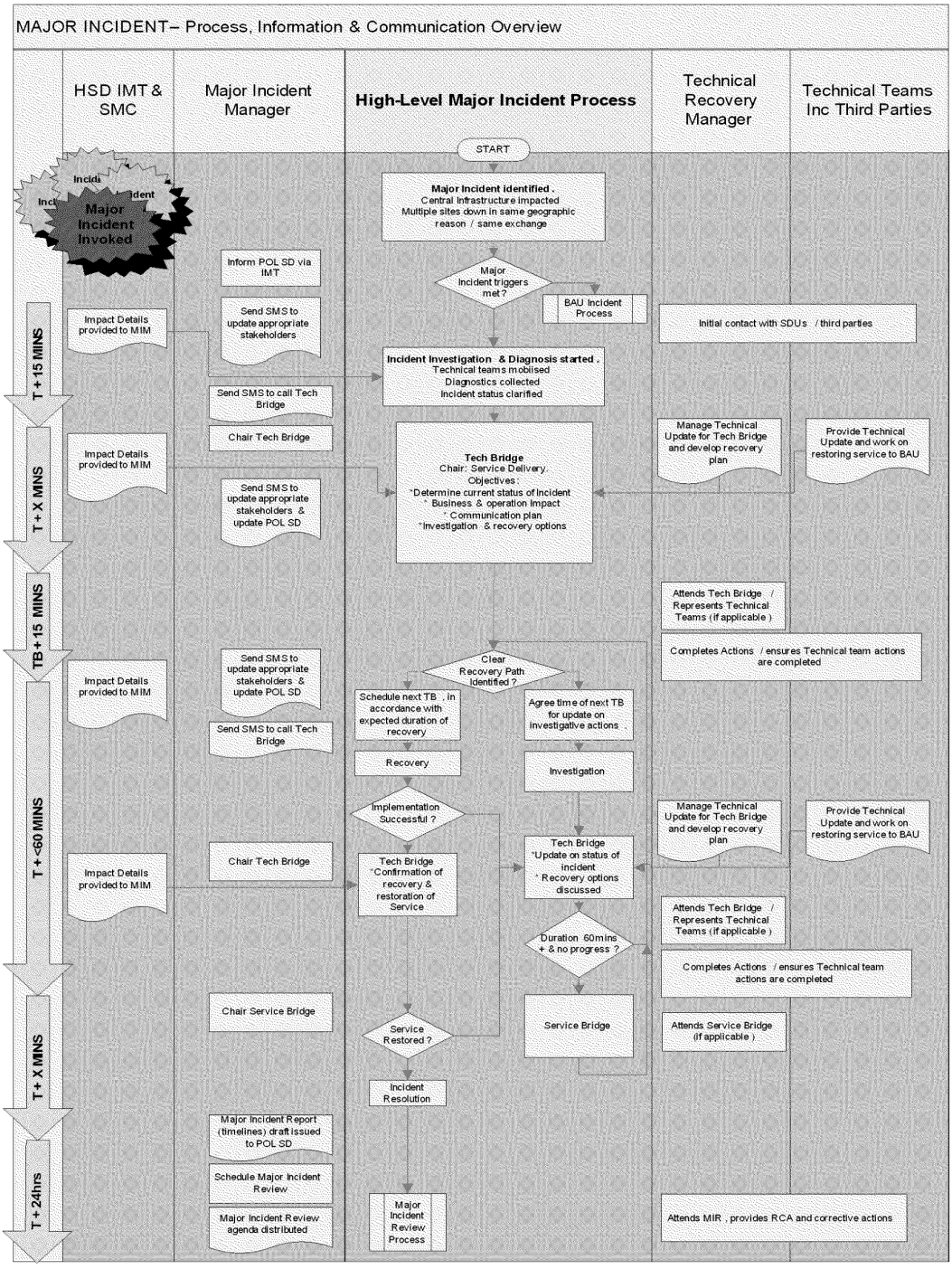
Where the impact of the incident is not immediately obvious, and it is not clear if a Major Incident should be called, escalation and discussion with the POA Operations management team should occur, and a collective decision made. If a Major Incident is not called, the incident should be monitored until 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 the POA Lead SDM, Problem and Major Incident Management, the POA Head of Service Operations or the POA Head of Service Management, who will remain in this role until incident closure.

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

FUJ00080222

5 Process Flow



FUJ00080222

5.1 Process Description (Any reference below made to T, = Time of incident occurring. Hence T+3 = Time Incident Occurred plus 3 minutes).

Box Title	Description	Key timescales	Action owner
Major Incident Identified?	Incident identified, the definition of an incident is "Any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of that service." (SVM/SDM/PRO/0018). An incident may be reported from within POL domain, a supplier domain or other route		
Major Incident Triggers Met?	An initial impact assessment of the incident is undertaken by members of the POA Service Team taking into account impact on: Live Service, Financial Integrity, Business Image The incident is profiled as a Major Incident as outlined within this document, including consideration of influencing factors, e.g. time, geographical coverage, business impact, security, public perception, duration and relevant business initiatives coinciding at POL, and decision taken to call a Major Incident. The Major Incident Manager will consult with the Business Continuity Plans (see section 0 of this document) to identify if potential MBCI or MBCI triggers have been met, and inform the POA Business Continuity Manager if appropriate. The POL Service Desk will be informed by the Major Incident Manager of the incident, and the incident will also be escalated to Service Management / Service Operations team managers, if this has not already occurred. With agreement from the POA SDM for the affected service, or the Duty Manager out of hours, an SMS will be sent to POA and POL Management alerting to the potential existence of a Major Incident.	T+3 All timescales quoted within this document should be viewed as a maximum, i.e. to be improved on where possible T+5	Major Incident Manager Major Incident Manager HSD IMT (in hours) SMC (out of hours)

FUJ00080222

BAU Incident Procedure	If a Major Incident is not declared then the BAU Incident procedure is followed – the POL Service Desk will be informed that there is no Major Incident and a closure SMS sent. The POA SDM for the service should ensure that the Incident is re-impacted during its lifecycle to ensure that the impact has not increased. If, subsequently the incident is declared a Major Incident, move to box "Incident Investigation and Diagnosis started".		
Incident Investigation & Diagnosis	Relevant internal SDUs / Third Parties contacted to initiate investigation & diagnosis. Major Incident Report opened Tech Bridge scheduled & agenda distributed.	T+ 5	Major Incident Manager Major Incident Manager
Tech Bridge	The Tech Bridge is chaired by the Major Incident Manager with assistance from the Technical Recovery Manager (TRM). The Tech Bridge is technically focussed. The Tech Bridge aims : • To discuss and agree the recovery, investigation and resolution of the Major Incident • To provide a forum for up-to-date progress reports • To aid communication, and if necessary, support the TRM in producing a short term technical recovery plan and if appropriate longer term corrective actions. These will be included in the Major Incident report. This is to ensure that Major Incident progress is known by all, whilst also, ensuring that all actions whether short term or long term are clearly stated. • To collate information for inclusion on the Service Portal. Attendees at the Tech Bridge may include POA Service	T + 15	Major Incident Manager

FUJ00080222

	Management, Fujitsu SDUs, Third Parties, POL, POA Operations Security, POL Security Managers and others The Tech Bridge follows a set agenda which covers: **Roll call, Summary of Incident, Incident Overview, Current Impact, Current Investigation / Recovery Action, Remedial Actions, Actions to carry forward to Major Incident Review** The agenda template is stored on **IRRELEVANT** Following the Tech Bridge, a further SMS will be sent, providing an update on the Incident If the outcome of the Tech Bridge is that the incident is determined Business As Usual (low) then an SMS communication will be sent stating that the incident is not a Major Incident. From this point forward SMS communication, timing and delivery requests becomes the responsibility of the Major Incident Manager. 30 minute updates should be the norm The Major Incident Manager will also distribute actions (provided by the TRM), following the conference call. At the time agreed at the first Tech Bridge, subsequent Tech Bridges are held as required. The same agenda is followed, and progress on actions / recovery is provided. If no clear recovery path is identified, the decision is then taken on whether to escalate for Service Bridge direction	Tech Bridge + 15	

FUJ00080222

Clear recovery path identified	If during the conference call a clear recovery path is identified, this should be discussed and agreed on the call. Following agreement the recovery should be implemented. If there is no clear recovery path, further investigation will be undertaken.		
Recovery / Investigation	The Technical Recovery Manager will liaise with the SDUs and /or third parties during the investigation / recovery. Where appropriate a Technical Bridge will be called for a technical discussion of the Major Incident.	T + x	Technical Recovery Manager
Tech Bridge 1+		T + x	Major Incident Manager
Service Bridge	The nature of the incident determines which POA Service Team members and POL Managers are involved in the Service Bridge but it would include **all or some** of the following: • POL (personnel as instructed by POL Live Systems Service Mgr) • POA Head of Service Management (Chair Person) • POA Head of Service Operations • POA Lead SDM, Problem and Major Incident • POA Business Continuity Manager • POA Security Manager • POA SDM owning the affected service • POA Technical Recovery Manager (if appropriate) • Third Party Executives (if appropriate) • Appointed working group representatives as appropriate	Timescale dependant on impact and nature of incident.	Major Incident Manager POL Service Manager

FUJ00080222

	• HSD IMT Representative The purpose of the Service Bridge is to: • Provide appropriate direction on incident resolution • Provide added impetus to restoration of service as quickly as possible • Define communication intervals to key stakeholders • Provide focused incident management in line with the impact and severity of the incident		
Incident Resolution	Once the incident is deemed to be resolved, a final Tech Bridge is held to agree and confirm resolution of the incident. A Major Incident Review date is set at the final Tech Bridge. An SMS communication is sent confirming resolution of the incident. A Draft Major Incident Report is distributed within 24 hours of resolution of the Major Incident.		Major Incident Manager
Major Incident Review & formal Incident Closure	Formal closure and a review of the Major Incident including consideration of: • Lessons learnt • Incident definition • What went well • Timeline • Changes required to the infrastructure • A review of the Major Incident communications		POA Lead SDM, Service Operations

FUJ00080222

	• Root Cause Analysis (if known at this point) • Business impact • Action plan, including any changes requiring MSCs • Service Improvement Plan update • Review any service risk(s) and update the Risk Register as appropriate		

FUJ00080222

6 Conference Calls

6.1 Technical Bridge

Dial in details: GRO Participant code: 72551658#.

Chair Code: 60233935#

This is a technical conference for experts 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.

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 all 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, and reconvened at regular intervals during the Major Incident; the exact scheduling will be discussed and agreed at each preceding Major Incident Call.

Each Technical Bridge follows a set agenda which will be distributed with the meeting invitation where possible. The conference call is chaired by the Major Incident Manager with the recovery managed by the Technical Recovery Manager.

A request for a Technical Recovery Manager (TRM) will be made to the POA Head of Service Operations, who will appoint one of his team to be the TRM.

Following each Technical Bridge, actions will be published by the Technical Recovery Manager to cater for any of the following

-Recovery / restoration actions (which should normally include associated MSC numbers),

-Service Improvement Plan recommendations

-Risk Register recommendations

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

The above should be documented in the Major Incident Report and stored on:

IRRELEVANT under Service Support > Major Incident Reports.

6.2 Service Bridge

Dial in details: GRO Participant code: 48461705#

Chair Code: 37289974#

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.

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

Attendance is made up of the following or their designated representative:

FUJ00080222

- POL (personnel as instructed by POL Live Systems Service Mgr)
- POA Head of Service Management (Chairperson)
- POA Head of Service Operations
- POA Lead SDM, Problem and Incident Management
- POA Business Continuity Manager
- POA Security Manager
- POA SDM owning the affected service
- POA Technical Recovery Manager (if appropriate)
- Third party representation (if appropriate)
- Appointed working group representatives as appropriate
- HSD IMT representative

FUJ00080222

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
- Management of potential / MBCIs within POL and the POA
- Co-ordinate meeting times and locations

In the event of a Major Incident requiring a Service Bridge, it is envisaged that this will be in place at T+60. Participants required in the Service Bridge will be contacted via SMS as appropriate.

The Major Incident Manager will send out a text to organise a Service Bridge.

Invitations to the Technical Bridge will be via SMS, email or voice. The SMS will be sent to the distribution list titled 'SMS HNGX External'

The SMS text should state such details as

an outline of the ongoing incident,

dial in details

and also the start time.

e.g. 'Your attendance is required at a Service Bridge to discuss the current Major Incident in relation to online Services. Please call GRO or GRO Participant code: 48461705# at 11.00 hrs.'

The chairperson's code is held by the POA Head of Service Management, POA Head of Service Operations, POA Lead SDM, Problem and Major Incident. The chairperson, normally the POA Head of Service Management, will initiate the call.

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

FUJ00080222

7 Formal Incident Closure & Major Incident Review

The Major Incident Review is chaired by the Major Incident Manager and follows a set agenda which should normally be distributed with the Major Incident Review meeting invitation, along with the draft copy of the Major Incident Report.

The purpose of a Major Incident Review is:

1. To understand the incident that prevented a Service or Services from being delivered.
2. To confirm the impact to the business during and after the Incident and agree the number of branches impacted and duration of Major Incident.
3. To confirm the end-to-end recovery process and timeline, and identify that all documented processes were followed.
4. To analyse the management of the incident and the effectiveness of the governance process.
5. To identify corrective actions to:
    i. prevent recurrence of the incident
    ii. minimise future business impact
    iii. improve the procedure for the management of incidents
6. To formally close the Major Incident

Output: To confirm details provided in the draft MIR provided to POL, update with corrective actions and redistribute. To also include

- any activities for a Service Improvement Plan
- any Changes and associated MSC numbers
- any Risks
- any Configuration changes
- any improvements to KELS, alerting and /or event management

The agreed impact of the Major Incident must be sent to the POA Infrastructure Manager 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 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.

The Agenda for the Major Incident Review is stored on:

IRRELEVANT under Service Support > Major Incident Management Templates

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

FUJ00080222

7.1 Calculating potential LD liability for Major Incidents

Major Incidents which qualify as Failure Events are detailed in the Branch Network Service Description (SVM/SDM/SD0011). 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 7.0.

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 below):

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

FUJ00080222

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.

8.1 Role of the HSD IMT

The role of the Horizon Service Desk Incident Management Team (HSD IMT) in the event of a Major Incident is two-fold:

- Receive and log calls from Post Masters, and communicate the progress of investigations to any Post Masters who call into the desk.
- Send service impact details (to include calls offered, abandoned, queuing) to the Major Incident Manager. This template should be completed every 15 minutes from the point of declaring a Major Incident, until the Major Incident Manager asks for this to cease.

8.2 Role of the Major Incident Manager

The primary role of the Major Incident Manager 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 POA Head of Service Operations, 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.

The Major Incident Manager:

- Has responsibility for creating the Major Incident Report
- Manages the communication internally within the POA
- Communicates with the POL Service Desk on the progression of the incident
- Identifies Business and Service impact though discussions with the users, the POL Service Desk and the HSD IMT – providing this input into the Tech Bridge.
- Calls and chairs the Technical Bridge
- Distributes the Technical Bridge actions provided by the TRM (if appropriate).
- Liaises with the SSC to update the Service Portal
- 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, the Major Incident Manager schedules and chairs the Major Incident Review and creates the Major Incident Report document.

FUJ00080222

8.3 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 corrective actions log and tracked through to completion. The updates will be distributed to POL 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.

8.4 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
    - 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 and MSC numbers
- any Risks
- any Configuration changes
- any improvements to KELS, alerting and /or events

FUJ00080222

8.5 Role of the SDUs: Technical Teams / Third Parties

The role is to investigate the Incident, and in the event of no pre-determined recovery options, suggest and evaluation of 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 / 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.

8.6 Role of the Service Delivery Manager owning the affected service

- Attends Post Major Incident review
- Responsible for any further action proposed by the Problem Manager that falls outside the Major Incident closure criteria.

FUJ00080222

9 Post Office / Fujitsu Interfaces

The Post Office / Fujitsu interfaces are detailed in the Procedure Description, section 5.1. However for ease the interfaces have been extracted into the table below.

POL Service Desk and POL management stakeholders updated – updated within 15 minutes of the Major Incident being called and after this according to the agreed timeline.

Draft MIR (timelines) provided – provided by the Major Incident Manager within one working day

MIR (timelines, root cause analysis, corrective actions) provided - provided by the Major Incident Manager within one working week

Service Bridge invitation – when the Major Incident has been unresolved for an hour or when it is deemed appropriate.

As detailed under Appendix 10.3, escalation of the Major Incident will also occur; this activity running concurrently to the interfaces detailed above.

FUJ00080222

10 Appendices

10.1 List of Templates

All templates are stored on the central share. : IRRELEVANT under Service Support > Major Incident Management Templates

NAME OF TEMPLATE	DESCRIPTION / NOTES	DISTRIBUTION
Major Incident Report Template	The Major Incident Report contains all the information about a Major Incident. This document is distributed to POL.	POL POA Service Management & Service Operations POA Head of Service Operations POA Head of Service Management Fujitsu Support Teams

FUJ00080222

10.2 Major Incident Manager Contact Details

- Steve Gardiner – GRO
- Mike Woolgar – GRO
- Steve Bansal – GRO

10.3 Out of Hours Duty Manager Contact Details

OOH Duty Manager Pager GRO) between the hours:

17.30 - 09.00 Monday PM to Thursday AM

17.00 - 09.00 Friday PM to Monday AM

Outside these times, please contact the Major Incident Manager

10.4 POA Service Delivery Manager Contact Details

AREA OF RESPONSIBILITY	EXAMPLE INCIDENTS	ESCALATION TO: SDM Service Owner	CONTACT DETAILS	BACK UP
Infrastructure issues. NT / UNIX / Data Centres	Data centre issues Storage Incidents NT /UNIX Incidents	Alex Kemp	GRO	Pete Thompson GRO
All Network Issues	Network Incidents / IP Stream / VSAT / ISDN Failures	Andy Hemingway	GRO 0	Alex Kemp GRO
POLSAP Issues	All POLSAP issues including File Delivery issues	Gaby Reynolds	GRO	Elizabeth Bailey GRO
Banking and Online Services (Inc: DVLA, Debit Card, EPAY)	Online Service outages	Elizabeth Bailey	GRO	Tony Atkinson GRO
Reference Data	New product not functioning	Steve Parker	GRO	Kevin McKeown GRO
Business Continuity	MBCIs or Potential MBCIs	Adam Parker	GRO	Pete Thompson GRO

FUJ00080222

Engineering	Major issue with engineering service	Leighton Machin	GRO	Tony Atkinson GRO
OBC Escalations	OBC job going wrong/ press involved /unhappy postmaster	Chris Bourne	GRO	Leighton Machin GRO
Major software problem	Major software problem	Steve Parker	GRO	John Simpkins GRO
HSD/ PostShops	Major TFS call logging issues. Major PostShop outage	Sandie Bothick	GRO	Leighton Machin GRO
Security	Security Issues Virus Alerts	Donna Munro	GRO	Pete Thompson GRO
Release Management / Service Introduction	Issues caused by Releases	Graham Welsh	GRO	Tony Atkinson GRO
SMC	Monitoring/ eventing of data centre environment	Saheed Salawu	GRO	Pete Thompson GRO

FUJ00080222

10.5 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.

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)
- HNG-X Engineering Service Business Continuity Plan (SVM/SDM/PLA/0030).

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

10.6 Security Major Incidents

In the event of a security major incident, the incident procedure as detailed in the POA Customer Services Incident Management Procedure (SVM/SDM/PRO/0018 Appendix A) must also be followed.

SVM/SDM/PLA/0031 HNG-X Security Business Continuity Plan defines the actions to be taken if security violations are identified.

10.7 Roles

- Major Incident Manager (MIM). This will by default be either the day time or OOH Duty Manager. A separate member of the Service Management team may be appointed as the MIM depending on the situation. The MIM will handle all communications to the HSD IMT and keep track of time lines. The MIM is also responsible for sending SMS messages but this can be delegated. The MIM will be assisted by a Technical Recovery Manager (TRM) for all technical aspects, (including actions for both recovery and longer term changes / risks and Service Improvement Plans) and also a Problem Manager who will be responsible for managing any resultant problems to resolution. 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.
- Head of Service Management – is solely responsible for verbal and written communications with POA senior managers and POL management.

FUJ00080222

10.8 Communication Process Flow

- On suspicion or confirmation of a Major Incident, the MIM will escalate to the Lead SDM, Problem and Major Incident Management, and to the Head of Service Operations
- The MIM will inform the POL Service Desk, via the HSD IMT, within 5 minutes of the start of the service incident
- All updates to the POL Service Desk are via the HSD IMT within agreed timescales controlled by the MIM
- The MIM will issue an SMS text to the POA alerting of potential issues – including date, time, nature of problems, severity, impact and name
- The POA Head of Service Management will inform the following within 10 minutes of start of the service incident
    - POA Operations Director
    - POL Senior Service Delivery Managers – currently Dave Hulbert and Tony Jamasb

  and will coordinate and ensure consistency of response to POL and POA Senior Management

- 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 Dist list
- On final service restoration, an SMS text message must be sent to the original SMS Dist list
- The Head of Service Management will confirm understanding of Major Incident closure with POL management and POA senior management, and agree next steps
- The MIM will continue liaising with the HSD IMT

10.9 Special Situations

10.9.1 Personnel Absence

- In the absence of the POA Head of Service Management, the POA Head of Service Operations to deputise
- In the absence of both, a nominated individual would have been chosen before hand

10.9.2 OOH

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

10.9.3 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
- The POA Head of Service Management will be informed, via text if out-of-hours, of who the active MIM is.