POL00001538

Document Date: 25/02/2009		Document Type	L/001
Version	0.38	Ref. Number	CON/MGM/006

Operations Directorate

SERVICE DELIVERY

POST OFFICE LIMITED

MAJOR INCIDENT MANAGEMENT PROCESS

Author: Gary Blackburn
Live Service & Business Continuity Manager

Sponsor: Dave Hulbert
Systems & Direct Channels Manager

Authoriser: Andy McLean
Head of Service Delivery

Document Control

0.1 Version History

Version	Dated	Change Details
0.1	01.08.2002	First version of Crisis Management Team High Level procedures – base-lined document.
0.2	25.01.2005	Updated following an internal formal review of Crisis Management procedures within Post Office Ltd.
0.3	01.02.05	Updated following internal review comments.
0.4	24.02.05	Updated following formal review .
0.5	24.03.2005	Updated following internal review comments.
0.6	25.03.2005	Updated following internal review comments.
0.7	07.04.2005	
0.8	07.04.2005	
0.9	19.04.2005	Updated with additional contact details for PR Team.
0.10	10.05.2005	General Manager Service details added to BPT
0.11	06.09.2005	Updated changes to contact details
0.12	01.11.2005	Updated changes to contact details
0.13	13.12.2005	Updated with additional contact details for BPT Team.
0.14	21.12.2005	Updated with details of Blackberry users and contact details.
0.15	05.01.2006	Updated to incorporate and align flowchart to EBT protocol process.
0.16	12.01.2006	Reference to POL Business Continuity database included at appendix G.
0.17	13.01.2006	Updated changes to contact details
0.18	23.01.2006	Updated changes to contact details
0.19	23.02.2006	Updated changes to contact details
0.20	08/03/2006	Updated changes to contact details
0.21	10/03/2006	Updated changes to contact details
0.22	24/03/2006	Updated changes to contact details
0.23	06/04/2006	Document updated to take account of changes to structure in Operations Control.
0.24	12/04/2006	Updated changes to contact details

Document Date: 25/02/2009		Document Type	L/001
Version	0.38	Ref. Number	CON/MGM/006

Version	Dated	Change Details
0.25	26/04/2006	Updated changes to contact details
0.26		Updated to take account of changes to structure due to Organisational Design Review
0.27		Update Appendix E blackberry Users
0.28	30/01/07	Update new members of the Major Incident Escalation Group
0.29	21/03/07	Update new members of the Major Incident Escalation Group & business Protection Team
0.30	01/04/07	Update new members of the Major Incident Escalation Group & Business Protection Team
031		Update Contact details and Blackberry Users. Update following comments from Adam Martin.
032	14/04/2008	Update contact details of the Business Protection Team and Blackberry Users
0.33	28/04/2008	Update contact details of the Business Protection Team
0.34	30/04/2008	Update contact details of the Major Incident Escalation Group
0.35	06/05/2008	Update members of the Major Incident Escalation Group
0.36	06/06/2008	Update contact details in Appendix A
0.37	11/08/2008	Change of name for Operations Control to Service Delivery. Update membership of Business Protection Team and Major Incident Escalation Group
0.38	24/02/2009	Added Telephone Conference call etiquette at Appendix I & new POL Payment Card Industry Major Incident Response Appendix J

0.2 Document References

REF:	DOCUMENT REF.	TITLE	VERSION	DATE
1	POL/HNG/PLA/001	PCI Incident Response Plan	0.3	29/02.08

2	S15	RMG Information Security Incident Response Policy (S15)		
3	PCI DSS	Payment Card Industry Data Security Standard	1.1	Sept 2006

0.3 Distribution List

Name	Title	Team
Gary Blackburn	Business Continuity Manager	Service Delivery
Dave Hulbert	Systems & Direct Channels Manager	Service Delivery
Andy McLean	Head of Service delivery	Service Delivery
Mike Young	Operations Director	Operations Directorate

0.4 Document and Change Control

The Service Delivery Change Control Team is responsible for maintaining and changing all the documentation created in Service Delivery. For further information on existing documentation and procedure please contact the Change Control Manager.

0.5 Glossary

Abbreviation	Description

Abbreviation	Description
BPT	Business Protection Team – Empowered senior management group within Post Office Ltd that would manage a lower severity major incident under the coordination of the Live Service Team.
Card Schemes	Means those companies that produce payment cards (credit or debit) e.g. Mastercard, VISA, American Express, Diners Club, JCB etc
EDS	Electronic Data Systems –supplier of the Post Office Card account
EBT	Electronic Benefits Transfer – Core Banking sub system provided by JP Morgan on behalf of Citigroup, which sits in the overall post office card account system infrastructure provided to PO Ltd by EDS.
FE	Forensic Expert. An investigator who has expertise examining computer systems for evidence of malicious activity. For the PCI Incident Response Plan such investigators must be approved by the Card Schemes otherwise they must not be engaged to investigate a PCI Incident.
LST	Live Service Team – team[s] within Service Delivery that coordinate the management of the POL Major Incident Management Process.
Merchant Acquirer	An organisation, usually a bank, that contracts with one or more Card Schemes to engage and contract with merchants who will accept payment for goods or services by a payment card (credit or debit)
MIEG	Major Incident Escalation Group – top-level management group [e.g. Board of Directors], which would manage a high severity impact incident under the coordination of the Live Service Team.
POL	Post Office Ltd
MBCI	Major Business Continuity Incident

0.6 Contents

1. Introduction

The Post Office Ltd Major Incident Management process is owned and managed by the Live Service & Business Continuity Team within Service Delivery.

Incidents impacting PO Ltd are managed using a three level management structure. The involvement of each level is influenced by the severity of the incident.

2. Purpose

The purpose of this document is to define:

- roles and responsibilities in managing an incident and the methods by which management will be notified that a] an incident has occurred and b] that their involvement will be required
- the types of incidents likely to result in the invocation of Major Incident Management procedure
- the procedures that will be used by Post Office Ltd [POL] should a major incident occur.

3. Roles and Responsibilities

There are three levels of management within PO Ltd who may be called upon to participate in the management of an incident, as follows:

Level 1 - PO Ltd Live Service team [Service Delivery]
All incidents and problems impacting live service within PO Ltd are reported into, controlled by and managed within this team. If appropriate, this team will communicate to the PO Ltd Business Protection Team and the Major Incident Escalation Group to inform them of an incident and/or to request their input. Appendix A includes the Service Delivery contacts.

Level 2 - PO Ltd Business Protection Team [Business wide working group]
This team consists of empowered business representatives from across PO Ltd. These business area 'experts' are available at all times and will be used to

support, inform and influence the management of a medium/high severity incident. They will be notified of all medium/high severity incidents via email or SMS text from the PO Ltd Live Service team. If required to participate in the management of a medium/high severity incident they will be contacted by SMS or telephone and provided with meeting details and a conference call number. The conference call will be operated as a Virtual Operations Room, see Appendix D BPT members are listed at Appendix A. A detailed set of BPT responsibilities is included at Appendix B.

Level 3 - Major Incident Escalation Group [Business Directors]
This group consists of Business Directors and some direct reports. They will be notified of all medium/high severity incidents via email from the PO Ltd Live Service team. If required to participate or lead the management of a medium/high severity incident they will be contacted by SMS or telephone and provided with meeting details and a conference call number. The conference call will be operated as a Virtual Operations Room, see Appendix D. The MIEG members are listed at Appendix A, page 18. A detailed set of MIEG responsibilities is included at Appendix C .

Blackberry Users can be found at Appendix E

The following table summarises involvement and communication:

	Incident severity / action		
Management Level	Low	Medium	High
Level 1 – Service Delivery teams	• Identified by Live Service Team [LST] • Immediate incident impact managed by LST. • Resolution managed by Service Improvement Team [SIT]. • Reporting via daily text updates within Service Delivery for incident duration.	• Incident identified by LST. • LST communicate incident detail to BPT and MIEG for information via email. • LST contact relevant BPG members by telephone to formulate action plan and to join working group [if required].	• Incident identified by LST. • LST contact relevant BPT members by telephone to join a conference call and assess the incident. • LST communicate incident detail to BPT and MIEG for information via email. • LST co-ordinate incident management and resolution, working with BPT and MIEG.
Level 2 -	• No	• Receive communication	• Receive communication

	Incident severity / action		
Management Level	Low	Medium	High
Business Protection Team	involvement.	from LST detailing the incident via email. This is supported by a text message notifying BPT that an incident is occurring. • LST contact BPT by telephone to seek input to action plan to resolve incident and form part of a working group [if required].	from LST detailing the incident via email. This is supported by a text message notifying BPT that an incident is occurring. • LST contact BPT by telephone to seek input to action plan to resolve incident and form part of a working group [if required].
Level 3 - Major Incident Escalation Group	• No involvement.	• Receive communication from LST by email detailing the incident. • Receive copies of the action plan developed by the working group [LST plus selected BPT members]. This comes from the LST via email. • Receive progress updates through to resolution from LST via email and/or text message.	• Receive communication from LST by email / text detailing the incident. • LST contact MIEG members by text/telephone requesting attendance on a conference call. LST will provide conference call details. • MIEG members then lead/direct Major Incident Management with LST acting as secretariat. LST will co-ordinate associated action plan through to resolution.

4. Major Incident Definition

‘An incident that has an immediate and/or potentially prolonged adverse impact on one, some or all of the following: PO Ltd Branches, POL employees , customers, clients or PO Ltd brand image’.

It is difficult to precisely define a Major Incident due to the number of variables that have to be considered as part of the impact assessment when an incident occurs. Such factors include time of day, business climate, day of week and time of year. Figure 2 provides a summary of these variables plus the components that combine to deliver key PO Ltd services. A failure in any of these *could* impact live service leading to a major incident.

Major IT suppliers to PO Ltd – Fujitsu Services, EDS and CSC - are currently re-defining major incident trigger points. These will be included in future versions of this document to further assist in Major Incident definition.

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 PO Ltd. Typically these incidents will initially require a significant amount of reactive management before they can then be controlled and resolved.
- ***Medium*** – an incident which has the potential to impact PO Ltd but which can be controlled and mitigated against through effective management
- ***Low*** – an incident that requires business attention but which if managed effectively will not have significant impact on PO Ltd.

To provide further guidance, a number of scenarios together with the resulting business impact are now defined. The level of management input is also clarified.

Scenario 1 Central London transport network security alert.

A major security alert on the tube network could during core business hours could have an immediate impact on our people in Administration sites, branches and the Supply Chain operation. Depending on the scale of the incident, there could be post office branch closures, disruption to transport routes, exclusion zones, and difficulties getting to and from work.

Conclusion: High Impact
Management Involvement: MIEG [Level 3]

Scenario 2 Electronic Benefits Transfer system failure during core business hours on a Monday.

EBT is the core banking sub-system provided by JP Morgan Electronic Financial Services Inc., which sits within the overall post office card account system infrastructure provided to Post Office Ltd by EDS. The EBT system authorises post office card account withdrawals and holds core data for the post office card account.

A failure of the EBT system, or an issue that required EBT to be taken offline during core business hours would have an immediate high profile business impact across the whole network because post office branches would not be able to perform card account transactions – one of the key product areas. This failure would have political sensitivity and potentially long recovery times.

Conclusion: High Impact
Management involvement: MIEG [Level 3]

Scenario 3. Industrial Action in Supply Chain.

Industrial Action within Supply Chain would impact on the ability of Post Office Ltd to maintain the delivery and collection of cash to, potentially, all post office branches. This could impact on all key product areas.

Conclusion: High Impact
Management involvement: MIEG [Level 3]

Scenario 4. Broadband Access Server Failure.

A Broadband Access Server [BAS] router is a component of the Fujitsu Services managed service supporting on-line services at Asymmetric Digital Subscriber Line [ADSL] connected post office branches.

A failure of a BAS router during core business hours would result in an on-line service failure to all branches attached to the failed BAS router for between one and two hours. This would typically impact between one and three hundred post office branches in a dispersed geographical area.

Conclusion: Medium Impact
Management involvement: LST and BPG [Levels 1 and 2]

Scenario 5. Automated Payment File Transfer Failure.

Automated Payment files detail payments made by customers at post office branches. The files are delivered overnight to clients by Fujitsu Services.

A failure in the delivery of the file[s] would have some impact on customers, post office branches and helplines, as clients will not have received details of AP payments made by customers at post office branches the previous working day. This impact would be relatively low.

There may also be financial penalties if POL are non-compliant to service delivery timescales.

Conclusion: Low / Medium Impact
Management involvement: LST and BPG [Levels 1 and 2]

Scenario 6. Generator Failure at Future Walk, Chesterfield.

A failure of the generator at Future Walk would have no immediate business impact.

There would be a loss of resilience in the event of a power failure scenario at Future Walk.

Conclusion: Low Impact
Management involvement: LST [Level 1]

Scenario 7. Payment Card Data Compromise at Data Centre.

Payment Card data (or Cardholder data) may include the 16 digit card account number, account name, expiry date, security code(s), amongst other information which may be stored on a payment card.

A suspected compromise of this data at a data centre will invoke certain obligations on POL under existing contracts with the Merchant Acquirer(s). Foremost is an investigation that which must include a complete forensic examination of all potentially affected systems and processes. This investigation is mandatory on POL. In order to complete their investigation the Forensic Examiners (FE) may require that the data centre be disconnected from all external networks and that affected systems be disconnected from all adjacent systems.

The investigation would also require a forensic copy be made of relevant data (process data, logs and audit records).

The affected data centre might not be reconnected until the investigation is complete which may take several weeks.

There may also be significant financial penalties if POL are non-compliant to the Card Schemes security standard (PCI DSS) and/or if Cardholder data is found to be compromised.

Conclusion: High Impact
Management involvement: MIEG [Level 3]

Figure 2: Service outages: Impact assessment pick-list

Factors to consider that overlay service failures and influence severity and impact

Influencing factors	Time of Year - Xmas and after Bank holidays are key for Benefit payments
	Time of day - early mornings and lunchtimes are busy times for Branches
	Scale of outage - clearly the greater the number of Branches affected, the higher the impact
	Geographical dispersion - clusters of affected Branches in the same location increases impact
	Business initiatives - impact greater if business has a campaign that is affected by the outage
	Duration - anything more than an hour becomes really high impact

Key Product areas	**Key components supporting service delivery**	
Bill Payments and Post Office Savings Products	Branches open	CSC Northern Data Centre
	Branch counter and equipment	Pin Pads
	FS Data Centres	Ingenico interface with Fujitsu
	Comms links from Branch to Data Centre	Ingenico call centre
	Overnight file transfer	DVLA interface with FS
	EDG and APADC service	E-Pay interface with FS
	Stores availability - pouches	Stock availability
	Cash supplied	
Banking and Insurance Personal Banking Cash Withdrawals Loans Motor Insurance Home Insurance Credit Cards	Branch counter and equipment	Branches open
	FS Data Centres	Pin Pads
	Comms links from Branch to Data Centre	POL FS
	Overnight file transfer	EDS Call Centre
	FS interface with Streamline	FS interface with A&L
	FS interface with EDS	FS interface with LINK
Mails Products High Margin Postage High Margin Postage Labels Special Delivery	Branches open	Pin Pads
	Branch counter and equipment	Cash supplied
	FS Data Centres	Counter printers
	Comms links from Branch to Data Centre	Stores availability - pouches
	Overnight file transfer	Stock availability
	EDG	
Travel Products Bureau de Change Travel Insurance	Branches open	FS interface with Streamline
	Branch counter and equipment	Cash supplied
	FS Data Centres	Foreign currency supplied
	Comms links from Branch to Data Centre	Stores availability
	Overnight file transfer	Stock availability
	Pin Pads	First Rate infrastructure
Telephone Products HomePhone Phonecards	Branches open	BT Stream call centre
	EDG and APADC service	CSC Northern Data Centre
	Stores availability	

Components which support all Products and Services

Support components	Sales MI system	P&BA settlement systems & processes
	Cash Centres	NBSC
	CIT depots	Post Office External Helpline

5. Major Incident Management process

In the event of a major incident, activities must be co-ordinated within the business in order to minimise adverse impact and protect service to both customers and clients.

The PO Ltd Live Service Team within Service Delivery is always the co-ordination point for this activity.

Depending on the severity of the incident, the PO Ltd Live Service Team will require the support of all or selected members of the POL Business Protection Team and/or the Major Incident Escalation Group to assist in the management of a major incident.

The process map at Figure 1 illustrates the sequence of events that take place when an incident occurs. Also illustrated at Figure 1 is the problem management process, which manages problems, which do not [or which no longer] require continual wider business involvement. The problem management process is owned and managed by the Service Improvement Teams in Service Delivery.

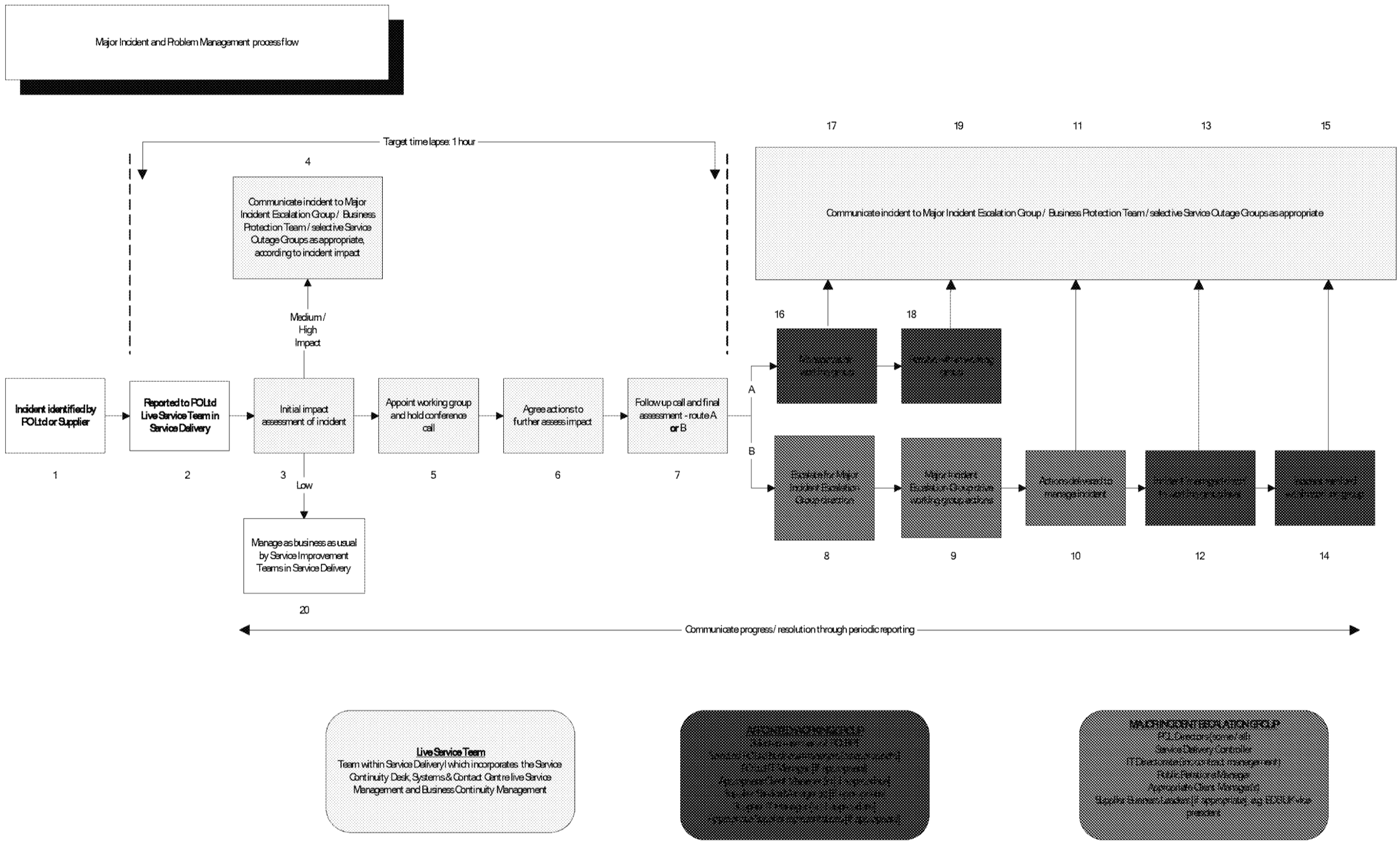
Figure 1 should be read in conjunction with the steps in the table on page 13.

In the case of a PCI Incident the initial steps will follow the process found in POL/HNG/PLA/001. That process will intersect at box 3 in the table on page 13. Note that the PCI Incident process contains additional requirements not found in this process and must therefore be used in parallel with this process.

Please note: where the process refers to the 'Working Group', this is made up of all or specified members of the POL Business Protection Team, as selected by the PO Ltd Live Service Team depending on the nature of the incident.

Document Date: 25/02/2009
Version 0.38

Document Type L/001
Ref. Number CON/MGM/006


Major Incident and Problem Management process flow
Target time lapse: 1 hour
4
Communicate incident to Major Incident Escalation Group / Business Protection Team / selective Service Outage Groups as appropriate, according to incident impact
Medium / High Impact
Incident identified by POLtd or Supplier
1
Reported to POLtd Live Service Team in Service Delivery
2
Initial impact assessment of incident
3
Low
Manage as business as usual by Service Improvement Teams in Service Delivery
20
Appoint working group and hold conference call
5
Agree actions to further assess impact
6
Follow up call and final assessment - route A or B
7
A
B
17
19
11
13
15
Communicate incident to Major Incident Escalation Group / Business Protection Team / selective Service Outage Groups as appropriate
16
18
Escalate for Major Incident Escalation Group direction
8
Major Incident Escalation Group drive working group actions
9
Actions delivered to manage incident
10
12
14
Communicate progress / resolution through periodic reporting
Live Service Team
Team within Service Delivery which incorporates the Service Continuity Desk, Systems & Contact Centre live Service Management and Business Continuity Management
MAJOR INCIDENT ESCALATION GROUP
POL Directors (some/all)
Service Delivery Controller
IT Directorate (incl contract management)
Public Relations Manager
Appropriate Client Manager(s)
Supplier Business Leaders (if appropriate) eg EDS UK vice president

POL00001538

Box	Title	Description	Key timescales	Action owner
1.	Incident identified	Incident identified – this may be from within PO Ltd, a supplier domain or other route. Operations Control man a 24x7 Technical Service Desk. [redacted]		
2.	Reported to PO Ltd Live Service team in Service Delivery	The incident is reported into the Live Service team in Operations Control from within PO Ltd, a supplier domain or other route.		
3.	Initial impact assessment of incident	An initial impact assessment of the incident is undertaken by members of the PO Ltd Live Service Team, taking into account impact on: • Live Service • Financial Integrity • Business Image	Within 15 minutes of incident reported.	PO Ltd Live Service Team
If the incident is low impact go to box 20. If the incident is medium to high impact proceed to box 4:				
4.	Communicate incident to MIEG and ALL WORKING GROUP MEMBERS	Details of the major incident are emailed to the full PO Ltd Business Protection Team and other interested parties [see Appendix A] An SMS text alert message is sent to advise that a major incident has occurred and that further detail has been sent out by email.	Within 5 minutes of the incident being assessed as medium to high impact.	PO Ltd Live Service Team
5.	Appoint working group and hold conference call	The PO Ltd Live Service Team appoints a working group to participate in the management of the incident. The working group will be made up of appropriate representatives from the Business Protection Team, relevant PO Ltd business/technical managers and appropriate representation from supplier domains [if appropriate]. An initial conference call is held.	Within 15 minutes of the incident being assessed as medium to high impact.	PO Ltd Live Service Team and appointed working group.
6.	Agree actions to further assess impact	**Conference Call 1**: An action plan is formulated and agreed. Time of next conference call is agreed.	Within 15 minutes of the incident being assessed as medium to high impact.	Appointed working group.
7.	Follow up call and final assessment – route A **or** B	**Conference Call 2**: Following feedback on actions	Within 15 minutes	Appointed

Box	Title	Description	Key timescales	Action owner
		further assessment of the situation takes place. A decision is then taken on whether to manage the incident within the appointed working group [route A] or escalate for Key stakeholder direction [route B]. **Please note**: Depending on the severity of the incident the decision to escalate may have already taken place.	of Conference Call 1.	working group.
If route A is chosen go to box 16. If route B is chosen proceed to box 8:				
8.	Escalate for MIEG direction	If the appointed working group are unable to provide a timely resolution to the incident, or the incident is of major severity, e.g. a card account incident that has no fix and requires EBT to be taken off line, it is escalated for MAJOR INDICENT ESCALATION GROUP direction, to ensure that PO Ltd Directors and Supplier Business Leaders [if appropriate] are involved in the decision making process. The nature of the incident determines which MIEG members are involved but it would include all or some of the following: • PO Ltd Director[s] • Supplier Business Leaders, e.g. vice president EDS UK. • Operations Controller • IT Directorate [including Commercial Management] • Public Relations Manager • Client Manager	Timescale dependant on impact and nature of incident.	PO Ltd Live Service Team
9.	MIEG drive working group actions	MIEG MEMBERS provide the appropriate direction on the incident resolution priorities.	Timescale dependant on impact and nature of incident.	Key stakeholders.
10.	Actions delivered to manage incident	Plan developed to resolve the incident with PO Ltd and other support teams as appropriate.	Timescale dependant on impact and nature of incident.	Key stakeholders.

Box	Title	Description	Key timescales	Action owner
11.	Communicate incident to MIEG and ALL WORKING GROUP MEMBERS	An update on current situation/status of the incident is emailed to the full PO Ltd Business Protection Team and other interested parties [see Appendix A]	Timescale dependant on impact and nature of incident.	PO Ltd Live Service Team.
12.	Incident 'managed down' to working group level	Plan agreed, scheduled and implemented to agreed timescales.	Timescale dependant on impact and nature of incident.	Appointed working group.
13.	Communicate incident to MIEG and ALL WORKING GROUP MEMBERS	An update on current situation/status of the incident is emailed to the full PO Ltd Business Protection Team and other interested parties [see Appendix A] **Please note**: Updates will be issued on a regular basis. – each update detailing the expected time of the next update.	Timescale dependant on impact and nature of incident.	PO Ltd Live Service Team.
14.	Incident resolved within working group	Verify incident is now resolved and can be closed.	Timescale dependant on impact and nature of incident.	Appointed working group.
15.	Communicate incident to MIEG and ALL WORKING GROUP MEMBERS	A final update on status of the incident is emailed to the full PO Ltd Business Protection Team and other interested parties [see Appendix A]	Timescale dependant on impact and nature of incident.	PO Ltd Live Service Team.
Route B [boxes 16 to 19]				
16.	Manage within working group	If the incident does not require senior management direction it can be managed through to resolution by the existing appointed working group.	Timescale dependant on impact and nature of incident.	Appointed working group.
17.	Communicate incident to MIEG and ALL WORKING GROUP MEMBERS	An update on current situation/status of the incident is emailed to the full PO Ltd Business Protection Team and other interested parties [see Appendix A] **Please note**: Updates will be issued on a regular basis. – each update detailing the expected time of the next update.	Timescale dependant on impact and nature of incident.	PO Ltd Live Service Team.
18.	Resolve within working group	Verify incident is now resolved and can be closed.	Timescale	Appointed

Box	Title	Description	Key timescales	Action owner
			dependant on impact and nature of incident.	working group.
19.	Communicate incident to MIEG and ALL WORKING GROUP MEMBERS	A final update on status of the incident is emailed to the full PO Ltd Business Protection Team and other interested parties [see Appendix A]	Timescale dependant on impact and nature of incident.	PO Ltd Live Service Team.
Low impact incident [continued from box 3]:				
20.	Manage as business as usual by problem management process.	Low impact incidents/problems are managed using existing business as usual processes by the Service Improvement Teams within Operations Control. **Please note: If a low impact incident/problem escalates to a medium/high impact, i.e. the initial impact worsens, then the incident would be reassessed and the process would return to step 3.**		

Testing the Major Incident Management Process

Testing of the Major Incident Management process will be undertaken quarterly in two formats:

- A workshop scenario test.

And

- A Business Protection Team member's availability test.

Workshop Scenario Test

The workshop scenario test will include members of the Business Protection Team, the MIEG [Board of Directors] and the Service Delivery Live Service Team . At the workshop a scenario in the form of a major incident with significant business impact will be worked through. Test members will be allocated a role such as key supplier.

The objective of the test will be to validate the documented processes and procedures by which Major Incidents are managed within Post Office Ltd.

Availability Test

The Business Protection Team availability test will take the form of a text message sent to Business Protection Team members' business mobile phones. The text message will request a response within a requested timescale to the Service Delivery Business Continuity Team.

The objective of the availability test will be to test the ability of Business Protection Team members to respond quickly in the event of a Major Incident.

Appendix A ~ Contact details

BUSINESS PROTECTION TEAM ~ Key Members & Deputies [Bold type = primary contact for functional area]			
Name	Directorate	Functional Area	Telephone
Lynn Hobbs	**Network**	**Network Support**	GRO
Gayle A Laverick	Network	Network Support	
Tom Pegler	**Network**	**Commercial**	
John Rattle	**RMG**	**Government Affairs**	
Mike Granville	**RMG**	**Regulation (Postcomm/Postwatch)**	
Manita Basra	RMG	Regulation (Postcomm/Postwatch)	
Crispin Beale	**Marketing**	**Marketing Services**	
David Simpson	**GCCA**	**External Communications/Government Affairs**	
Mary Fagan	GCCA	External Communication	
David Gray	**Operations**	**Change & IS**	
Tim Connold	Operations	Change & IS	
Keith Rann	**Operations**	**Supply Chain**	
Mark Plant	Operations	Supply Chain – South	
Steve Sims	Operations	Supply Chain – North	
Dave Hulbert	**Operations**	**Service Delivery**	
Adam Martin	Operations	Service Delivery	
Doug Brown	**Operations**	**Supply Chain – Retail Cash**	
Clive Holmes	Operations	Supply Chain – Inventory & Planning Manager	
John M Scott	**Operations**	**Head of Security**	
Julian Tubbs	Operations	Senior Security Manager	
Sue Lowther	**Operations**	**Change & IS**	
Alan Simpson	Operations	Change & IS	
Rod Ismay	**Finance**	**Product & Branch Accounting**	
Alison Bolsover	Finance	Product & Branch Accounting	
Nick Warwick	**Operations**	**Property Projects**	
Steve Bates	Operations	Property Projects	
Teresa Beckingham	**P&OD**	**Operations Advisor**	
Debra Lewis	P&OD	Network & Sales – Advisor	
Steve Allchorn	**Strategy**	**Strategic PMO**	
Alana Renner	**P&OD**	**Internal Comms & Engagement**	
Paul Swanton	P&OD	Internal Comms	
Richard Weaver	P&OD	Internal Comms	

Note
Some members of the BPT also have access to Blackberrys ,a hand held communications device – see Appendix F.

Document Date: 25/02/2009		Document Type	L/001
Version	0.38	Ref. Number	CON/MGM/006

MAJOR INCIDENT ESCALATION GROUP ~
Board of Director Members and Deputies
[**Bold** type = primary contact for functional area]

Name	Functional Area	Job Title	Telephone
Alan Cook	**Directorate**	**Managing Director**	GRO
Mike Young	**Operations**	**Director Operations**	
Deputy: Andy McLean Dave Smith	Operations Directorate	Head of Service Delivery Head of Change & IS	
David Glynn	**Sales Directorate**	**Sales Director**	
Deputy: George Hooper	Sales Directorate	Head of Sales Strategy & Productivity	
Gary Hockey-Morley	**Marketing Directorate**	**Marketing Director**	
Deputy: Crispin Beale	Marketing Directorate	Head of Marketing Services	
Peter M Corbett	**Finance Directorate**	**Finance Director**	
Deputy: Stephen Hirst	Finance	Head of Finance (network & Sales)	
Debbie Moore	**HR Directorate**	**HR Director**	
Deputy: Alana Renner	Human Resources	Head of Engagement & Internal Comms	
Paula Vennells	**Network Directorate**	**Network Director**	
Deputy: Lynn Hobbs	Network Directorate	Head of Outlet Support	
Sue Whalley	**Strategy Directorate**	**Strategy Director**	
Deputy: Adrian Baker	Strategy	Head of Strategy Development	
As a matter of course, the MIEG will also include the following people:			
Dave Hulbert	Operations Directorate	Systems & Direct Channels Manager	GRO
Lynn Hobbs	Network Directorate	Head of Outlet Support	
Mary Fagan	GCGA Directorate	Group Corporate & Government Affairs Director	
Paul Budd	GCGA Directorate	External Relations Director	
Alana Renner	P&OD	Head of Engagement & Internal Comms	

Post Office Ltd Service Delivery			
Name	**Functional Area**	**Job Title**	**Telephone**
Andy McLean	Service Delivery	Head of Service Delivery	GRO
Dave Hulbert	Service Delivery	Systems & Direct Channels Manager	
Adam Martin	Service Delivery	Senior Ops Manager – Service Engagement & Transition	
Steve Beddoe	Service Delivery	Senior Ops Manager – Service Engagement & Transition	
Jill Kennedy	Service Delivery	Senior Ops Manager – Service Engagement & Transition	
Mandy Jepson	Service Delivery	Gateway Manager	
Gary Blackburn	Service Delivery	Live Service & Business Continuity Manager	
Live Service Desk	Service Delivery	Manned 24/7	

External Board of Director Equivalent Contacts			
Name	**Supplier Domain**	**Job Title**	**Telephone**
Craig Wilson	EDS	Vice President, EDS Applications Services, Field Operations,EMEA	GRO
David Masson	EDS	Operations Director , UK Civil Government & transport EMEA	
Steve Groppi	JP Morgan	EMEA Region Executive	
Ian Terblanche	Fujitsu Services	Director - Post Office Account	GRO
Ivan Goldsmith	CSC	POL Account Manager	

External Contacts			
Name	**Supplier Domain**	**Job Title**	**Telephone**
Wendy Warham	Fujitsu Services	Operations Director RMG Account	GRO
Tony Wicks	Fujitsu Services	Business Continuity Manager	
Product Support	EDS	1st Line Support – 24 x7	
Mike Daley	EDS	Service Manager	
Ian Fenlon	EDS	Business Continuity Manager	
Bob Hewitt	EDS	Deputy Business Continuity Manager	
Richard Yarwood	Alliance & Leicester	Contingency Manager	
Ben Bawden	CSC	Service Delivery manager	
David Anderson	Streamline	National Helpdesk	
Frank Peel	Streamline	Operational Contact	
Service Desk	LINK	LINK Duty Incident Manager	

Appendix B ~ Business Protection Team responsibilities

The Post Office Ltd Business Protection Team is made up of empowered representatives from key areas throughout the business. See the table at Appendix A for details of the current Business Protection Team membership and additional useful contact points.

Responsibilities of members:

a) Be available and contactable on a 24x7 basis – business mobiles should be left switched on at all times except when on annual leave. They may be muted if required preferably on 'vibrate' mode as a minimum, but text/voicemail messages from the Live Service Team must be acted upon. These will appear in your message in box as being from '**DutyManager**'.
b) Be the single contact point and co-ordinate all activities within your directorate/function.
c) Be responsible for making decisions on behalf of the business, and taking actions to quickly manage the adverse impacts of a major service incident.
d) Facilitate two-way communications between your directorate/function and the appointed working group– ensuring that where the incident impacts your directorate/function you have kept all interested parties within your directorate informed and continue to keep them informed on the progress of the incident through to resolution.
e) Ensure that members of the Live Service Team are informed/notified about any events in your area, which may lead to a major service incident.
f) Consider any communications that may be required following the post major incident review, and be instrumental in their delivery, if appropriate to your directorate/function . For example, giving recognition if appropriate, sending out control reminders, etc.
g) Participate in periodic business continuity tests of the Major Incident Management procedures.

Responsibilities in the event of being assigned to the appointed Business Protection working group for a major incident:

a) Ensure consistent attendance throughout a major incident to ensure progress is not hindered. You should therefore make every conceivable effort to attend any meeting and/or conference call arranged. This may mean that pre-booked appointments have to be rescheduled.

b) Complete all actions assigned to you within the agreed timescales.

c) Wherever possible, take a second person to the working group meetings / conference calls. This will allow people to leave the meeting to seek additional information [if it is required during the meeting], without losing input from the directorate/function, or delaying the activities of the working group.

d) Participate in a post major incident review.

e) Consider any communications that may be required following the review, and be instrumental in their delivery, if appropriate to your directorate/function . For example, giving recognition if appropriate, sending out control reminders, etc.

Appendix C ~ Major Incident Escalation Group responsibilities

The PO Ltd Major Incident Escalation Group is made up of PO Ltd Directors and some of their direct reports. See the table on page 17, Appendix A for details of the current Major Incident Escalation Group membership and additional useful contact points.

Responsibilities of members:

As per BPG plus:

- Be contactable on a 24x7 basis – business mobiles should be left switched on at all times except when on annual leave. They may be muted if required, but text/voicemail messages from the Live Service Team must be acted upon. These will appear in your message in box as being from 'DutyManager'.
- Chair the Major Incident Escalation Group once invoked

Appendix D ~ Virtual Operations Room

Virtual Operations Room

In the event of a major incident the PO Ltd Live Service Team will immediately invoke the Virtual Operations Room [VOR].

The VOR will operate as a conference call facility and will remain open for the duration of the incident.

The VOR will be chaired by the PO Ltd Live Service Team, or by a BPT member nominated by the PO Ltd Live Service Team, and will be the central point of contact to which members of the Business Protection Team report progress on assigned actions and information updates.

The VOR will also act as the conference call facility for strategic conferencing at specified times, as directed by the Chairperson. In the event of considerable information traffic flowing through the VOR then an alternative conference call facility would be employed for strategic forums, details provided via the VOR Chairperson.

Roles and Responsibilities

Chairperson

- Open VOR facility and chair facility for duration of the incident.
- Manage Incident and Decision Log for duration of the incident – this will be made up of the following headings:
  - Time of Contact
  - Contact From
  - Contact With
  - Notes of Discussion/Information
  - Decisions Made

Secretary

- Maintain Incident and Decision Log for duration of the incident as directed by Chairperson
- Advise Business Protection Team times of strategic conferences.

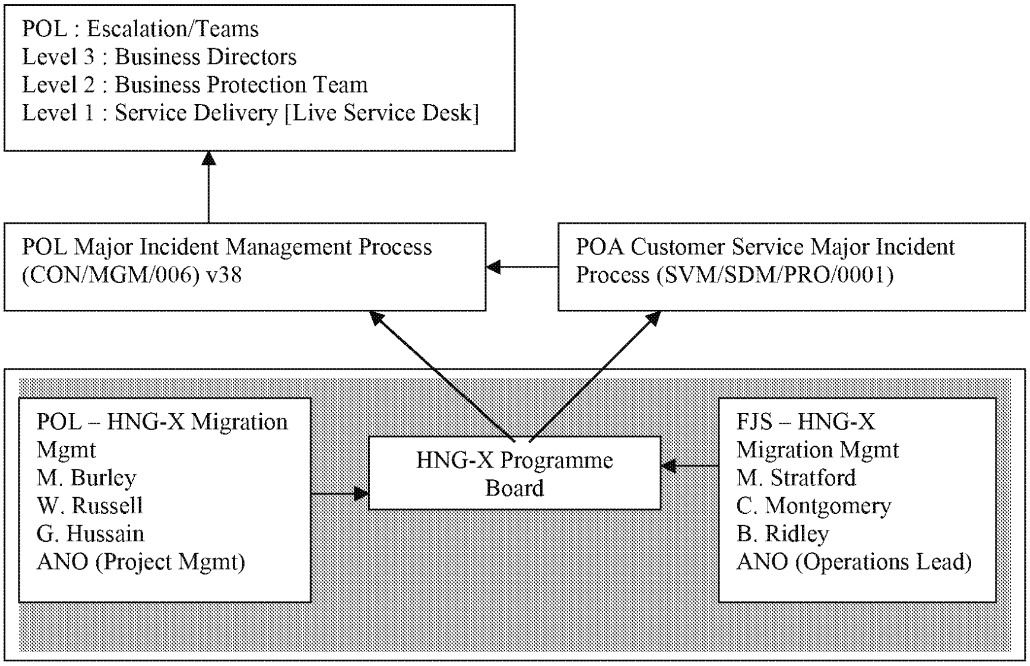
Business Protection Team

- On receipt of SMS log attendance at VOR with chairperson.
- Complete all actions assigned to you within the agreed timescales.

- Update the VOR [and the VOR only] on status of assigned actions.
- Feedback any information on incident/impact to the VOR [and the VOR only].
- Attend strategic conferences as directed by chairperson.
- Use the VOR for obtaining information

POL00001538

Appendix E ~ HNG-X Data Centre Migration – Incident Escalation and Management


POL : Escalation/Teams
Level 3 : Business Directors
Level 2 : Business Protection Team
Level 1 : Service Delivery [Live Service Desk]
POL Major Incident Management Process (CON/MGM/006) v38
POA Customer Service Major Incident Process (SVM/SDM/PRO/0001)
POL – HNG-X Migration Mgmt
M. Burley
W. Russell
G. Hussain
ANO (Project Mgmt)
HNG-X Programme Board
FJS – HNG-X Migration Mgmt
M. Stratford
C. Montgomery
B. Ridley
ANO (Operations Lead)

Responsibilities :

Regression up of Point of No Return (PONR) – Programme Board
Delays or Impact on Business As Usual – Major Incident Process (via Programme Board)
Incidents between Migration weekends – Major Incident Process

Appendix F – Blackberry Users

Blackberrys are a wireless hand held telecommunications device (very similar to a mobile telephone) that can receive and send e-mails without being connected to the LAN. Word attachments to e-mails can be viewed but Excel spreadsheets are difficult to read.

These people can be contacted by e-mail even in the event that the mobile communication system is congested/unavailable.

The following list details those people within POL that have access to a Blackberry device.

"Blackberry" Users	e-mail address
Adam Martin	Adam Martin/e/POSTOFFICE
Adrian Baker	Adrian Baker/e/POSTOFFICE
Alan Cook	Alan Cook/e/POSTOFFICE
Alana Renner	Alana Renner/e/POSTOFFICE
Andy McLean	Andy Z McLean/e/POSTOFFICE
Crispin Beale	Crispin Beale/e/POSTOFFICE
Dave Hulbert	Dave Hulbert/e/POSTOFFICE
David Glynn	David Glynn/e/POSTOFFICE
David Gray	David X Gray/e/POSTOFFICE
David Simpson	David Simpson/e/POSTOFFICE
David X Smith	David X Smith/e/POSTOFFICE
Debbie Moore	Deborah Moore/e/POSTOFFICE,
Gary Hockey-Morley	Gary Hockey-Morley/e/POSTOFFICE
Gary Blackburn	Gary Blackburn/e/POSTOFFICE
Jill Kennedy	Jill Kennedy/e/POSTOFFICE
John M Scott	John M Scott/e/POSTOFFICE
John Rattle	John Rattle/e/POSTOFFICE
Keith Rann	Keith Rann/e/POSTOFFICE
Lynn Hobbs	Lynn Hobbs/e/POSTOFFICE
Mark Plant	Mark Plant/e/POSTOFFICE
Mary Fagan	Mary Fagan/e/POSTOFFICE
Mike Granville	Mike Granville/e/POSTOFFICE
Mike Young	mike young/e/POSTOFFICE
Paula Vennells	Paula Vennells/e/POSTOFFICE

"Blackberry" Users	e-mail address
Paul Budd	Paul Budd/e/POSTOFFICE
Paul Swanton	Paul Swanton/e/POSTOFFICE
Peter M Corbett	Peter M Corbett/e/POSTOFFICE
Richard W Barker	Richard W Barker/e/POSTOFFICE
Richard Weaver	Richard R Weaver/e/POSTOFFICE
Stephen Hirst	Stephen Hirst/e/POSTOFFICE
Steve Beddoe	Steve Beddoe/e/POSTOFFICE
Steve Sims	Steve Sims/e/POSTOFFICE
Sue Whalley	Sue Whalley/e/POSTOFFICE
Tim Connold	Tim C Connold/e/POSTOFFICE

Appendix G - Business Continuity Information

[redacted]

Appendix H – Personal Secretaries to POL's Executive Team

Name of Director	Personal Secretary	Telephone of Secretary
Alan Cook	Tracey Abberstein	GRO
Mike Young	Beverley Hodis	
Peter M Corbett	Ruth Phillips	
David Glynn	Stefanie Rush	
Gary Hockey-Morley	Glenda Hansen	
Debbie Moore	Theresa Iles	
Paula Vennells	Angela Johnston	
Sue Whalley	Sara Howarth	

Appendix I – Telephone Conference Call Etiquette

In order for telephone conferences to run professionally the following etiquette is to be followed.

- The chairperson will set up and enter the conference call at least five minutes before its advertised start time and then start the conference call within five minutes of the advertised start time.
- The conference call should be treated like any other meeting.
- If you can not attend the conference call then please let the chair know before the advertised start time , if possible.
- The conference call will aim to last no longer than 45 minutes.
- If possible arrange to be in a quiet room, away from the office or other disturbances to participate in the connference call.
- Upon joining the conference call the participant must state their full name and the directorate/team that they are representing.
- The chairperson will identify them self , host the call and set the scene/state the reason for the conference call.
- A roll call will be undertaken prior to the conference call starting by the note taker who will issue actions etc after the conference call to all participants.
- When participants are not speaking then they must mute their telephone handset – Participants can mute their line by pressing * then 6 to cut out any background noise when this is present. They can then unmute their line by pressing * then 6. This will reduce background noise on the conference call.
- If you are joining a conference call using your mobile phone, check beforehand that you will be in a good signal reception area
- Be sure to keep your mobile phone a few feet away from your landline telephone handset as it can create a 'hum' when active.
- Take care not to rustle paper, type or make a noise that might disturb the call, unless your line is muted.
- Prior to speaking on the call the participant must state their full name.
- All participants on the call must observe common curtsey to other participants when they are speaking.
- At the end of the conference call, the chair will summarise the key actions and agree the next meeting date and time ,if relevant & thank everyone for their attendance and participation.
- The objective of the conference call is to resolve/manage the MBCI to a satisfactory conclusion.

Appendix J - POL's Payment Card Industry Incident Response Plan

HNG X Programme

PCI Incident Response Plan

Author(s)	Richard Barber
Reviewer(s)	Sue Lowther Connie Penn Alan Simpson Gary Blackburn Gary Dooley Rod Ismay Martin Roe Chris Hall
Sign off authority	Sue Lowther
Reference configuration	POL/HNG/PLA/001
Operational Baseline Number	
Version	0.3
Status	Issued
Classification	Working Document
Date	29/02/2008
Circulation	Reviewers, Service Helpdesk, Operations Control, POL and RMG Security teams

Document Control
Version History

VERSION	DATED	CHANGE DETAILS
0.1	18/02/2008	First version of PCI Incident Response Plan
0.2	22/02/2008	Updated following informal review
0.3	29/02/2008	First Issue including comments from formal review

Change Co-ordinator

All changes to this document are to be sent to the Change Controller below:

Name	Alan Simpson
Job Title	POL Security Incident Manager
Business Address	148 Old Street London EC1V 9HQ
Business Telephone Number(s)	tbd

Related Documents

REF:	DOCUMENT REF.	TITLE	VERSION	DATE
1	CON/MGM/006	CMT high level procedures	0.38	
2	S15	RMG Information Security Incident Response Policy (S15)		
3	PCI DSS	Payment Card Industry Data Security Standard	1.1	

Abbreviations

ABBREVIATION	DESCRIPTION
Card Schemes	Means those companies that produce payment cards (credit or debit) e.g. Mastercard, VISA, American Express, Diners Club, JCB etc
CPP	Common Point of Purchase. A term used by the Card Schemes to refer to merchants suspected of being used to compromise payment cards
CSIRT	RMG Computer Security Incident Response Team
FE	Forensic Expert. An investigator who has expertise examining computer systems for evidence of malicious activity. For this PCI Incident Response Plan such investigators must be approved by the Card Schemes otherwise they must not be engaged to investigate a PCI Incident.
FS	Fujitsu Services Ltd
HNGX	Horizon Next Generation
HNGX Data Centre	Fujitsu Services Data Centre(s) used for provision of services for HNGX
IRE11 / IRE19	Fujitsu Data Centres for HNGX. IRE11 is Primary. IRE19 is Secondary
Merchant Acquirer	An organisation, usually a bank, that contracts with one or more Card Schemes to engage and contract with merchants who will accept payment for goods or services by a payment card (credit or debit)
PCI	Payment Card Industry
POA	Fujitsu Services Post Office Account (= RMGA)
POL	Post Office Ltd
RMG	Royal Mail Group
RMGA	Fujitsu Services RMG Account (= POA)
SAN	Storage Area Network
User	An employee of Royal Mail Group, a contractor or a third party employee, authorised to access Royal Mail Group information systems for resources or for the purpose of providing IT support or maintenance.

This page intentionally left Blank

Contents

Introduction

While the POL Major Incident Management process is owned and managed by the Business Continuity Team within Operations Control the PCI aspect is owned by Information Security but manages and escalates a PCI incident as far as possible using processes already established within POL and RMG.

A PCI Incident may impact POL in a number of ways. Minor incidents will be handled using established processes within and across POL and RMG Security teams.

A Major PCI Incident will require escalation to and management by the Operation Control Major Incident Management Process as defined in document CON/MGM/006.

This document derives from RMG Information Security Incident Response Policy (S15)
Purpose
The purpose of this document is as follows:

- To define a PCI Incident
- To specify how a PCI Incident should be categorised.
- To define the roles and responsibilities in managing a PCI Incident at its various stages and the methods by which management will be notified and informed of an incident
- To outline the forensic response to a Major PCI Incident
- To define why and when a Major PCI Incident may necessitate the elective invocation of a Major Business Continuity Incident at the HNGX Data Centres
- To identify reporting requirements
- To identify test requirements and propose test scenarios

Scope

This document applies to POL HNGX programme after it goes live.
This document only applies in respect of the contract between POL and Streamline. It does not apply to any other payment card service used by or for POL.
This document does not apply to suppliers other than Fujitsu Services Ltd Post Office Account.
This document does not apply to any Web Portal.

PCI Incident Definition

A PCI Incident is one where information is received that indicates that cardholder data may have been compromised. It is not necessary to demonstrate that cardholder data has been compromised to declare an incident. Part of the

PCI Incident Response Plan will be an investigation to confirm whether a compromise has or has not taken place.
PCI Incidents are defined as Minor or Major.

Minor PCI Incident Definition
The definition of a Minor PCI Incident is not an exact science and will involve the judgement of the POL Security Incident Manager. Such an incident will typically appear to be the work of opportunist theft not organised crime.
Such an incident is one where, for example:

a) Up to 1,000 cardholder details are suspected of being compromised over a period of 12 months or more in four or more locations, AND
b) It can be shown conclusively that a HNGX Data Centre cannot have been involved in the compromise

Major PCI Incident Definition
The definition of a Major PCI Incident while not an exact science requires less judgement but must involve the judgement of the POL Security Incident Manager and the POL Head of Information Security. Such an incident will appear to be an organised activity to obtain credit or debit card details and will necessarily imply large scale compromise of data. Regardless of the volumes of data involved an incident will be categorised Major if any HNGX Data Centre appears to be involved. The determination that an HNGX Data Centre is involved will depend on an interpretation of the evidence obtained of the suspected compromise.
Thus a Major PCI Incident is one where, for example:

a) a single large volume compromise appears to have occurred e.g. more than 1,000 cardholder details over a period of no more than one week in four or less locations, OR
b) the evidence indicates that payment card data compromised could only have come from POL systems.

PCI Incident Management
This section describes the entry points to the PCI Incident Management Process and the decision points leading to a Minor Incident declaration or a Major Incident declaration.
The process is shown in Figure 1 on page 51. and described in Table 1 on page 52.

Initial Reporting
An Initial Report is one made by any POL team receiving an allegation from any

source that payment card data may have been compromised while in the possession of POL.

Sources include (but are not limited to): Business Partners, Suppliers or External Agencies, Customers or Users.

It is also possible that the Merchant Acquirer may be the source. This may occur if POL has been identified as a Common Point of Purchase (CPP).

An Initial Report is the first indication received of the possible compromise of cardholder data whilst in the POL environment (counters, business processes, data centre networks, systems, suppliers etc).

Each POL team that may be expected to make an Initial Report must ensure they know what information must be obtained from the source. See Section 0 and 0.

Escalation Path

The Initial Report must be passed to the first person in the list below. That person must respond with a positive written confirmation that the Initial Report has been received and that they are dealing with it.

If no such response is received within 24 hours then the Initial Report must be passed to the next person on the list in exactly the same manner and each time allowing 24 hours for a response.

ESCALATION	ROLE
1	POL Security Incident Manager
2	POL Head of Information Security
3	RMG Head of Information Security
4	RMG Computer Security Incident Response Team

Severity Analysis

The POL Security Incident Manager will obtain, confirm and review the evidence of the incident if it is not provided with the Initial Report. It is presumed that such evidence will be a copy of the cardholder data that is purported to have been compromised. The content and format of the cardholder data can point to how the incident may have taken place.

If no evidence exists then the incident is closed.

The Severity Analysis will be entered into the Incident Report.

PCI Incident Reports

The POL Security Incident Manager is responsible for completing a PCI Incident Report according to the format described in Section 0

PCI Minor Incidents Reports must be passed to the POL Head of Information

Security on a monthly basis.
PCI Major Incident Reports must be passed to the POL Head of Information Security within 5 minutes.

PCI Incident Classification
The POL Security Incident Manager must review the evidence and classify the incident as Minor or Major. See Section 0.

PCI Minor Incident Declaration
Based on the evidence received the POL Security Incident Manager may declare an incident a PCI Minor Incident and will pass the investigation of the incident to the relevant security team within POL or RMG.
The POL Security Incident Manager will also pass a copy of the PCI Incident Report to the Head of Product and Branch Accounting in the Finance Department so that the Merchant Acquirer can be informed of the incident. The PCI Incident Report remains open until the incident is resolved. The PCI Incident Report must be updated with any progress made and this must also be communicated to the Merchant Acquirer through the normal channels. See Section 0.

NB If the Initial Report and the evidence shows that a HNGX Data Centre may be implicated then the incident is automatically a PCI Major Incident.

PCI Major Incident Declaration
If the POL Security Incident Manager decides the evidence received indicates a PCI Major Incident the PCI Incident Report must be passed to the POL Head of Information Security within 5 minutes.
The POL Head of Information Security will review the evidence and Severity Analysis and must confirm or downgrade the Analysis.
If the Severity Analysis is confirmed this is entered into the PCI Incident Report and a PCI Major Incident is declared.

The POL Head of Information Security must pass a copy of the PCI Incident Report to the Head of Product and Branch Accounting in the Finance Department so that the Merchant Acquirer can be informed of the Major Incident. The PCI Incident Report must be updated by the POL Head of Information Security as part of the Working Group (see Section with any progress made and this must also be communicated to the Merchant Acquirer through the normal channels.
See Section 0.

PCI Minor Incident Management Process

A PCI Minor Incident will not have occurred within the HNGX Data Centres. However applications hosted within the HNGX Data Centres may have been used to compromise cardholder data.
PCI Minor Incidents could be a result of abuse of POL, RMG or Supplier staff using privileges to obtain cardholder data from Audit, Transaction Enquiry or other systems. Or they could be the result of PO Counter staff falsely obtaining cardholder data at the Counter e.g. through techniques such as “skimming”.

The POL Security Incident Manager will obtain, confirm and review the evidence of the incident. It is presumed that such evidence will be a copy of the cardholder data that is purported to have been compromised. The content and format of the cardholder data can point to how and/or where the incident may have taken place.

Minor Incidents will be passed to and investigated by the POL Security Team. The POL Security Team will become responsible for the incident and will report progress back to the POL Security Incident Manager who will update the Incident Report and distribute according to Section 0.
Whichever team receives a PCI Minor Incident Declaration will investigate the incident following their normal processes and with due regard to safeguarding evidence that may be needed for a prosecution.

PCI Major Incident Management Process

Introduction

In the event of a major incident, activities must be co-ordinated within the POL, RMG and Supplier businesses in order to minimise adverse impact and protect service to both customers and clients. Due to the large number of teams and activities involved this cannot effectively be managed by POL Information Security.

Consequently a PCI Major Incident requires the invocation of the Operations Control Major Incident Management Process.
This process is identified in Operations Control Procedure CON/MGM/006. The highest incident level in that process is Level 3 and is applicable to a PCI Major Incident.

The reason that a Major PCI Incident is automatically a Level 3 Major Incident is because the requirements of the forensic investigation process may necessitate the decision to disconnect the entire data centre from all its connecting networks in order to preserve and analyse the data within for evidence.

The steps toward making the decision to disconnect a HNGX Data Centre are detailed in 0 below.

Differences from Operations Control Procedure CON/MGM/006
This description and the Operations Control Process refers to the 'Working Group'. This is made up of all or specified members of the POL Business Protection Team, as selected by the POL Live Service Team for the specific incident.

The investigation of a PCI Major Incident requires the formal engagement of an external company approved by the MasterCard and VISA to provide a Forensic Expert (FE). Normally this FE is imposed by the Card Scheme usually via the Merchant Acquirer. However it is **vital** that POL engage their own pre-selected FE.
The FE company will be selected by the POL Head of Information Security from a list maintained within POL Information Security.
The POL Live Service Team within Operations Control retains the co-ordination point for this incident process.

The POL Head of Information Security must be an active participant in the Working Group. If the POL Head of Information Security is not available they will appoint a substitute and will communicate this to the Live Service Team. If the POL Head of Information Security cannot be contacted then the RMG Head of Information Security will assume that role.

The POL Head of Information Security will report the progress and findings of the forensic investigation to the Working Group established to manage the incident.

The Working Group must ensure that the PCI Incident Report reflects any progress made during the incident investigation and is formally communicated to the Merchant Acquirer via the Head of Product and Branch Accounting.

The POL Security Incident Manager must re-locate to the HNGX Data Centre where the investigation is taking place and act as coordinator and liaison between the POL Head of Information Security, the HNGX Data Centre Incident Response Team and the Forensic Investigation Team.

Figure 1: PCI Incident Management Flowchart

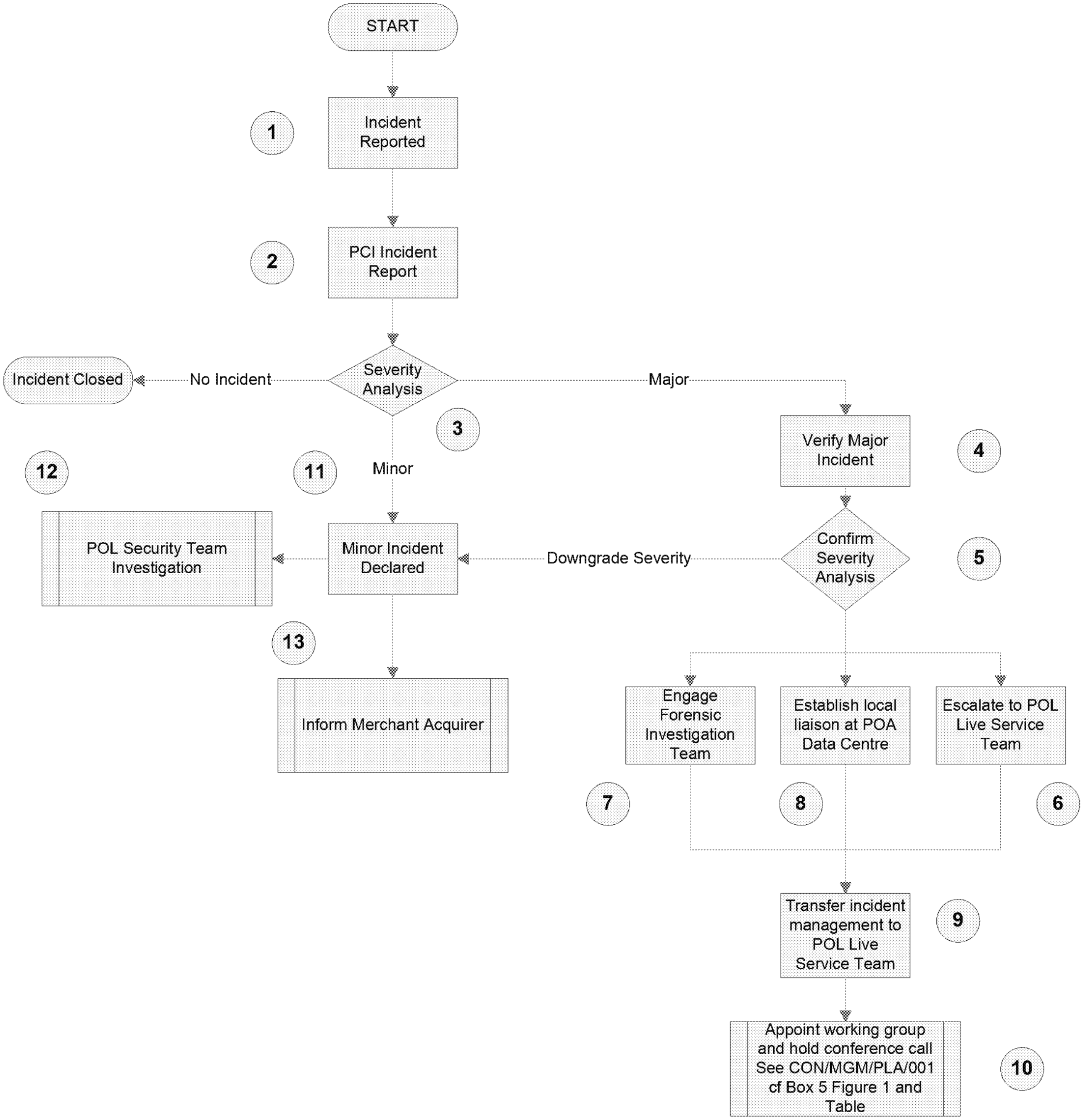

START
1
Incident Reported
2
PCI Incident Report
Incident Closed
No Incident
Severity Analysis
Major
3
Verify Major Incident
4
12
11
Minor
POL Security Team Investigation
Minor Incident Declared
Downgrade Severity
Confirm Severity Analysis
5
13
Inform Merchant Acquirer
Engage Forensic Investigation Team
Establish local liaison at POA Data Centre
Escalate to POL Live Service Team
7
8
6
Transfer incident management to POL Live Service Team
9
Appoint working group and hold conference call See CON/MGM/PLA/001 cf Box 5 Figure 1 and Table
10

Table 1: PCI Incident Management Process

Box	Title	Description	Key timescales	Action owner
21.	Incident reported	Incident identified (clause 0) The Initial Report is passed to the POL Security Incident Manager or another member of the Escalation path (clause 0). A minimum of 24 hours and a maximum of 96 hours is allowed.		
22.	PCI Incident Report	• The Initial Report is reviewed • Copy of Evidence is obtained • Incident Report opened	Within one business day of Initial Report.	POL Security Incident Manager or alternative
23.	Severity Analysis	Evidence reviewed and incident is: • closed, or • classified as Minor, or • assessed as Major	Within 2 hours of Incident Report being opened	POL Security Incident Manager or alternative
If the incident is low impact go to box Error! Reference source not found.. **If the incident is medium to high impact proceed to box 24:**				
24.	Verify Major incident	Incident Report with Severity Analysis and evidence is passed to Head of Information Security if incident is classified as Major	Within 1 hour of the incident being assessed as Major.	POL Security Incident Manager or alternative
25.	Confirm Severity Analysis	Incident Report with Severity Analysis and evidence is assessed. If downgraded incident passes back to POL Security Incident Manager. If confirmed escalation to POL Live Service Team begins Copy of PCI Incident Report sent to Head of Product and Branch Accounting for formal communication to Merchant Acquirer.	Within 1 hour of the incident being assessed as Major.	POL Head of Information Security or alternative
If Severity Analysis is downgraded go to box Error! Reference source not found.. **If the incident is confirmed as Major proceed to box 26**				
26.	Escalate to POL Live Service Team	• Email Incident Report to POL Live Service Team • follow up with phone call. • Set out PCI Major Incident Management Process requirements	Within 1 hour of the incident being confirmed as Major.	POL Head of Information Security or alternative
27.	Engage Forensic Investigation Team	• Select Forensic Team from list of POL approved companies. • Confirm POL approved company is VISA	Within 1 day of the incident being confirmed as	POL Head of Information Security or

Box	Title	Description	Key timescales	Action owner
		and Mastercard approved. • Follow POL process to engage Forensic Investigation Team	Major.	alternative
28.	Establish local liaison at HNGX Data Centre	POL Security Incident Manager relocated to POA to effect local liaison and incident management with Supplier teams.	Within 1 day of the incident being confirmed as Major.	POL Head of Information Security or alternative
29.	Transfer incident management to POL Live Service Team	Control of Incident is passed to POL Live Service Team in conjunction with POL Head of Information Security because of specialist security assessments and skills required.	Within 1 day of the incident being confirmed as Major.	POL Head of Information Security or alternative
30.	Appoint working group and hold conference call	The POL Live Service Team appoints a working group to participate in the management of the incident. The working group will be made up of appropriate representatives from the Business Protection Team, relevant POL business/technical managers and appropriate representation from supplier domains [if appropriate]. An initial conference call is held.	Within 1 day of the incident being confirmed as Major.	POL Live Service Team and appointed working group.
Low impact incident [continued from box 23]:				
31.	Minor Incident Declared	• Incident confirmed as Minor on Incident Report. • Copy of PCI Incident Report sent to Head of Product and Branch Accounting for formal communication to Merchant Acquirer.	Within 4 hours of incident being confirmed as Minor	POL Security Incident Manager or alternative
32.	POL Security Team Investigation	POL Security Incident Manager passes control of incident to POL Security Team for investigation (PCI Minor Incidents are managed using existing business as usual processes by the POL Security Team.)	Within 4 hours of incident being confirmed as Minor	POL Security Incident Manager or alternative
33.	Inform Merchant Acquirer	Head of Product and Branch Accounting formally communicates PCI Incident Report to Merchant Acquirer and acts as liaison for future updates to this report.	Within 4 hours of receiving Minor PCI Incident report	Head of Product and Branch Accounting or alternative
If a PCI Minor Incident escalates to a PCI Major Incident, i.e. the initial impact worsens, then the incident would be reassessed and the process would proceed to box 4.				

Reporting

Initial Reports

An Initial Report is the first indication received of the possible compromise of cardholder data whilst in the POL environment (counters, business processes, data centre networks, systems, suppliers etc).
An Initial Report is a term that describes the details that must be taken when it becomes apparent that cardholder data may have been compromised.

An Initial Report may arise from any Supplier or External Agency or from within POL or RMG.

An Initial Report may be taken by any of the channels that normally receive calls from any party external or internal to POL. Examples of external parties could be Law Enforcement Agencies, Suppliers, Merchant Acquirer, APACS, members of the public, the media – this is not an exhaustive list.

The channels that might receive calls from external parties could be Business Service Centres, RMG Corporate Security Centre, POL Security Team, RMG or POL Portal Webmaster(s), eBusiness team, Horizon Service Desk, POL Security Helpdesk.

Whichever channel receives a call from an external or internal (POL or RMG) party should log the call using their local procedure and in addition ensure they obtain the details for an Initial Report.
The details that must be taken for a Initial Report are defined in 0.

PCI Incident Reports

PCI Minor Incident reports must be completed and logged by the POL Security Incident Manager using the HNGX Incident Report format or as otherwise determined. Within any HNGX Incident Reports PCI Minor Incidents must be clearly marked as such.
PCI Minor Incident Reports must be presented to the POL Head of Information Security on a monthly basis.

Merchant Acquirer PCI Incident Reports

The POL Security Incident Manager should pass each PCI Incident Report to the Head of Product and Branch Accounting in order that the incident can be communicated to the Merchant Acquirer in accordance with the

requirements of the contract between POL and the Merchant Acquirer.
Any change in the progress of an open incident will be reflected in the Incident record and will be reported to the Merchant Acquirer as described.

This applies for both Minor and Major Incident Reports. The point at which the reports are provided to the Merchant Acquirer are described in the relevant sections above.

PCI Minor Incident Report Format

PCI Minor Incident Reports will include all the details of the Initial Report plus the Severity Analysis. Additionally the PCI Minor Incident Report will include a unique Incident number; a summary of the incident, status of incident, issues arising from incident and chase/resolution dates.

Major Incident Reports

It is presumed that PCI Major Incidents will only occur within HNGX Data Centres.

The POL Security Incident Manager will complete a PCI Major Incident Report as soon as the incident is declared. This report will be made available to all management involved in deciding how to manage the Incident.

The PCI Major Incident Report must include a unique incident reference (which clearly shows the incident as Major) and will describe the incident, the reason for the severity (which will also describe the evidence), the status and the likelihood that the Data Centres are at risk.
PCI Major Incident Reports will be updated following the process for reporting defined in the Operations Control Major Incident Management Process.
The POL Security Incident Manager will liaise with external organisations involved in the incident e.g. Third Parties, Forensic experts etc in preparing a Post Incident Report. All such liaison will be communicated to the POL Head of Information Security and be communicated via the channels implemented within the Operations Control Major Incident Management Process.

The POL Security Incident Manager will complete and distribute a post-incident report, initially within one week of the incident. Such report will include a root-cause analysis and will be passed to the POL Head of Information Security to approve and distribute to senior management.

Testing

PCI DSS requires the plan be tested at least annually.
Test scenarios may be worked into the existing Business Continuity tests and it is preferable for that Major Incident that this be the case.
Minor incidents should be tested more frequently and should cover likely scenarios involving low numbers of cardholder details e.g. 100 PANs over 6 months
Tests should at least focus on:

a. ensuring that channels of communication work as expected and are timely
b. ensuring that Initial Reports are accurate and reliable
c. ensuring that evidence is gathered
d. ensuring that severity analyses are conducted; are effective and are appropriate
e. confirming that staff, third parties and especially key suppliers are aware of their responsibilities and have effective incident processes in place
f. confirming that all third party forensic response and capability is appropriate and effective.
g. ensuring that lessons learned are adopted back into the incident process

Awareness and Training

PCI DSS requires that appropriate training be given to those with security breach responsibilities.
This needs to ensure that the following teams, in PO Ltd, RMG and Third Parties, are aware of their roles and responsibilities in the event of a suspected and a declared breach:

a. Security teams
b. Helpdesk teams
c. Operations teams

Training needs to focus on:

a. how to complete an Initial Report;
b. ensuring that POL liability is not admitted
c. ensuring that Initial Reports are passed to correct contact
d. how to interpret evidence for Severity Analysis

Appendix A Payment Card Industry[1]

Card schemes set the business rules that govern the issue of the payment cards that carry their logo. Typically, these rules apply throughout the world to ensure interoperability of cards. In many countries, domestic schemes also operate. The schemes operate the clearing and settlement of payment card transactions. In the UK, banks and building societies must be members of the appropriate scheme to issue cards and acquire card transactions. Examples of international card schemes in the UK are Visa, MasterCard, American Express and Diners Club.

A Merchant Acquirer is a bank having a business relationship with merchants, retailers and other service providers to process their plastic card transactions. Acquirers obtain financial settlement from the card issuers, typically via the card schemes which maintain the clearing systems, and pay the proceeds to the merchant, charging a fee.
The Card Schemes define a security standard on all merchants which is legally binding on all merchants by virtue of their contract with the Acquiring Bank. For the purposes of this document the Merchant Acquirer for POL is Streamline. This standard is the Payment Card Industry Data Security Standard (PCI DSS).

PCI DSS requirements are applicable if a Primary Account Number (PAN) is stored, processed, or transmitted. If a PAN is not stored, processed, or transmitted, PCI DSS requirements do not apply. At present the design for HNGX falls under these requirements.

The PCI DSS security standard requires a documented incident process for any incident that affects or may affect the security of cardholder data. This documented process is required to be audited and tested annually and must be invoked should it be suspected that cardholder data may have been compromised.

Cardholder data includes all data on the Payment Card or on its magnetic stripe or encoded into the chip if it is a so-called Chip and Pin card. This data includes but is not limited to the: Primary Account Number (PAN), Cardholder name, Service code, Expiration date, Security codes (e.g. CVV2 etc), magnetic stripe data, PIN code etc.

Appendiox B Excerpt from PCI DSS v1.1

12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.

12.9.1 Create the incident response plan to be implemented in the event of system compromise. Ensure the plan addresses, at a minimum, specific incident response procedures, business recovery and continuity procedures, data backup processes, roles and responsibilities, and communication and contact strategies (for example, informing the Acquirers and credit card associations)

12.9.2 Test the plan at least annually

12.9.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts

12.9.4 Provide appropriate training to staff with security breach response responsibilities

12.9.5 Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems

12.9.6 Develop process to modify and evolve the incident

Appendix C Content of Initial Report

Anyone receiving an initial report must NOT under any circumstances admit any liability for or on behalf of POL and must not pass any personal opinion regarding the incident. At this stage the incident is not confirmed.

An Initial Report must include:

a) Date and time

b) Agent name, contact details and network identifier

c) contact details of the person making the report e.g. name, organisation (e.g. Police, member of public, RMG, Supplier etc), landline telephone number, mobile telephone number, address etc

d) Complete description of the cardholder data and format in which it may have been compromised e.g. PANs (Primary Account Numbers – the 16 numbers normal found on the front of the card), cardholder name etc

e) Caller's description of events that indicate a compromise of cardholder data may have taken place.

f) How many card details are thought to be involved

g) How the compromise happened

h) Why the caller believes POL is involved.

i) Agent must ask and record what is the evidence that cardholder data may have been compromised.

j) Agent must also ask for copies of the evidence that cardholder data may have been compromised.

Anyone receiving an initial report must NOT under any circumstances admit any liability for or on behalf of POL and must not pass any personal opinion regarding the incident. At this stage the incident is not confirmed.

Appendix D Forensic Investigation of PCI Major Incident

Purpose and Background

The purpose of a forensic investigation is to:

a) Determine what logs and records need to be used for the investigation
b) Secure those logs and records as evidence
c) Examine the evidence gathered
d) Determine whether or not cardholder data was compromised via the data centre
e) Report their findings to the Merchant Acquirer

It is assumed that this Major Incident involves the HNGX Data Centres. It is a contractual requirement on POL that an external and fully qualified forensic team must investigate a PCI Major Incident.

The POL Head of Information Security will maintain a list of approved forensic investigators. No other forensic team may be involved without the explicit written approval of the POL Head of Information Security otherwise POL risks a breach of contractual obligations which may result in a cessation of payment card processing by the Merchant Acquirer.

The forensic investigators may decide that the incident may only be resolved by an elective disconnect of the Data Centres. The decision to disconnect all or some of the systems that comprise HNGX will necessarily involve the correct level of management.

Process Assumptions

a) There will be a phased approach to forensic investigation of data in HNGX. This would utilise a principle of "least invasive to most invasive".
b) Once forensic experts are brought in this process allows POL a 2 week window before an elective disconnect of IRE11 and / or IRE 19 might need to happen.
c) The parallel steps i.e. A1, A2 etc, can only take place if there are sufficient FEs to carry out those steps in parallel. Fewer resources will increase the number of steps needed.
d) The process includes multiple checkpoints en route to validate the need to invoke an elective disconnect.
e) Live service from IRE11 and IRE19 will be maintained as long as possible with minimal interruption to service
f) There will be a period of investigation before it can be decided whether or not an elective disconnect of HNGX Data Centres is necessary. This will be nominally 2 weeks
g) Forensic copy will be required of only selected areas of the SAN in IRE11 (**DN if replication protocol allows it then this step may be performed at IRE19**)

h) Elective disconnect is the last option to be considered and only if forensic investigation can be shown to require it.

Forensic Investigation Process

A1. Forensic experts (FE) briefed on design of data centre, PCI data flows, storage locations, data formats etc - I think this is envisaged in the Permeation Map.

A2. Immediately suspend all planned changes to data centre servers, applications, storage etc. I.e. no code releases, no servers deployed or removed from service

A3. All admin access to data centre hosts restricted to "4 eyes" access e.g. admins must be effectively escorted during any access to any host by another admin.

A4. Initiate an immediate physical security escalation of data centre access. Secure data centre CCTV and access control records, work records etc.

B. Initial Report reviewed by FEs to determine which systems, transport networks or processes may be out of scope. This is based on a comparison of the evidence against the data in the systems and processes.

C. Based on the Initial Report FE assess what external links, servers, applications, processes and storage might be compromised. All others placed out of scope.

D. FE decides what SAN data must be secured and begins activities to identify and secure that data

E. Any external links implicated are physically checked for monitoring tools by external team from POL or RMG assisted by external FS staff and escorted by FS data centre operations manager

F1. FE review all SYSMAN3 logs

F2. FE review IRE11 bladeframe server processes in live memory for rogue processes (**DN1 best information at present indicates this activity could occur without interruption to live service - this needs confirmation by architects**) (**DN2. This presumes that FS can produce and maintain a list of authorised processes, sockets and protocols for the processes in live memory. If not then this step must be re-considered**)

F3. FE copy selected areas of SAN in IRE11 for systems and applications in scope.

F4. FE review SAN data

G. If none of the above yields sufficient information to exclude the possibility that data has been compromised (and arriving at this stage this is exceedingly unlikely) then elective disconnect of IRE11 is invoked if that is the only remaining area of forensic investigation.

Appendix E Elective Disconnect of HNGX Data Centre

This is a major Business Continuity Event in which a Data Centre is disconnected from its connecting networks in a planned and organised manner.

It is similar to a major Business Continuity Incident but is different in that it is planned and is forced by the requirement to comply with an obligation under contract with the Merchant Acquirer.

The purpose of the Elective Disconnect is to ensure that no network based process or traffic may deliberately or unintentionally change the state of the processes or data in the affected environment.

The consequences of not complying may be the withdrawal of the facility to process card transactions under that contract. This in itself may not have the same overall effect on POL operations at the Counters as disconnecting the Data Centre(s) but which may endure for a good deal longer. Whether this would be the case and how much longer it would last depends almost entirely on negotiation with the Merchant Acquirer.

The worst case scenario is one where the Merchant Acquirer is not influenced by outside pressures or negotiation and denies POL the facility to process any relevant payment card transactions until satisfied that the security breach has been completely identified; that the breach did not compromise or no longer compromises cardholder data.

Relevant payment cards are those falling under the contract with that Merchant Acquirer. In the scope of this PCI Incident Plan that would be Streamline.

Planning the Elective Disconnect

This ideally would have already been completed by the Data Centre supplier. It should form part of the annual test of this plan.

The disconnect must identify two scenarios:

a). The Primary Data Centre must be disconnected from its corporate network, the internet and any other Data Centres

b) Specific systems within the Data Centre must be disconnected from internal networks.

It should also include a planned re-connection. It might be assumed that would be the same as bringing the Data Centre(s) back online after a major BC incident. However a test would demonstrate whether this would be the case or not and a test should therefore be undertaken.