FUJ00080109



| | |
|---|---|
| **Document Title:** | POA Customer Service Major Incident Process |
| **Document Type:** | Process (PRO) |
| **Release:** | Not Applicable |
| **Abstract:** | This document describes the Customer Service Major Incident Management Process. |
| **Document Status:** | APPROVED<br>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 FUJITSU (UK & IRELAND) Acceptance Manager. |
| **Author & Dept:** | Mike Woolgar – RMGA CS Service Delivery Manager |
| **Internal Distribution:** | Peter Thompson, Adam Parker, Mike Woolgar, Ian Venables, Dave Keeling, Andy Gibson, Tony Little, Dave Jackson, John Flannigan, Joep Niens, Rosemary Burgess, Barry Flemming, Mike Stewart, Nick Crow, Neneh Lowther, Dave Wilcox, Ian Mills, Kirsty Gallacher, Tom Lillywhite Michael Jacklin, Sarah Hill, Leighton Machin, Karen Harrod, Sandie Bothick, Susan Appleby-Robbins, Adrienne Thompson, Claire Drake, Andy Dunks |
| **External Distribution:** | Dave Hulbert (POL), Mark Weaver (POL), Gary Blackburn (POL) Alan Simpson( POL) |
| **Security Risk Assessment Confirmed** | YES |



## Approval Authorities:

| Name | Role | Signature | Date |
|---|---|---|---|
| Gaeten Van Achte | Director Customer Services | | |

*Note: See Royal Mail Group Account HNG-X Reviewers/Approvers Role Matrix (PGM/DCM/ION/0001) for guidance.*

FUJ00080109



# 0 Document Control

## 0.1 Table of Contents

FUJ00080109

FUJ00080109



## 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for Acceptance by Document Review by Fiona Woolfenden including the removal of references to CS/PRD/074 which has been Withdrawn and replaced by SVM/SD/PRO/0018 and other tidying up changes.<br>Other changes to update Contact details. | |
| 2.2 | 14-Apr-2009 | Some Personnel Name changes and POA to RMGA + 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 | |



## 0.3 Review Details

| | |
|---|---|
| Review Comments by : | |
| Review Comments to : | Mike Woolgar & PostOfficeAccountDocumentManagement@ GRO |

| Mandatory Review | |
|---|---|
| Role | Name |
| Director Customer Services | Gaeten Van Achte |
| Service Support Manager | Kirsty Gallacher |
| **Optional Review** | |
| Role | Name |
| FUJITSU (UK & IRELAND) CS Business Continuity Manager | Adam Parker |
| FUJITSU (UK & IRELAND) CS Service Delivery Manager Engineering | Leighton Machin |
| FUJITSU (UK & IRELAND) CS Service Delivery Manager BankOnLine | Mike Stewart |

FUJ00080109



| | |
|---|---|
| FUJITSU (UK & IRELAND) CS System Support Centre Manager | Tony Little |
| FUJITSU (UK & IRELAND) HSD Operations Manager | Michael Jacklin |
| FUJITSU (UK & IRELAND) SMC Manager | Karen Harrod |
| FUJITSU (UK & IRELAND) Acceptance Manager | David Cooke |
| FUJITSU ( UK & Ireland) RMGA Quality Manager | Tom Lillywhite (acting) |
| Issued for Information – Please restrict this distribution list to a minimum | |
| Position/Role | Name |
| FUJITSU (UK & IRELAND) CS Service Delivery Manager: Networks | Ian Mills |
| FUJITSU (UK & IRELAND) CS Security Manager | Tom Lillywhite |
| Unix Team Leader | Andy Gibson |
| NT Team Leader | Adrienne Thompson |
| Network Manager | Dave Jackson |
| Operations Manager | John Flanagan |

( * ) = 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 |
| 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 | | | RMGA/POL Interface Agreement for the Problem Management Interface | PVCS |
| CS/PRD/021 | | | RMGA Problem Management Process | PVCS |
| CS/PRO/110 | | | RMGA Problem Management Database Procedures | PVCS |
| PA/PRO/001 | | | Change Control Process | PVCS |
| CS/QMS/001 | | | Customer Service Policy Manual | PVCS |

FUJ00080109



| | | | | |
|---|---|---|---|---|
| SVM/SDM/SD/0001 | | | Service Desk – Service Description | Dimensions |
| CS/FSP/002 | | | Horizon System Helpdesk Call Enquiry Matrix and Incident Prioritisation | PVCS |
| TBA | | | SMS Messaging User Guide | PVCS |
| CS/PRD/121 | | | SMS Major Communication Framework Process | PVCS |
| CS/PLA/015 | | | Horizon Systems Service Desk and Business Continuity Plan | PVCS |
| 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 |

***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 |
| HSD | Horizon Service Desk |
| ISO | International Standards Organisation |
| ITIL | Information Technology Infrastructure Library |
| KEDB | Known Error Database |
| KEL | Known Error Log |
| MBCI | Major Business Continuity Incident |
| MSU | Management Support Unit |
| OCP | Operational Change Proposal |
| PO | Post Office |
| RFC | Request For Change |
| RMGA | Royal Mail Group Account |
| POL | Post Office Limited |
| SCT | Service Continuity Team |
| SDM(s) | Service Delivery Manager(s)<br>(NB: Throughout this document SDM refers to a person responsible for the Service, |

FUJ00080109



| | |
|---|---|
| | 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 |
| SRRC | Service Resilience & Recovery Catalogue |
| SSC | System Support Centre |
| 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 |

## 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.

# 1 Introduction

## 1.1 Process Owner

The owner of this process is the RMGA Service Support Team Manager.

FUJ00080109



## 1.2 Process Objective

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

- Improvements of communication channels.
- Clarify the need to communicate awareness of potential incidents
- Improved accuracy of reporting against status of incident
- Allowing technical teams the right amount of time to diagnose and impact an incident
- Avoid unnecessary alerting of the customer
- Demonstrate to the Post Office a more professional approach
- Provision of clear defined roles and responsibilities
- Defined reporting/update timelines through duration of a major incident.
- Improved governance
- Assessing which incidents are major and which are 'Business as Usual'



## 1.3 Process Rationale

This document outlines the communication and management process and guidelines to be followed in relation to Major Incidents impacting the live estate.

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

The aim of the document is to provide a pre-defined process on which future major incident communication and management will follow and that any parties involved in that process provide updates /receive updates at defined intervals from inception to closure of any major service impacts.

FUJ00080109



# 2 Mandatory Guidelines

Whilst 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) Avoid unnecessary alerting of the customer

c) Assessing which incidents are major and which are 'Business as Usual'

The following guidelines should be adhered to.

- During HSD Core Hours (Monday – Friday 08:00 – 18:00 and Saturday 08:00 – 14:00) Post Office Horizon Service Desk should be the first point of contact for operational contact between Fujitsu and the end user. Outside these hours SMC acts as the first point of contact.
- Any activity detailed in this document which is assigned to the HSD is handed over to SMC outside the HSD Core Hours.
- The relevant technical teams who are monitoring and aware of a potential major incident must page/call the appropriate Fujitsu Service Delivery Manager / Owner (Duty Manager out of hours) as ***soon as possible***, rather than wait. The Fujitsu Service Delivery Managers are detailed in Appendix 10.2. This is not limited to major incidents alone, but must be delivered wherever a state other than Business as Usual has been detected. The Fujitsu Service Delivery Manager / Owner must in turn communicate the potential incident, to POL SCT for awareness and monitoring in POL. However this could be done via the HSD IMT.
- The Fujitsu Service Delivery Manager / Owner (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 (i.e. leave, out of hours, unavailable), the initiative should be taken to jump up the organisation. The important fact 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 owner for contact.
- The Fujitsu Service Delivery Manager / Owner (Duty Manager) should also initiate communication using SMS via HSD, 08.00 to 18.00 Monday to Friday, and Saturday 08.00 to 14.00. Outside of these hours, SMS should be via SMC.

FUJ00080109



# 3 Definition of a Major Incident

## 3.1 Incident Classification

As a general rule a Major Incident will always be an incident rated as severity level A (critical) in the RMGA Customer Service Incident Management Process Details document (SVM/SDM/PRO/0018) version 2.0, or a series of connected lower severity rated Incidents which combine to have a significant business impact. However not all incidents rated at severity level A qualify. This is because the severity levels do not necessarily translate to the global business impact on POL's business. For example a single counter post office which is unable to transact, regardless of its business volumes is rated as a Severity A.

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 mitigated against 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 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. The following parameters will also feed into the consideration of whether a major incident exists, as follows:

- 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 – eg Christmas / Easter / End of month/quarter DVLA
- 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 be considered. As such the list below can never be exhaustive, whilst if an incident occurs which is not detailed, this should not be precluded from being a major incident.

FUJ00080109



### 3.3.1 Network Triggers

Network Major Incident triggers are as follows:

- Complete or significant outage of Central network
- Complete or significant outage of BT network
- Complete or significant outage of VSAT sites

### 3.3.2 Infrastructure Components Triggers

Infrastructure component Major Incident Triggers are as follows:

- Total loss of environments providing individual on-line 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
- Breach of security

### 3.3.4 On-Line Services Triggers

On-Line services Major Incident Triggers are as follows:

- On-line service unavailable within Data centre (not counter level)
- Number of Branches not able to provide on-line services – as defined by POL
- 3rd party provided service failure – Link, Fujitsu Group

### 3.3.5 Security Triggers

Security major incident triggers are as follows:

- Actual or suspected attacks on the Fujitsu Services RMGA Network or Information System.
- Theft of IT equipment / property, including software

In the event of a Security Major Incident (which may also include PCI Incidents), the security incident management process as detailed in

SVM/SDM/PRO/0018 Appendix A must also be followed by the SDM owning the Service.

FUJ00080109



SVM/SDM/PLA/0031 HNG-X Security Business Continuity Plan defines the actions to be taken if security violations are identified. This must also be followed by the SDM owning the service.

FUJ00080109



# 4 Calling the Major Incident

During business hours the Service Delivery Manager / Owner responsible for the Primary Service affected declares Major Incident and is designated the Incident Manager for the duration of the Incident (with handovers to the Duty Manager where applicable.)

Where the impact of the incident is not immediately obvious, and it is not clear if Major Incident should be called, escalation and discussion with the Service Delivery / Service Support Team Manager, Head of Service Management or CS Director should occur, and a collective decision made. If Major Incident is not called, the incident should be monitored until closure, to ensure that the impact does not increase to Major Incident.

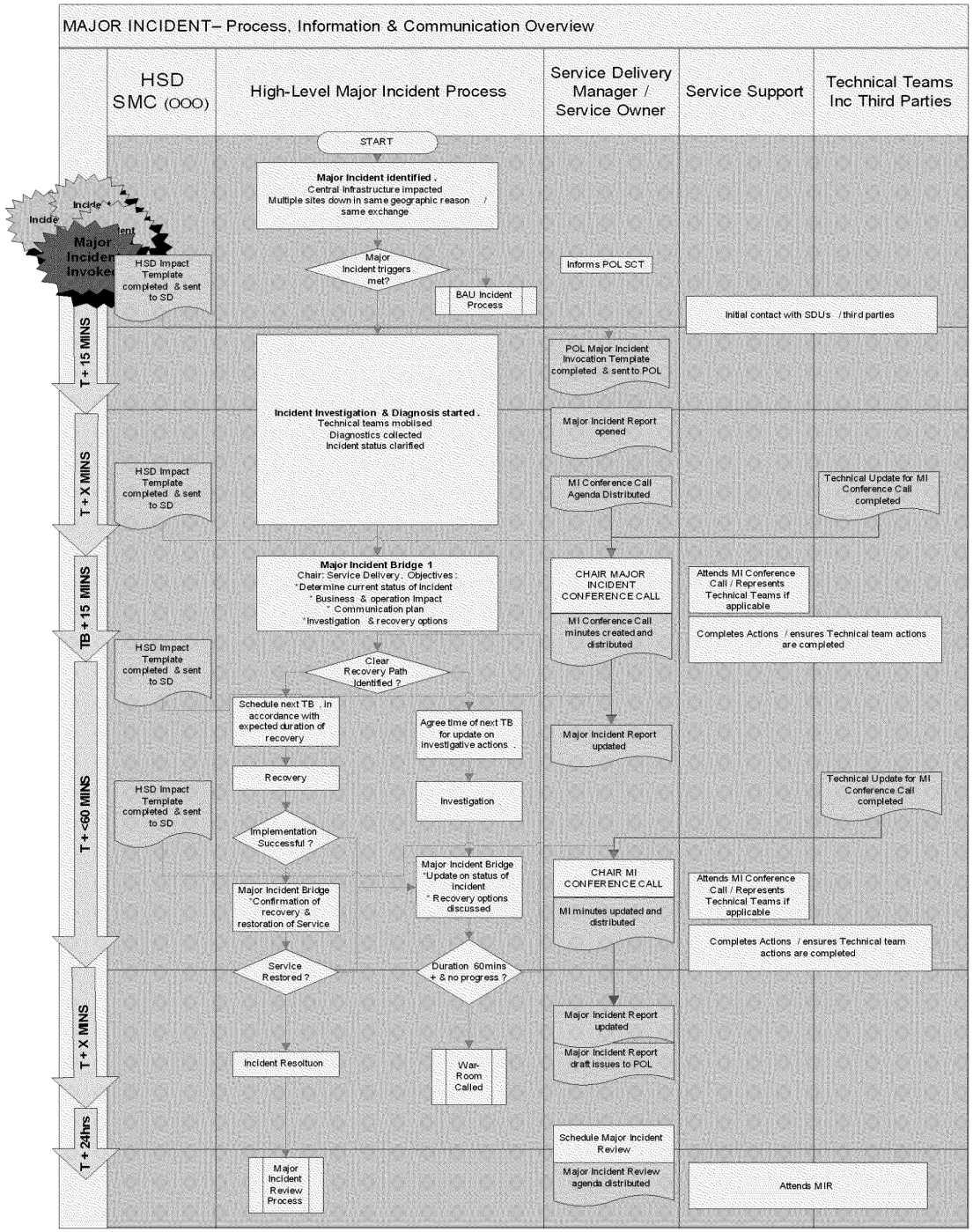
In the event that multiple Services are impacted, an Incident Manager will be appointed by Service Delivery / Service Support Team Manager, Head of Service Management or CS Director, who will remain in this role until incident closure.

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

FUJ00080109



# 5 Process Flow



FUJ00080109



## 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 RMGA Service Team taking into account impact on:<br>Live Service, Financial Integrity, Business Image<br>The incident is profiled as a Major Incident as outlined within this document, including consideration of all influencing factors, time, geographical coverage, business impact, security, public perception, duration and relevant business initiatives coinciding at POL and decision taken to call Major Incident<br>POL SCT will be informed by the Service Delivery Manager / Owner managing the Major Incident of the incident & the incident will also be escalated to Service Delivery / Service Support team managers, if this has not already occurred.<br>With agreement from RMGA Service Delivery Manager, or Duty Manager out of hours, SMS will be sent to RMGA and POL Management alerting to the potential existence of a Major Incident. | T+3<br>All timescales quoted within this document as viewed as maximum, to be improved upon wherever possible<br>T+5 | RMGA Service Delivery Manager / Owner(Duty Manager), RMGA Service Delivery / Support Manager, Head of Service Mgmt, CS Director<br>Service Delivery Manager / Service Owner<br>HSD (in hours)<br>SMC (out of hours) |
| BAU Incident Process | If Major Incident is not declared then the BAU Incident process is followed – POL SCT will be informed that there is no MI & a closure SMS sent. The 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 Major Incident, move to box "Incident | | |

FUJ00080109



| | | | |
|---|---|---|---|
| | Investigation and Diagnosis started". | | |
| Incident Investigation & Diagnosis | Relevant internal SDUs / Third Parties contacted to initiate investigation & diagnosis.<br><br>Major Incident Report opened<br>Major Incident Conference call scheduled & agenda distributed. | T+ 5 | Service Support Manager<br><br>Service Delivery Manager |
| Major Incident Bridge 1 | The Major Incident Bridge is chaired by the Service Delivery Manager / Owner who has been nominated as the Major Incident Manager. The Major Incident Bridge is SERVICE FOCUSSED.<br>The Major Incident Bridge aims :<br>• To discuss & agree the recovery investigation & resolution of Major Incidents<br>• To provide a forum for up-to-date progress reports<br>• To aid communication, and the creation of Technical Bridge Minutes which are distributed to all involved parties and RMGA & POL Management. This ensures that Major Incident progress is known by all.<br>• To collate information for inclusion on the Service Portal.<br>Attendees at the Major Incident Bridge include, but are not limited to, RMGA Service Management, SDU, Third Parties, POL., CS Security & POL Security Managers<br>The Major Incident Bridge follows a set agenda which covers: | T + 15 | Service Delivery / Service Support Manager |

FUJ00080109



| | | | |
|---|---|---|---|
| | **Roll call, Summary of Incident, Incident Overview, Current Impact, Current Investigation / Recovery Action, Remedial Actions, Actions to carry forward to Major Incident Review**<br>The agenda template is stored on<br>\\ATCFS7\POcust_serv\01Public\Major Incident Management \Templates<br>Following the Major Incident Bridge, a further SMS will be sent, providing an update on the Incident<br>If the outcome of the Technical Conference Call 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.<br>From this point forward, SMS communication, timing and delivery requests, becomes the responsibility of the RMGA Service Delivery Manager / Owner acting as Major Incident Manager. 30-minute updates should be the norm<br>Service Delivery Manager / Owner will also distribute minutes following the conference call | MIB + 15 | |
| 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.<br>If there is no clear recovery path, further investigation will be undertaken. | | |
| Recovery / Investigation | The RMGA Service Support Team Manager, acting as recovery manager will liaise with the SDUs and /or third parties during the investigation / recovery.<br>Where appropriate a Technical Bridge will be called for a technical discussion of the Major Incident. | T + x | RMGA Service Support Team Manager |

FUJ00080109



| | | | |
|---|---|---|---|
| Major Incident Bridge 1+ | At the time agreed at the first Major Incident Bridge, the subsequent Major Incident Bridges are held. The same agenda is followed, and progress on actions / recovery is provided.<br><br>If no clear recovery path is identified, the decision is then taken on whether to escalate for War Room direction | T + x | RMGA Service Delivery Manager |
| Escalate for War Room direction | The nature of the incident determines which RMGA Service Team members and POL Managers are involved in the War Room but it would include all or some of the following:<br>• POL<br>• RMGA Service Support Manager (War Room Chairman)<br>• RMGA CS Director<br>• 3rd party Executives<br>• Appointed working group representatives as appropriate<br><br>The purpose of the War Room is to:<br>• Provide appropriate direction on Incident resolution<br>• Provide added impetus to restoration of service ASAP<br>• Involve 3rd party Executives<br>• Define communication intervals to Key Stakeholders<br>• Provide focused Incident Management in line with the impact and severity of the Incident. | Timescale dependant on impact and nature of incident. | RMGA Service Support Team Manager<br><br>POL Service Manager |

FUJ00080109



| | | | |
|---|---|---|---|
| War Room drive working group actions | War Room provide the appropriate direction on the incident resolution priorities. | Timescale dependant on impact and nature of incident. | RMGA Service Support Team Manager.<br>War Room. |
| Incident Resolution | Once the incident is deemed to be resolved, final Major Incident conference call is held to agree & confirm resolution of incident. Major Incident Review date to be set at the final Major Incident Conference call.<br>SMS communication sent confirming resolution of incident.<br>Draft Major Incident Report distributed within 24hrs of resolution of Major Incident. | | RMGA Service Support Team Manager |
| Major Incident Review & formal Incident Closure | Formal Closure of the Major Incident & a review of the Incident including consideration of:<br>• Lessons learnt<br>• Incident definition<br>• What went well<br>• Timeline<br>• Changes required to infrastructure<br>• A review of the Major Incident Communication Process<br>• Root Cause Analysis * if known at this point<br>• Business impact<br>• Action plan<br>• Service Improvement Plan update | | RMGA Service Delivery Manager |

FUJ00080109



# 6 Conference Calls / War Room

## 6.1 Major Incident Conference Call

This is a Service Focussed call for Service Management, Technical experts and POL to discuss the service impact of the Major Incident and to receive updates on progress of the Incident.

Invitations to the Major Incident Conference Call will be via SMS, email or voice. The dial in details will be provided at the same time as the meeting invitation.

The Major Incident Conference Call will be incepted at T + 15, and at regular intervals during the Major Incident, the exact scheduling will be discussed and agreed at each preceding Major Incident Call.

Each Major Incident Conference Call follows a set agenda which will be distributed with the meeting invitation where possible. The conference call is chaired by the Service Delivery Manager / Owner acting as Major Incident Manager.

Following each Major Incident Conference Call, a set of minutes will be published, which will subsequently form part of the Major Incident Report.



## 6.2 Technical Conference Call

This is a technical conference for experts to discuss and analyse the incident enabling an appropriate action plan to be formulated to restore the service to POL without delay. The Technical Conference Call will baseline the anticipated response, covering resolution, time and resources required.

The Technical Conference Call will be incepted as required by the Service Support Manager.

## 6.3 War Room

The purpose of the War Room is to provide a focused area from which strategic decisions can be made regarding a Major Incident confirmed a MBCI.

Attendance will be mandatory from the following or their designated representative:

- RMGA Customer Services Director
- RMGA Service Management Team Manager
- RMGA Business Continuity Manager
- RMGA Service Delivery Manager / Owner (Business line specific)
- POL Head of Technical Services
- POL Service Continuity Manager
- POL Service Delivery Manager
- POL Business Continuity Manager
- 3rd Party Account/Service Delivery Manager
- RMGA Security Manager (If MI is a PCI or Major Security Incident)
- POL Security Incident Manager ( If MI is a PCI or Major Security incident)

FUJ00080109



Actions within the War Room include:

- Agreement of Containment Plan
- Documentation of all agreed actions with owners, and timescales
- Consistent management of the major incident across all involved locations
- Management of potential / MBCIs within POL & RMGA
- Co-ordinate meeting times and locations

In the event of a major incident requiring a War Room to be incepted, it is envisaged that this will be in place at T+60. Participants required in the War Room will be contacted via SMS as appropriate.

The RMGA Service Delivery Management Team Manager will call and chair a War Room. The telephone number for the War Room will be the Fujitsu Conferencing Number owned by the RMGA Service Delivery Management Team Manager. The Chairman will enter the call prior to the attendance of other callers and enter a designated PIN, allowing direct entry for subsequent callers.

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

FUJ00080109



# 7 Formal Incident Closure & Major Incident Review

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 impact to the business, during and after the Incident and agree number of branches impacted and duration of Major Incident.
3. To confirm the end-to-end recovery process & timeline and identify that all documented processes were followed.
4. To analyse the management of the Incident & the effectiveness of the governance process.
5. To identify corrective actions to:
   i. prevent recurrence of Incident
   ii. minimise future business impact
   iii. improve 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. The agreed impact of Major Incident must be sent to Branch Network Service Delivery 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. 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: \\ATCFS7\POcust_serv\01Public\Major Incident Management \Templates

It is critical that the number of branches impacted and the duration of the Major Incident is agreed at the Major Incident Review and this agreement must come from POL. If for some reason POL is not present at the Major Incident Review meeting, a separate conversation must take place. This information is required because Major Incidents affect Counter Availability and Liquidated Damages (LDs) are paid on Counter Availability as detailed in 7.1 below.

## 7.1 Calculating Liquidated Damages payable on Major Incidents.

Liquidated damages are payable on Major Incidents which qualify as Failure Events as detailed in the Branch Network Service Description (SVM/SDM/SD0011). 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 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 Services to agree the number of Branches and Counter Positions affected and the duration of the outage;

The duration of the Incident must be agreed with Post Office & 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 |
|---|---|

FUJ00080109



| | |
|---|---|
| 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 |

FUJ00080109



# 8 Fujitsu Services Roles and Responsibilities

This section defines the roles and responsibilities individuals and teams have with regard to the Major Incident Escalation Process.

## 8.1 Horizon Service Desk

### 8.1.1 Role of the HSD in a Major Incident

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

* Receive & log calls from the Post Masters, and communicate the progress of investigations to any PMs who call into the desk.

* The HSD should also complete the "HSD Impact" template and forward to the RMGA CS Service Delivery Manager, who is managing the Incident. This template should be completed every 15mins from the point of declaring Major Incident, until the RMGA SDM asks for this to cease. The Service Delivery Manager / Owner will provide the Summary of Incident to be included in the template.

### 8.1.2 HSD Templates

| NAME OF TEMPLATE | LOCATION | DESCRIPTION / NOTES | DISTRIBUTION |
|---|---|---|---|
| Impact on HSD | \\ATCFS7\POcust_serv\01Public\Major Incident Management \Templates | This template is used to communicate the impact of a Major Incident to RMGA Service Management (Service Delivery.) The template can be copied to email. | RMGA Service Delivery Manager |

FUJ00080109



## 8.2 Service Delivery Manager / Owner

Throughout this document the term Service Delivery Manager refers to the RMGA owner of the Service impacted, and is not limited to a manager working as part of the Service Delivery Team.

### 8.2.1 Role of the Service Delivery Manager / Owner in Major Incident

The primary role of the Service Delivery Manager / Owner 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 & effective as possible. The Incident Manager acts as the central point for communication and non-technical information flow, allowing the Recovery Manager to focus on the technical & the resolution of the Incident. The Service Delivery Manager / Owner is also responsible for creating and maintaining all the associated documentation.

The Service Delivery Manager:

* Has responsibility for creating the Major Incident documentation: Major Incident Report

* Manages the communication, internally within Royal Mail Group Account (RMGA).

* Communicates progress of Incident with POL SCT

* Identifies Business & Service impact, though discussions with the users, POL SCT & HSD – providing this input into the Major Incident Conference Call.

* Calls & chairs the MI conference call

* Produces & distributes the MI conference call minutes.

* Liaises with SSC to update the Service Portal / updates the Service Portal

Following resolution of the Incident the Service Delivery Manager / Owner schedules and chairs the Major Incident Review and creates the Major Incident Report Document. 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, then the POL Security team will receive a copy of the report.

FUJ00080109



## 8.2.2 Service Delivery Templates

| NAME OF TEMPLATE | LOCATION | DESCRIPTION / NOTES | DISTRIBUTION |
|---|---|---|---|
| Notification of Major Incident | \\ATCFS7\POcust_serv\01Public\Major Incident Management \Templates | Used to communicate the key information as requested by POL.<br>***THIS MUST BE EMAILED WITHIN 15 MINS OF MAJOR INCIDENT INVOCATION.*** | POL<br>RMGA Service Support & Service Delivery<br>RMGA Head of Service Management<br>RMGA Head of CS |
| Major Incident Report Template | \\ATCFS7\POcust_serv\01Public\Major Incident Management \Templates | The Major Incident Report contains all the information about a Major Incident. This document is distributed to POL. | POL<br>RMGA Service Support & Service Delivery<br>RMGA Head of Service Management<br>RMGA Head of CS |
| MI Conference Call Agenda | \\ATCFS7\POcust_serv\01Public\Major Incident Management \Templates | Used to provide structure to the MI Conference Call and ensures that all relevant information is collected. | Attendees of MI CONFCALL<br>RMGA Service Support & Service Delivery<br>RMGA Head of Service Management<br>RMGA Head of CS |
| MI Conference Call Minutes | \\ATCFS7\POcust_serv\01Public\Major Incident Management \Templates | Ensures that minutes from the MI Conference Call are produced in a consistent format, and that all attendees are aware of actions & status of recovery.<br>Aids communication | Attendees of MI CONCALL<br>RMGA Service Support & Service Delivery<br>RMGA Head of Service Management<br>RMGA Head of CS |
| Major Incident Review Agenda | \\ATCFS7\POcust_serv\01Public\Major Incident Management \Templates | Standard format for Major Incident Review & ensures that all areas are addressed. | Attendees of MIR<br>RMGA Service Support & Service Delivery<br>RMGA Head of Service Management<br>RMGA Head of CS |
| Major Incident Review Minutes | \\ATCFS7\POcust_serv\01Public\Major Incident Management \Templates | Standard format for Major Incident Review minutes. Ensures that information is collected in correct format for inclusion in other reports / to be taken to Service Review. | Attendees of MIR<br>RMGA Service Support & Service Delivery<br>RMGA Head of Service Management<br>RMGA Head of CS |

FUJ00080109



## 8.2.3 Service Delivery Activities

This template can be printed out and used as a checklist during a Major Incident.

| Incident Management Timeline | | Service Delivery Manager Activities |
|---|---|---|
| Incident + 0 mins | Incident identified | ☐ Invoke Major Incident<br><br>Documentation<br><br>☐ Open Major Incident Report (tfs number, start timeline)<br>☐ Save Major Incident Report on central server.<br>☐ Open Service Portal Incident<br>☐ Prepare Notification of Major Incident template<br><br>Communication<br><br>☐ Ensure HSD / SMC is aware of Incident & request HSD Impact template to be completed. Provide Incident Summary details for HSD / SMC to add to the template<br>☐ Inform POL<br>☐ Escalate to RMGA management<br>☐ Send alert SMS |
| Incident + 15 mins | | ☐ Determine Business impact (impact on transactions, & branches.)<br>☐ Calls MI Conference Call<br><br>Documentation<br><br>☐ HSD Impact template received.<br>☐ Information added to POL Major Incident invocation template.<br>☐ Email completed POL Major Incident invocation template to POL<br>☐ Update Major Incident Report<br>☐ Update Service Portal<br><br>Communication<br><br>☐ Send update SMS (including time of MI Conference Call – if applicable) |
| Incident + x mins | MI Conference Call | ☐ Chairs MI Conference Call<br><br>Information Required<br><br>☐ HSD impact including Business impact (impact on branches / counters & transactions) |
| Incident + x mins<br><br>MI CONCALL + 15 mins | Post MI Conference Call | ☐ Creates & distributes the MI Conference Call Minutes<br>☐ Save copy of MI Conference Call Minutes on central server<br><br>Documentation<br><br>☐ Update Major Incident Report (timeline & impact)<br>☐ Update Service Portal<br><br>Communication<br><br>☐ Send update SMS |
| To be repeated following every MI Conference Call | | |
| Incident + x mins<br><br>(Within 24hrs) | Post recovery | Documentation<br><br>☐ Update Major Incident Report & save on server.<br>☐ Email draft Major Incident report to POL<br>☐ Update Service Portal Incident<br>☐ Schedule follow up MI Conference Call to ensure that recovery has been effective & that Incident is resolved. |

FUJ00080109



| | | |
|---|---|---|
| | | Communication<br><br>☐ Ensure HSD is aware of Incident resolved / downgraded to BAU.<br>☐ Cease completion of HSD Impact template.<br>☐ Inform POL / RMGA Management of Incident Status<br>☐ Send closure SMS |
| Incident + 24hrs | | ☐ Schedule MI Review and distribute agenda<br>☐ Chair MI Review<br>☐ Track Corrective Actions<br><br>Documentation<br><br>☐ Update Major Incident Report & save on server.<br>☐ Email Major Incident report to POL |
| Incident + 48hrs | Major Incident Review | ☐ Chair Major Incident Review<br>☐ Agree timescales and number of branches impacted as required for HNG-X LD payments |
| Incident + 48hrs | Post Major Incident Review | ☐ Create Major Incident Review Minutes and save to central server.<br>☐ Distribute Major Incident Review Minutes.<br>☐ Add corrective actions to the "corrective actions spreadsheet" |

FUJ00080109



# 8.3 Service Support Manager – Recovery Manager

## 8.3.1 Role of the Service Support Manager in Major Incident

The primary functions of the Service Support Manager is to act as Recovery Manager and to co-ordinate and manage the restoration of Service, focusing on the technical teams and acting as the communication point for the technical teams and 3rd parties.

The Service Support Manager:

* Manages the technical recovery of the Incident – liaising with SDUs & Third Parties.

* Provides updates on the recovery, when technicians / representatives of technical teams are unable to attend the MI Conference Call.

* Is the only person to liaise directly with the technical teams, including technical third parties.

* Ensures that technical investigative actions are tracked and completed.

* Tracks technical corrective actions through Service Review meetings

In the event of a central infrastructure Major Incident with no impact on the business, the SDM will not be involved and the SSM will be responsible for chairing any meetings / creation of documentation.

Service Support may well feel the need to schedule a Technical Conference Call, which will have a technical focus.

## 8.3.2 Service Support Templates

| NAME OF TEMPLATE | LOCATION | DESCRIPTION / NOTES | DISTRIBUTION |
|---|---|---|---|
| Technical Update for MI Conference Call | \\ATCFS7\POcust_serv\01Public\Major Incident Management \Templates | Contains technical information which should be brought to the MI Conference Calls | None |

FUJ00080109



### 8.3.3 Service Support Activities

This template can be printed out and used as a checklist during a Major Incident.

In the event that there is no business impact, the Service Support Manager will assume the documentation responsibilities.

| Incident Timeline | Management | Service Delivery Manager Activities |
|---|---|---|
| Incident + 0 mins | Incident identified | ☐ Invoke Major Incident<br>☐ Ensure that Data Centre Ops are running ping scripts (every 15 mins from each DC)<br>☐ Contact Technical Teams for update.<br>☐ Agree next update point with Technical Team (if not MI Conference Call) |
| Incident + x mins | MI Conference Call | ☐ Provide technical input into the MI Conference Call if technical teams are unavailable. |
| Incident + x mins<br><br>MI CONCALL + 15 mins | Post MI Conference Call | ☐ Complete actions assigned to Service Support<br>☐ Ensure that SDUs complete actions. |
| To be repeated for every MI Conference Call | | |
| Incident + x mins<br><br>(Within 24hrs) | Post recovery | ☐ Ensure that all Technical teams are aware that the Incident has been resolved / downgraded. Thank teams for their effort.<br>☐ Provide input into update of Major Incident Report. |
| Incident + 48hrs | Major Incident Review | ☐ Attend Major Incident Review |
| Incident + 48hrs | Post Major Incident Review | ☐ Add corrective actions to the "corrective actions spreadsheet" to be tracked through Service Review meetings.<br>☐ Ensure SDUs complete MI Corrective Actions |

FUJ00080109



# 8.4 SDUs: Technical Teams / Third Parties

## 8.1.1 Role of the SDUs: Technical Teams / Third Parties during a Major Incident

The role of the Technical Teams / Third Parties during a Major Incident 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 Service Support Manager (Recovery Manager.)

The Technical Teams / Third Parties should send an attendee to the MI Conference Call and following resolution to the Major Incident Review meeting. Where attendance on the MI Conference Call is not possible, a full update MUST be provided to the Service Support Manager to ensure that that the Bridge can be updated.



## 8.1.2 Technical Teams Templates

This template has been designed to assist the technical teams / Third Parties in compiling the information required for a MI Conference Call.

| NAME OF TEMPLATE | LOCATION | DESCRIPTION / NOTES | DISTRIBUTION |
|---|---|---|---|
| Technical Update for MI Conference Call | \\ATCFS7\POcust_serv\01Public\Major Incident Management \Templates | Used to provide structure to the MI Conference Call and ensures that all relevant information is collected. | Not for distribution |

FUJ00080109



# 9 Post Office / Fujitsu Services Interfaces

The Post Office / Fujitsu Services interfaces are all detailed in the Process Description, section 5.1, however for ease the interfaces have been extracted into the table below.

| Stage in Process | Description of Interface | Timescales | FJS Owner |
|---|---|---|---|
| Major Incident Triggers Met? | POL SCT will be informed by the Service Delivery Manager / Owner managing the Major Incident of the incident.<br>SMS will be sent to RMGA Management alerting to the potential existence of a Major Incident. | T+3<br>T+5 | RMGA SDM / Owner (Duty Manager)<br>HSD / SMC (out of hours) |
| BAU Incident | POL SCT will be informed that there is no Major Incident<br>SMS sent | As appropriate | RMGA SDM / Owner (Duty Manager)<br>HSD / SMC (out of hours) |
| Incident Investigation & diagnosis | POL invited to Major Incident Bridge | T+5 | RMGA SDM / Owner (Duty Manager) |
| Major Incident Bridge | POL attendance on MI Bridge | T+15 | N/A |
| MI Minutes distributed | POL recipient of the MI Bridge Minutes | MI Bridge +15 | RMGA SDM / Owner (Duty Manager) |
| As determined on MI Bridge / in person with POL | Regular SMS / phone updates to POL SCT | As determined on MI Bridge / in person with POL | RMGA SDM / Owner (Duty Manager) |
| War Room | POL attendance at War Room | Timescale dependant on impact and nature of incident & progress of resolution. | RMGA SDM / Owner (Duty Manager) |
| Incident Resolution | POL attendance on conference call<br>SMS sent | | RMGA SDM / Owner (Duty Manager)<br>HSD / SMC (out of hours) |
| Major Incident Draft Report | POL sent MI draft report including Security for PCi Major Failures | MI + 24hrs | RMGA SDM / Owner (Duty Manager) |
| Major Incident Review & formal Incident Closure | POL attendance at Major Incident Review | MI + 48hrs | RMGA SDM / Owner (Duty Manager) |



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

FUJ00080109



# 10 Appendices

## 10.1 List of Templates

All templates are stored on the central share. : \\ATCFS7\POcust_serv\01Public\Major Incident Management \Templates

| NAME OF TEMPLATE | DESCRIPTION / NOTES | DISTRIBUTION |
|---|---|---|
| Impact on HSD | This template is used to communicate the impact of a Major Incident to RMGA Service Management (Service Delivery.) | RMGA Service Delivery Manager |
| Notification of Major Incident | Used to communicate the key information as requested by POL.<br>***THIS MUST BE EMAILED WITHIN 15 MINS OF MAJOR INCIDENT INVOCATION.*** | POL<br>RMGA Service Support & Service Delivery<br>RMGA Head of Service Management<br>RMGA Head of CS |
| Major Incident Report Template | The Major Incident Report contains all the information about a Major Incident. This document is distributed to POL. | POL<br>RMGA Service Support & Service Delivery<br>RMGA Head of Service Management<br>RMGA Head of CS |
| MI Conference Call Agenda | Used to provide structure to the MI Conference Call and ensures that all relevant information is collected. | Attendees of MI CONCALL<br>RMGA Service Support & Service Delivery<br>RMGA Head of Service Management<br>RMGA Head of CS |
| MI Conference Call Minutes | Ensures that minutes from the MI Conference Call are produced in a consistent format, and that all attendees are aware of actions & status of recovery.<br>Aids communication | Attendees of MI CONCALL<br>RMGA Service Support & Service Delivery<br>RMGA Head of Service Management<br>RMGA Head of CS |
| Major Incident Review Agenda | Standard format for Major Incident Review & ensures that all areas are addressed. | Attendees of MIR<br>RMGA Service Support & Service Delivery<br>RMGA Head of Service Management<br>RMGA Head of CS |
| Major Incident Review Minutes | Standard format for Major Incident Review minutes. Ensures that information is collected in correct format for inclusion in other reports / to be taken to Service Review. | Attendees of MIR<br>RMGA Service Support & Service Delivery<br>RMGA Head of Service Management<br>RMGA Head of CS |
| Technical Team Update to MI CONCALL | The technical teams / third parties are responsible for updating the MI Conference Call with<br>☐ Input into the Incident Timeline<br>☐ Service & Infrastructure impact<br>☐ Risk & Impact assessment of recovery actions<br>☐ Progress against recovery actions / investigation.<br>☐ Provide update from third parties from which the technical teams / third parties are responsible for. | Not distributed – to assist in preparation for the MI CONCALL. |

FUJ00080109



# 10.2 Service Delivery Managers, Areas of Responsibility & Contact Details.

**All alerts to be raised to Service Manager within 3 minutes**

**OOH Duty Manager Pager (GRO) is to be used between the hours:**

**17.30 - 09.00 Monday to Thursday**

**17.00 - 09.00 Friday**

**24 hour i.e. all day Saturday/Sunday**

Outside of these times, please use the contacts list below

| AREA OF RESPONSIBILITY | EXAMPLE INCIDENTS | ESCALATION TO: | CONTACT DETAILS | BACK UP |
|---|---|---|---|---|
| **Infrastructure issues**.<br><br>NT / UNIX / Data Centres<br><br>All network issues | Network Incidents<br><br>Data centre issues<br><br>Storage Incidents<br><br>NT /UNIX Incidents | **Ian Mills/Claire Drake** | **GRO** | Kirsty Gallacher<br><br>GRO |
| **Banking and Online Services** (Inc: DVLA, Debit Card, EPAY) | Online Service outages | **Mike Stewart**<br><br>1st point of contact | Pager<br><br>GRO<br><br>Mobile<br><br>GRO | Kirsty Gallacher<br><br>3rd Point of Contact<br><br>GRO |
| **Banking and Online Services** (Inc: DVLA, Debit Card, EPAY) | Online Service outages | **Mike Woolgar**<br><br>2nd point of contact | Pager<br><br>GRO<br><br>Mobile<br><br>GRO | Kirsty Gallacher<br><br>3rd Point of Contact<br><br>GRO |
| **Reference data escalations** | New product not functioning | **Dave Wilcox** | GRO | **Kevin Mckeown**<br><br>GRO |
| **APS/TPS/SAP/POLFS, LFS** | Files Not delivered, Data Transfer | **Mike Stewart**<br><br>1st Point of Contact | Pager<br><br>GRO<br><br>Mobile<br><br>GRO | Kirsty Gallacher<br><br>3rd Point of Contact<br><br>GRO |
| **APS/TPS/SAP/POLFS, LFS** | Files Not delivered, Data Transfer | **Mike Woolgar**<br><br>2nd point of | Pager<br><br>GRO | Kirsty Gallacher<br><br>3rd Point of Contact |

FUJ00080109



| | | | | |
|---|---|---|---|---|
| | | contact | Mobile<br>GRO | GRO |
| **Business Continuity** | Invoking business continuity incident | **Adam Parker** | GRO | Kirsty Gallacher<br>GRO |
| **Engineering** | Major issue with engineering service | **Leighton Machin**<br>1st Point of contact | GRO | Sarah Bull<br>3rd Point of Contact<br>GRO |
| **Engineering** | Major issue with engineering service | **Susie Appleby-Robbins**<br>2nd Point of Contact | GRO | Sarah Bull<br>3rd Point of Contact<br>GRO |
| **Branch services** | Potential environmental issues at individual branches | **Nick Crow** | GRO | Kirsty Gallacher<br>GRO |
| **OBC Escalations** | OBC job going wrong/ press involved /unhappy postmaster | **Ian Venables** | GRO | Chris Bourne<br>GRO |
| **Major software problem** | Major software problem | **Tony Little** | GRO | John Simpkins<br>GRO |
| **HSD/SMC/PostShops** | Major Powerhelp call logging issues. Major PostShop outage | **Sandie Bothick** | GRO | Sarah Bull<br>GRO |
| **Security** | Security Issues<br>Virus Alerts | **Tom Lillywhite** | GRO | Bill Membury<br>GRO |
| **Release Management / Service Introduction** | Issues caused by Releases | **Sarah Bull** | GRO | Gaeten Van Achte<br>GRO |
| | | | | |

FUJ00080109



## 10.3 Escalation Communication Protocol

The primary principle:

**Up"**

**and**

**"Across**

**Escalation protocol:**

| Fujitsu; Service Owners | SCT / Problem Managers |
|---|---|
| Service Delivery Team Manager | Service Improvement Manager |
| Head of Service Management | Supplier and Service Performance Manager |
| Customer Service Director | Head of Network Support / IT Director |



## 10.4 Major Business Continuity Incidents (MBCI)

For Horizon the MBCI triggers are listed in:

- Horizon Services Business Continuity Plan (CS/PLA/079)
- Horizon Support Services Business Continuity Plan (CS/PLA/080)
- Horizon Service Desk Business Continuity Plan (CS/PLA/015).

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.

## 10.5 Security Major Incidents

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

FUJ00080109



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