FUJ00234983

Document Title:	POA Operations Incident Management Procedure
Document Ref:	SVM/SDM/PRO/0018
Release:	Not applicable
Abstract:	This document details the POA incident processes which supplements the incident processes defined in the Fujitsu EMEIA Business Management Systems Incident Procedure with the Post Office Limited specific requirements or requests.
Document Status:	APPROVED This document contains sections that have been identified to POL as comprising evidence to support the assessment of named Acceptance Criteria by Document Review. These sections must not be changed without authority from the FS Acceptance Manager
Author & Dept:	Matthew Hatch – POA Operations Kelly Nash – POA Operations
Internal Distribution:	Steve Bansal, Matthew Hatch, Steve Evans, Andy Hemingway, Jason Muir, Sandie Bothick, Bill Membery, Chris Harrison, Jerry Acton, Sonia Hussain, Piotr Nagajek, Kelly Nash, Vicki Williams
External Distribution:	Michaela Reay, POL Business Continuity Manager Dave King, POL Security Manager Architect
Security Risk Assessment Confirmed:	Yes

Approval Authorities:

Name	Role	See Dimensions for record
Steve Bansal	POA Senior Service Delivery Manager	
Sandie Bothick	POA MAC & OBC Team Manager	

Note: See Post Office Account HNG-X Reviewers/Approvers Role Matrix (PGM/DCM/ION/0001) for guidance.

FUJ00234983

0 Document Control

0.1 Table of Contents

FUJ00234983

FUJ00234983

0.2 Document History

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
0.1	16/10/06	First draft taken from CS/PRO/074. Updated to include HNG-X document references. Security Management appendix added Incident Management Process modified to reflect current working practises. Hardware and Network Call priorities referenced Problem Management escalation changed to SDM rather than Problem Initiator.	
1.0	06/11/06	Updated with comments following review of v0.1. Issued for approval	
1.1	02/03/07	Security Annex has been updated.	
2.0		Updated with comments following review of v1.1 Issued for approval	
2.1	14/04/09	Document updated names & job descriptions. Acceptance section added.	
2.2	16/04/2009	Version 2.1 is corrupt	
2.3	10/06/2009	Updated to incorporate PCI DSS and comments received from Connie G Penn.	
3.0	28/07/09	Issued for approval	
3.1	03/08/09	Updated to incorporate further comments received from Paula Hillsden	
4.0	03/08/09	Issued for approval	
4.1	13/06/11	Updated to include clarified incident priority definitions and changed personnel names.	
4.2	30/06/11	Updated with comments following review of v4.1	
5.0	06-Jul-2011	Approval version	
5.1	23-Jan-2012	Update to include POLSAP and Security updates	
5.2	24-Oct-2013	Major update to align with Business Assurance Management procedures and for organisational changes.	
6.0	13-Nov-13	Incorporated changes for Sarah Hill HSD and issued for approval.	
6.1	11-Jun-14	Amended to replace the HSD function with the Atos Service Desk and replaced IMT references with the MAC team. Also updated to reflect the introduction of Atos as POL's Service Integrator.	
6.2	26-Jun-14	Section 9.1 enhanced to include , and any Payment	

FUJ00234983

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
		Brand incident (PCI)	
7.0	17-Jul-14	Incorporates minor amendments	
7.1	20 Oct-15	A major re-write to realign to the BMS Managed Incident procedure.	
7.2	23-Jun-16	Further major updates following a round-table review within POA on 3rd November 2015. Major amendments to Appendix A handling of security incidents.	
8.0	12-Jul-16	Incorporated minor changes for comments from the POA Senior Service Delivery Manager and issued for approval.	
8.1	20-Jul-2017	The procedure was checked for changes for CCNs 1602, 1609 and 16.14, no amendments were required. The distribution list was amended for organisational changes.	
8.2	12-Sep-2017	Revised Appendix B, Contacts.	
9.0	12-Sep-2017	Approval version	
9.1	19-Oct-2018	Major re-write so that the Fujitsu EMEIA Incident Procedure is used as the primary process and this document maps those process requirements to specific POA teams, see flow diagrams. Also updated for TfSNow which replaces TSD. Amended section 9.5.2 to include breach of data protection legislation Amended section 0.5 Associated Documents removing withdrawn documents. Amended section 8.0 as SVM/SDM/SD/0001 has been superseded by SVM/SDM/SD/0007. Issued for formal POA Fujitsu review.	
9.2	28- Nov-2018	Amended sections 1.3, 2, 3.1, 4 and 4.2 for comments received.	
10.0	29-Jan-2019	Incorporated comments made by Steve Bansal and issued for approval Amendments made as part of Author review Removed the comment "Unavailability of sufficient tools for Incident diagnosis" from section 3.1 Risks	
10.1 DRAFT	22-July-2019	Added Splunk as a monitoring tool.	
10.2	24-March-2020	Updates in reqards to only GDPR/PCI as a a result of comments made by Bill Membery, following the AMEX SSK EPA file issue. Sections 6 Outputs, 7 Standards and 9.1 Scope	
10.3 DRAFT	20-April-2020	Following a Major Incident Management – Transition to Post Office Meeting held on the 15th April 2020, conducting a full review of the document in order to replace any reference to Atos with Post Office as of 1st May 2020. Reviewed the Author and Dept section, resulting in	

FUJ00234983

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
		the removing of Tony Wicks and adding Kelly Nash. Following a review by Steve Bansal, the required changes have been made in-line with his comments. Will accept the changes and create Version 11.0	
11.0	18-June-2020	Reviewed by Sonia Hussain and minor changes have been made in line with her comments. Approved Version.	
11.1	14-July-2020	Added a minor change to section 9.5.2 Incident Categories, in relation to using the configuration items to indicate if there are GDPR, PCI or PCI and GDPR implications.	
12.0	15-Jul-2020	Approval version	

0.3 Review Details

Review Comments by :	
Review Comments to :	Matthew Hatch & Kelly Nash
Mandatory Review	
Role	Name
POA Senior Service Director	Steve Bansal
POA MAC & OBC Team Manager	Sandie Bothick
POA Acceptance Manager	Steve Evans
Optional Review	
Role	Name
POA Infrastructure Operations Manager	Andy Hemingway
POA Business Continuity Manager	Almizan Khan
POA SDM Networks	Chris Harrison
POA SMC Manager	Jerry Acton
POA Security Manager	Jason Muir
POA Problem Manager	Matthew Hatch
Head of Online Services	Sonia Hussain
Post Office Ltd	
Security Manager	Dave King
POL Business Continuity Manager	Michaela Reay

(*) = 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:

FUJ00234983

POL NFR DR Acceptance Ref	Internal FS POL NFR Reference	Document Section Number	Document Section Heading
SEC-3166	SEC-3285	9.5.2	Incident Categories

0.5 Associated Documents (Internal & External)

Reference	Version	Date	Title	Source
PGM/DCM/TEM/0001 (DO NOT REMOVE)			Fujitsu Services Post Office Account HNG-X Document Template	Dimensions
CS/IFS/008			POA/POL Interface Agreement for the Problem Management Interface	PVCS
SVM/SDM/SD/0025			POA Problem Management Process	Dimensions
PA/PRO/001			Change Control Process	PVCS
SVM/SDM/SD/0007			Service Desk – Service Description	Dimensions
SVM/SDM/SD/0023			POA Incident Enquiry Matrix	Dimensions
SVM/SDM/PRO/0001			POA Customer Service Major Incident Process	Dimensions
SVM/SDM/PLA/1048			SMC Business Continuity Plan	Dimensions
SVM/SDM/PLA/0031			Security Business Continuity Plan	Dimensions
SVM/SDM/PRO/0875			End to End Application Support Strategy	Dimensions
			EMEIA Incident Management Process	EMEIA BMS
			EMEIA Major Incident Management Process	EMEIA BMS
			EMEIA Root Cause Analysis (RCA) Process	EMEIA BMS
			Fujitsu Europe Security Policy Manual	EMEIA BMS

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

0.6 Abbreviations

Abbreviation	Definition
BCP	Business Continuity Plan
BMS	Business Management System
HDI	Help Desk
ISO	International Standards Organisation
ITIL	Information Technology Infrastructure Library
KEL	Known Error Log (in the context of this document, this is a workaround and diagnostic database) (These are also known as Knowledge Articles).
MAC	Major Account Controllers (MAC team)
OLA	Operational Level Agreement
OTI	Open Teleservice Interface

FUJ00234983

Abbreviation	Definition
PCI	Payment Card Industry
PCI DSS	Payment Card Industry Data Security Standard
POL	Post Office Limited
POA	Post Office Account
SDM(s)	Service Delivery Manager(s)
SDU	Service Delivery Unit
SLT	Service Level Targets
SMC	Systems Management Centre
SSC	Software Support Centre
TfSNow	Triole for Services Now

0.7 Glossary

Term	Definition
KELs and KAs	Note that different support teams refer to knowledge database information as either Knowledge Articles or Known Error Log. Where within this document KELs are referred to the reader can also consider them as Knowledge Articles.
Peak	The Incident Management System used by POA 3rd and 4th line support teams and other capability units involved in HNGX releases. It is linked with the TfSNow call management system.

0.8 Changes Expected

Changes
Within the next version of this document it will be discussed with Bill Membery regards a new EBMS Incident Procedure as this might mean that a POA Incident Procedure exemption is obtained.

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 Copyright

FUJ00234983

1 Introduction

1.1 Purpose

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

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

1.2 Owner

The owner of the Incident Management process at the local POA level is the Fujitsu POA Senior Service Delivery Manager.

1.3 Objective

For the purpose of this document an Incident is defined as:

"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."

The quality of the service includes the protection of the confidentiality of business, personal and card data as defined by the POA Information Security Policy (SVM/SEC/POL/0003).

The document applies to all Incidents raised by the POA MAC or by SMC (out of hours or from systems monitoring tools), where they are related to the Fujitsu outsourcing contract. N.B calls presented to POA MAC / SMC that should be placed with the POL Service Desk are transferred/ referred from POA MAC / SMC to Post Office Service Desk.

The scope of the process is from the receipt of an incident by the MAC / SMC, through to the successful resolution of the incident (or providing a workaround).

For clarity, it should be noted that the MAC team are responsible for managing/owning Incidents between 08.00 and 20.00 Monday to Friday, 08.00 to 17.00 Saturday and Bank Holidays 0800 – 1400 excluding Christmas Day. The SMC assume this responsibility out of hours, i.e., outside these hours. The SMC are responsible for escalation of incidents to the POA OOH Duty Manager.

The key objectives of the process are:

- Log, track and close all types of incident requests
- Respond to all types of incident requests
- Restore agreed service to the business as soon as possible
- Resolve incidents within the target timescales set for each priority level within the Service Level Agreement(s)
- Resolve a high number of requests at first contact
- Ensuring incident priorities are linked to business priorities
- Keeping the user informed of progress
- Reduced unplanned downtime
- Improved Customer satisfaction

1.4 Process Rationale

FUJ00234983

The primary goal of the Incident Management process is to restore normal service operation as quickly as possible, thereby minimising adverse impact to the business. In turn, this ensures the highest level of service quality and availability. Normal service operation is defined here as service operation within Service Level Targets (SLT).

Demonstrating a professional approach to, and Post Office Limited (the customer) and their clients.

1.5 Mandatory Guidelines

It is important to maintain a balance between:

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

b) Avoiding unnecessary alerting of the customer

c) Assessing which incidents are major

The following guidelines should be adhered to.

- During the MAC Core Hours (Monday – Friday 08:00 – 20:00 and Saturday 08:00 – 17:00 and Bank Holidays 0800 – 1400 excluding Christmas Day.) the MAC should be the first point of operational contact between Fujitsu and the Post Office Service Desk. Outside these hours the SMC acts as the first point of contact.
- Any activity detailed in this document which is assigned to the MAC is handed over to the SMC outside the MAC Core Hours.

2 Inputs

The inputs to this process are:

- All Incidents reported by Contact with the MAC / SMC. Contact is defined as voice, e-mail, incident transfers over the HDI interface from Post Office Service Desk or Tivoli Alert as the methods of communication with the MAC / SMC and fall into the following categories:
  - Business process error
  - Hardware or software error
  - Request for information e.g. progress of a previously reported Incident
  - User complaint
  - Network Error
- Severity and SLT information.
- Evidence of an Error.
- System Alerts received automatically from transaction monitoring tools. Due to the urgent nature of some of these alerts, they may be dealt with directly by SSC, with an update of workaround or resolution supplied to MAC / SMC. It should be noted that these alerts enter the process at step 1.2.3, and are not subject to prior steps in 1.1 & 1.2 of this process.
- Splunk will monitor the Azure environment and will be used by the SMC to identify incidents from alerts. In the Full Azure Foundation Service Splunk will automatically raise incidents in TfSNow. It should be noted that these automatically raised incidents enter the process at step 1.2.3, and are not subject to prior steps in 1.1 & 1.2 of this process.

3 Risks and Dependencies

3.1 Risks

The following define the risks to the successful delivery of the process:

- Break in the communications chain to third parties. Mitigation is to invoke escalation procedures.

FUJ00234983

- Non-availability of the MAC / SMC Incident Management System. Mitigation is given in the MAC / SMC Business Continuity Plan.
- Non-availability of the HDI interface with the POL Service Desk. Mitigation is via e-mail.
- Non-availability of the OTI links to internal & external service desk tools. Mitigation is via e-mail.
- Lack of information given to the MAC / SMC regarding changes, POL Business updates, request for changes, status of Problems etc. Processes must be followed to lessen this risk, such as the Change Management and Problem Management Processes.
- Unavailability of sufficient support unit staff to investigate and resolve issues.
- Unavailability of sufficient tools for Incident diagnosis whereby manual diagnostics are unable to provide the same level of information as automated tooling.
- Non-availability of KEL or call management systems. Mitigation is a secondary SSC server for KELs and manual call processes.
- The provision of inadequate staff training within the MAC / SMC, SDU's or 3rd party suppliers
- Unavailability of systems for evidence gathering.

3.2 Dependencies

This process is dependent on:

- Effective Incident handling by the MAC / SMC
- The known error information being available and kept up to date with all errors as the root cause becomes known to Problem Management
- Knowledge database kept up to date with POL business and services knowledge
- Fujitsu infrastructure support of the MAC / SMC tools
- Appropriate training plans / skills transfer
  Appropriate training needs to include hardware, software and networks support staff, SDU's and 3rd party suppliers
- Effective routing of calls to SDUs and third parties
- Effective escalation procedures and the maintenance thereof within Fujitsu, POL and third parties
- Governance of Incident / Problem Management procedures
- Effective feedback to POL through Service Management SRFs, contributing to end user education and reduced Incident rates.
- Internal feedback to improve the Incident / Management Process.
- SLT and OLA knowledge and understanding across all Fujitsu and 3rd party support
- POA, SDU and 3rd party consistent co-operation in incident identification and resolution.

FUJ00234983

4 Resources

The resources required for this process are:

- Process Owners
- Major Account Controllers team
- Service Management Team
- System Management Centre team
- Software Support Centre team
- Service Delivery Units
- Triole for Service Now incident management system
- Peak (third and fourth line incident database)
- ServiceNow and the HDI interface into TfSNow.
- OTI links
- TIVOLI (system components and event monitoring software)
- Splunk to monitor Azure environment
- Additional remote Management, Operational and Diagnostic tools
- Detailed Process and Procedure documentation

4.1 Roles

The main roles required by the process are:

- Incident Manager - To drive the Incident Management process, monitor its effectiveness and make recommendations for improvement. The key objective is to ensure that service is improved through the efficient resolution of Incidents.
- Major Account Controller - To provide a single point of contact for Post Office Service Desk, dealing with the management of routine and non- routine Incidents, Problems and requests
- Incident Resolver - To accurately diagnose and resolve Incidents and to assess, plan, build/test and implement Changes in accordance with the Change Management Process. This role will typically be fulfilled by the support teams and service delivery units.

4.2 Incident Prioritisation within POA

The priority assigned to a TfSNow incident is either based on the priority documented in an existing KEL or based upon the Urgency and Impact of the incident, refer to POA Incident Enquiry Matrix.

With the exceptions of Major Business Continuity Incidents and Major incidents POA generally utilise three priorities for incidents based upon the following guidelines.

Consideration must also be given to if the incident being reported is a Security Incident, if it is it must be classified and managed under the POA Operational Security process (See Appendix A for guidance). Priority 1 where there is an immediate impact to any live service or potential security incident requiring timely attention. Priority 1 incidents are voiced to a Support Delivery Unit, the POA Duty Manager and the Post Office Service Desk.

Priority 3 where there is an infrastructure failure which has caused a loss of resilience or a failure or event which needs the timely attention of a Support Delivery Unit whose team will be voiced.

Priority 5 for other less urgent incidents.

FUJ00234983

Note1: Generally Priority 2 and Priority 4 incidents are not utilised within POA. However, if there is a genuine business reason to do so incidents may be allotted at these priorities when it is consistent with EMEIA processes.

Note2: When incidents are transferred to the Software Support Centre (SSC) the TfSNow incident is transferred into a Peak incident system. Within Peak the incident priorities are defined as A, B, C and D. Therefore, when transferring TfSNow incidents into Peak ensure the following is adhered to:

TfSNow priority 1 equates to Peak priority A
TfSNow priority 2 equates to Peak priority B
TfSNow priority 3 equates to Peak priority C
TfSNow priorities 4 and 5 equates to Peak priority D

If this cannot be achieved through automation the MAC or SMC Agent undertaking the transfer is to log a comment on the TfSNow incident stating the TfSNow and Peak priorities.

FUJ00234983

5 Process Flow

As stated in section 1.1 Purpose, this Post Office Account Incident Procedural document is solely to supplement the incident processes defined in the Fujitsu EMEIA Business Management Systems Incident Process. https://emeia.fujitsu.local/emeia/c/P0004/Process_Maps/Incident_Management_Process.pdf

Procedure: https://emeia.fujitsu.local/emeia/sites/cdc/d/EBMS/SDM/Incident_mgt_procedure.htm

The following flowcharts provide an overview of the interactions for incidents with Post Office Account.

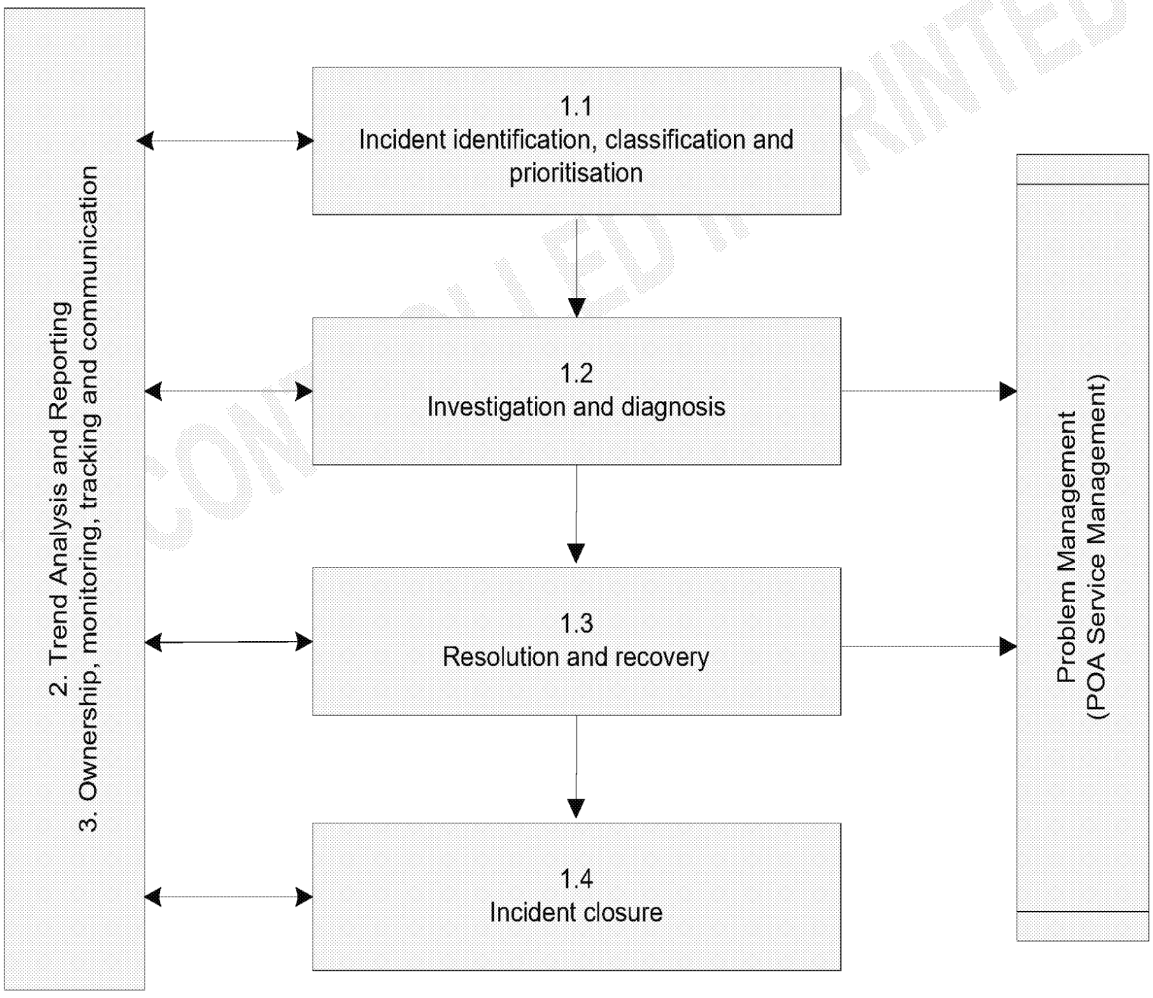


Figure 1: Level 1 Incident Management Process

FUJ00234983

5.1.1 Step 1.1: Incident identification, classification and prioritisation

Responsible: MAC / SMC, users, SDU's, Service Management

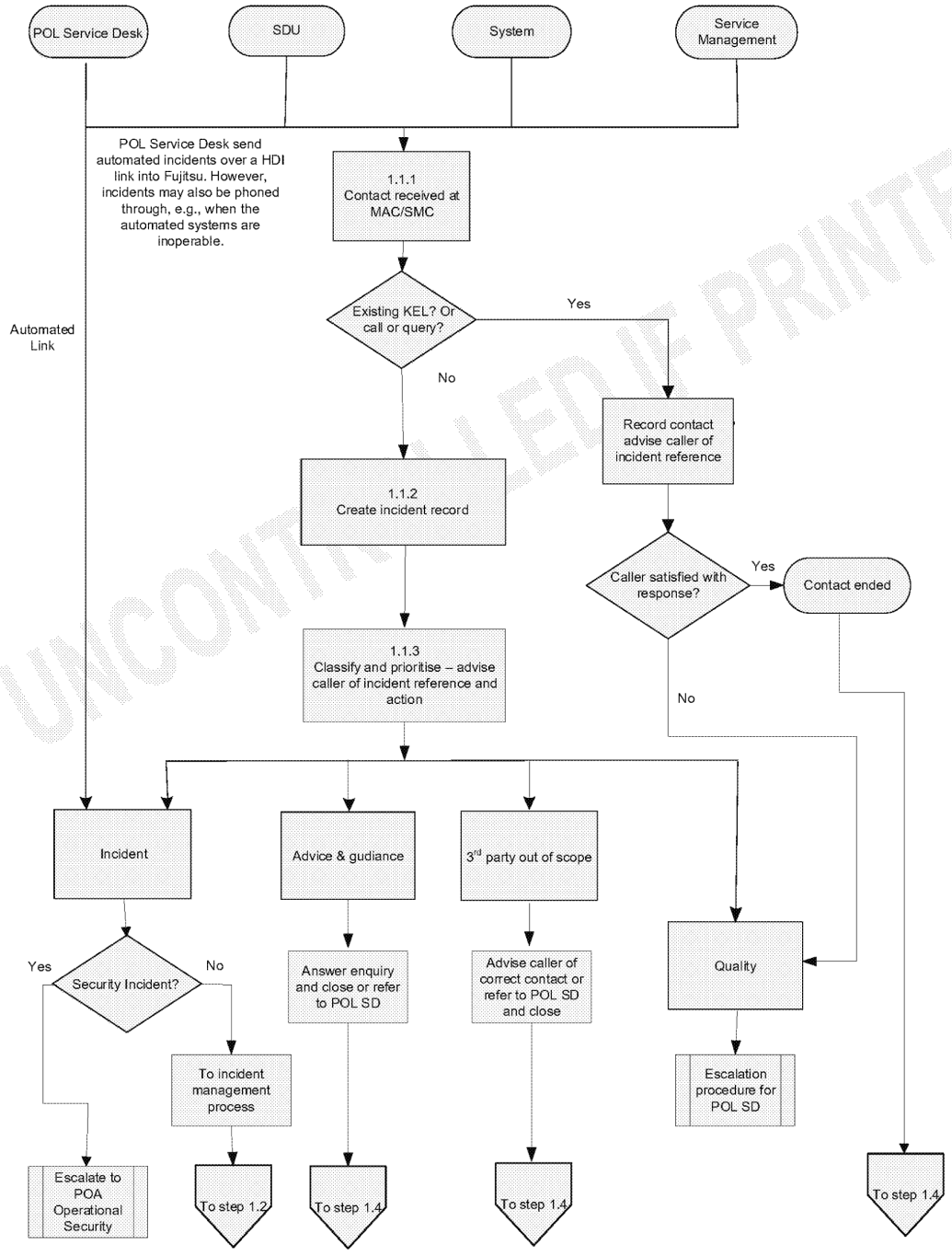


Figure 2: Level 2 Incident Management Processes

FUJ00234983

5.1.2 Step 1.2: Investigation and Diagnosis

Responsible: MAC / SMC

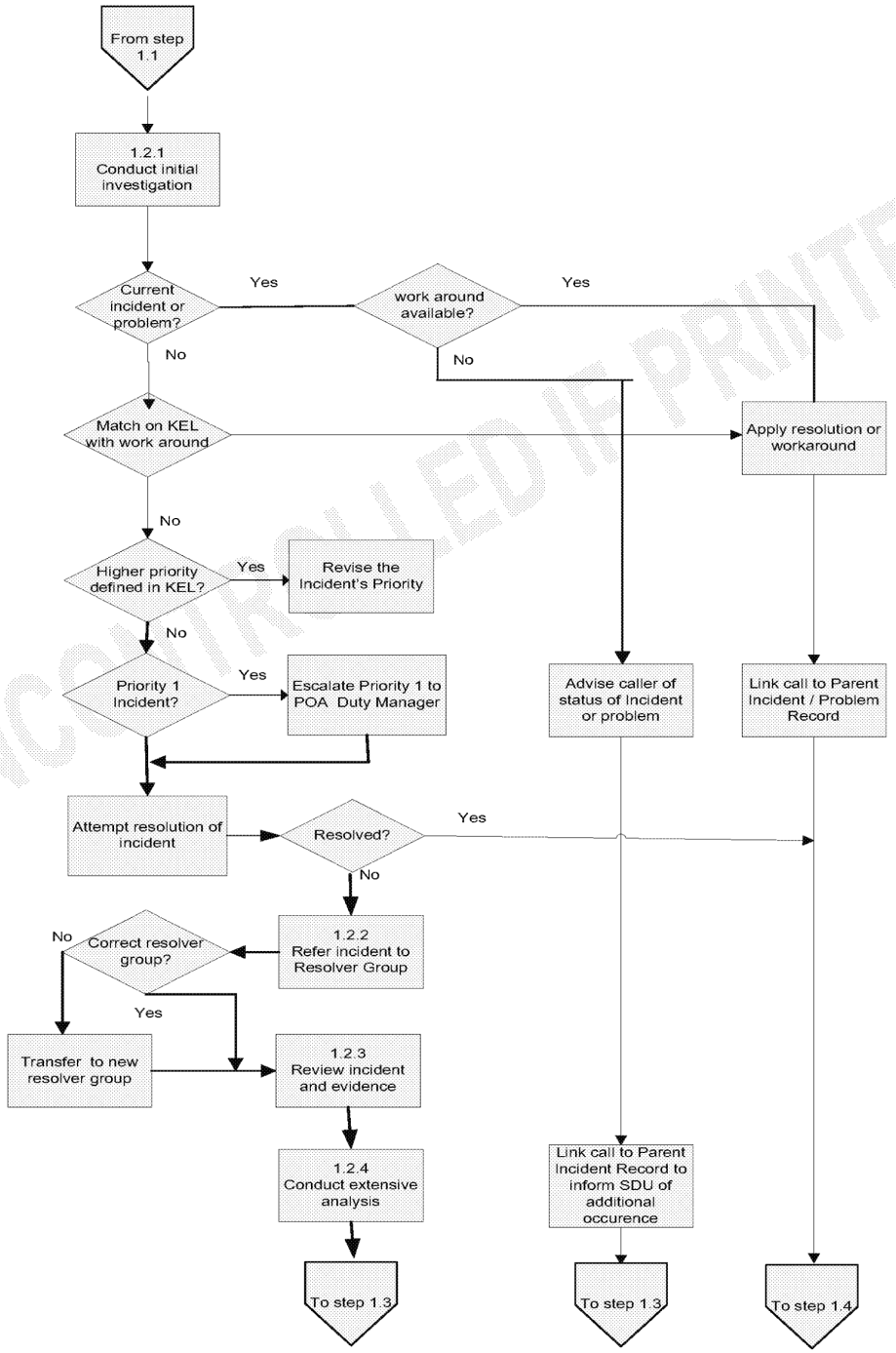


Figure 3: Investigation and Diagnosis

FUJ00234983

5.1.3 Step 1.3: Resolution and Recovery

Responsible: SDU's

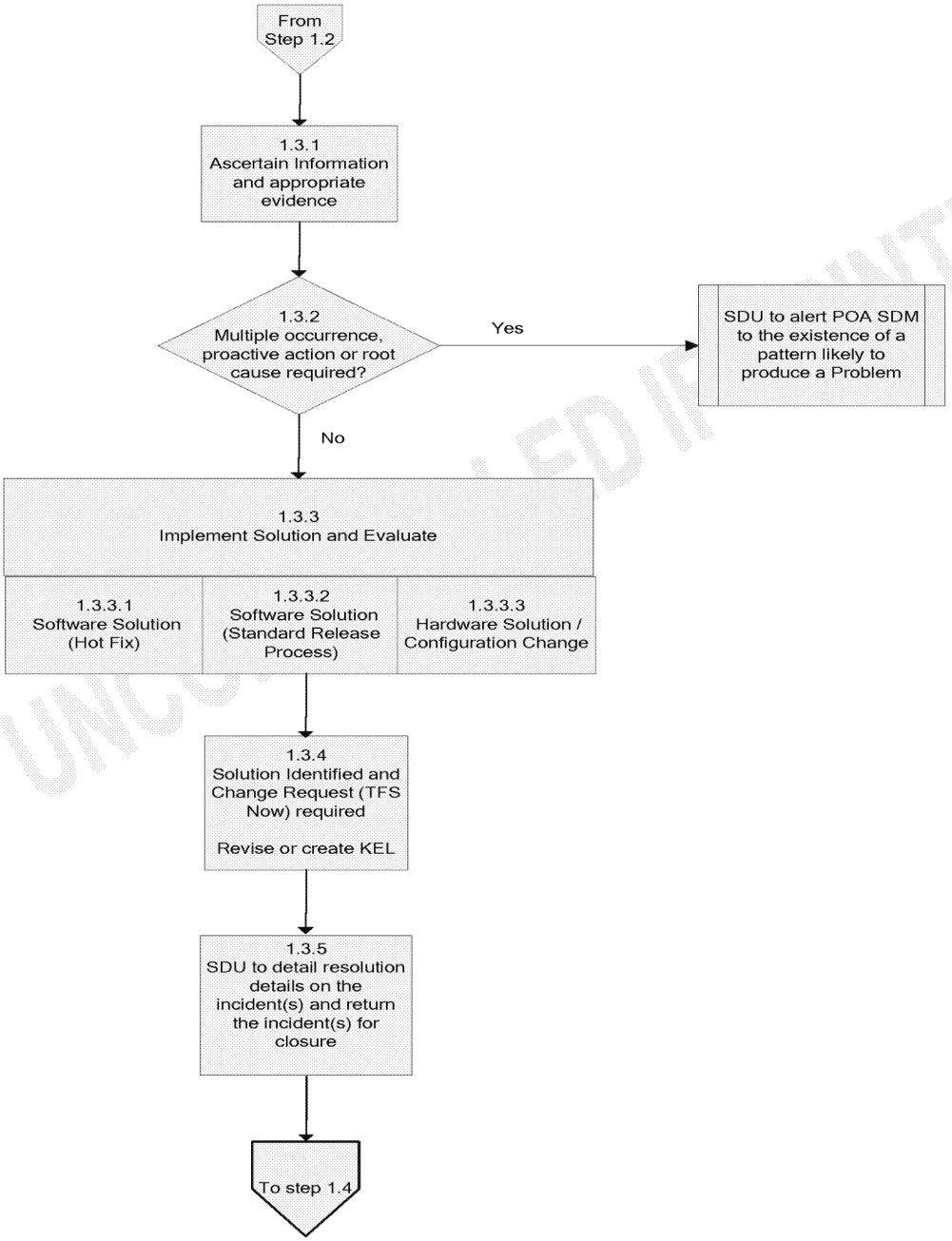


Figure 4: Resolution and Recovery

FUJ00234983

5.1.4 Step 1.4: Incident Closure

Responsible: MAC / SMC

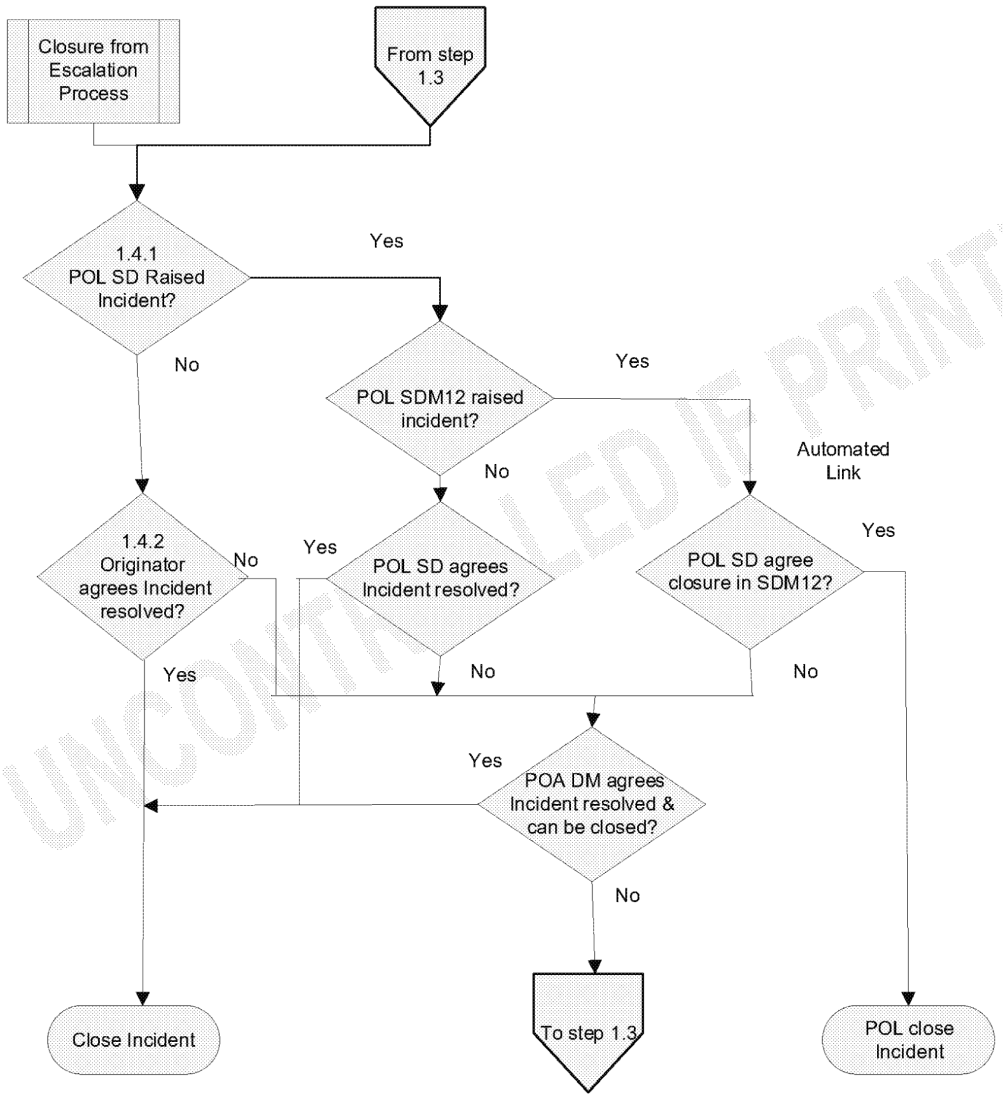


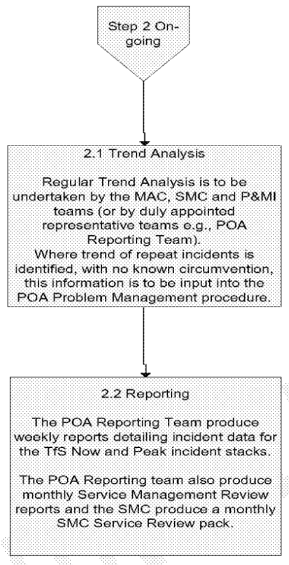
Figure 5: Incident Closure

FUJ00234983

5.1.5 Step 2: Trend Analysis and Reporting

Responsible: Reporting Team, MAC / SMC, P&MI

Figure 6: Trend Analysis and Reporting



FUJ00234983

5.1.6 Step 3: Ownership, Monitoring, Tracking and Communication

Responsible: MAC / SMC, SSC

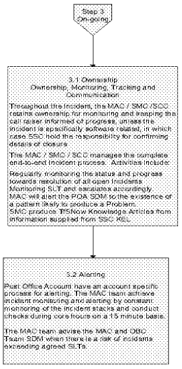


Figure 7: Ownership, Monitoring, Tracking and Communication

FUJ00234983

6 Outputs

The outputs from this process are:

- Where one or more Incidents has been raised for a failure for which the underlying cause is unknown and a trend is identified, consideration shall be given to raising it as a Problem.
- An update to the Knowledge Database
- A workaround or permanent resolution for a hardware, software or network error
- An answer to a question from a user
- The receipt and onward transfer of information received by the MAC / SMC
- A service improvement recommendation.
- Change of operations procedures.
- Change of Business Continuity Plan (BCP) priorities and documentation.

Where appropriate:

- Monthly Report on all PCI minor incidents
- Record in the Incident Security Portal.
- Individual reports for potential GDPR/PCI breaches such as AMEX EPA files (SSK)

7 Standards

This Process conforms to:

- ITIL Best Practice
- BS15000
- BS9001
- BS/ISO IEC 27001
- IEC 17799:2005
- PCI DSS version 1.2
- ISAE3402

8 Control Mechanisms

The contractual measures that apply to this service are described in the Service Management Service Description (SVM/SDM/SD/0007).

FUJ00234983

9 Appendix A: Security Incident Reporting

9.1 Scope

This annex contains **guidance** regarding the reporting and investigation of security incidents concerning the HORIZON Network, POA and any Payment Brand incident (PCI) and/or GDPR breaches such as the AMEX EPA files i.e. SSK not conforming to the Application Interface Specification due to naming or encryption inconsistencies.

9.2 Aim

The aim of this guidance is to ensure that the reporting routes for Security Incidents are kept as simple as possible and that investigations are managed in an efficient and auditable manner.

9.3 Changes

This guidance is primarily for use by the MAC team, the POA Security Team, the POL Security Team, and SSC staff. The SecOps team also have their own work instructions for handling security incidents and there is also an overarching Information Security Incident Management Procedure ISSC-11a.

All incident documentation is subject to review and update by the business continuity and information security teams as part of the lessons learnt process following an incident and following the annual review of the incident process as part of business continuity.

9.4 POL Incident Handling Guidance

All POL incidents will still be handled in accordance with existing POL guidelines. This document does not replace these or, indeed, replace any part of the content rather it details POA guidance on handling security incidents.

9.5 IT Incidents

9.5.1 Incident Definition

An information security Incident is: "an adverse event or series of events that compromises the confidentiality, integrity or availability of Fujitsu Services Post Office Account information or information technology assets, having an adverse impact on Fujitsu Services and/or Post Office Ltd reputation, brand, performance or ability to meet its regulatory or legal obligations." This will also extend to include assets entrusted to Fujitsu including data belonging to Post Office Ltd, its clients and its customers.

9.5.2 Incident Categories

Incidents can be categorised in many ways, they can occur alone or in combination with other incident categories and can vary significantly in severity and impact. It is important that all incidents are recognised and acted upon.

For the purpose of illustrating the impact of incidents two levels of severity have been defined (Note: in practice the assessment may be less straightforward):

A MINOR incident will normally have limited and localised impact and be confined to one domain, resulting in one or more of the following:

FUJ00234983

- Loss or unauthorised disclosure of internal or sensitive material leading to minor exposure, or minor damage of reputation
- Loss of integrity within the system application or data, leading minimal damage of reputation; minimal loss of customer / supplier / stakeholder confidence; negligible cost of recovery
- Loss of service availability within the domain, leading to reduced ability to conduct business as usual; negligible loss of revenue; minimal loss of customer / supplier / stakeholder confidence; negligible cost of recovery
- Individual attempts to breach network security controls shall be treated as a minor security breach.
- Subject to discussions with the POA Duty Manager due to high volume of calls relating to the same type of incident it may well be a requirement to follow the POA Major Incident Process (SVM/SDM/PRO/0001) following the advice from the POA Duty Manager.

A MAJOR incident will have a significant impact on the Network Banking Automation Community resulting in one of more of the following:

- Loss or unauthorised disclosure of confidential or strictly confidential material, leading to brand or reputation damage; legal action by employees, clients, customers, partners or other external parties
- Loss of integrity of the applications or data, leading to brand or reputation damage; loss of customer / supplier / client confidence; cost of recovery
- Loss of service availability for applications or communications networks, leading to an inability to conduct business as usual; loss of revenue; loss of customer / supplier / client confidence; cost of recovery
- A concerted attempt or a successful breach of network security controls shall be treated as a major security breach.
- Breach of Data Protection Legislation – inclusive of the GDPR, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and all other Applicable Law in respect of data protection and data privacy including any applicable guidance or codes of practice that are issued by the Information Commissioner, Working Party 29 and/or the European Data Protection Board (and each of their successors); For example AMEX sending EPA files, such as the SSK file not conforming to the Application Interface Specification owing to being unencrypted, resulting in GDPR/PCI data such as PAN numbers being in the clear.

NB. Also, please add the appropriate configuration item to the incident i.e. GDPR, PCI or PCI and GDPR. This will allow us to report against any incident where GDPR and/or PCI breaches have been identified.

NB. For a Major Incident the POA Major Incident Process (SVM/SDM/PRO/0001) should be followed.

9.5.3 Examples of IT Incidents

- Theft of IT equipment / property, including software
- Malicious damage to IT equipment /property, including software
- Theft or loss of Protectively Marked, caveat or sensitive IT Data
- Actual or suspected attacks on the Fujitsu Services POA Network or Information System
- Potential compromise of systems or services at the Data Centre through evidence retrieved and presented by Police or POL's card acquirer

FUJ00234983

- Attacks on Fujitsu Services Post Office Account personnel via Information Systems. (I.e. Harassment, Duress
- Malicious/offensive/threatening/obscene emails
- Obscene phone calls
- Breaches of software licensing
- Virus attack and other malicious code attacks
- Hacker attacks
- Terrorist attacks
- Insider attacks
- Competitive Intelligence gathering (Unethically)
- Unauthorised acts by employees
- Employee error
- Hardware or software malfunction
- Suspected Fraudulent Activity
- Specific compromise of card data.
- Files being sent to Fujitsu by 3rd party suppliers that don't conform to the Application Interface specification e.g. unencrypted AMEX EPA files (SSK), resulting in GDPR\PCI data such as PAN numbers being in clear.

The above list is a non-exhaustive list of examples. Any other IT related incidents reported, will be considered and passed to the appropriate authority for action.

9.5.4 Containment

Whenever an Incident is identified which presents a serious threat to conduct normal business it should be contained and isolated as quickly as possible. This will mean platforms that appear to have suffered virus attack or other malicious code attack need to be quarantined immediately to prevent further spread. It may also be necessary to isolate network connections that appear to be the source for Denial of Service threats or where they have been subjected to suspected hacking attack.

If the incident relates to card data, the environment may be subject to a Forensic Investigation imposed by POL's merchant acquirer. In this instance log data will need to be reviewed and analysed.

9.6 Reporting

Whenever a security incident is identified which presents a serious threat to conducting normal business it is contained and isolated as quickly as possible.

A security Incident is first notified to either the MAC or SMC Team, then transferred to the SecOPs call stack, once it is initially assessed as a Security Incident by MAC/SMC.

Security Incidents may also be reported directly into the POA SecOps team via the reporting button on the POA Portal. It is important to allow the 2 reporting methods, as some staff may want to report some types of security incidents directly to the SecOps team. The initial report will be validated and clarified by SecOps, with calls made to the initiator if more information is required. SecOps will follow team work instructions to progress their investigation.

FUJ00234983

All Security Incidents are to be reported to the SecOps team via a dedicated mailbox and escalated by phone if necessary. Depending on the type of Incident and the severity of the incident, POA Security makes the decision to escalate details to the POL Security teams. In the case of Data Centre incidents, POA Security also informs the Data Centre.

Regardless of the severity of the incident, when a compromise in card data occurs, the incident is reported to POL Security so that POL can comply with its contractual obligations with its card acquirer.

The investigation of a reported incident is carried out by a nominated investigator from the POA SecOps team. POL Security Teams will be on hand to provide support as required and in accordance with the POL Information Security Incident Management Procedure. The investigator will obtain as much original evidence as possible to ensure that is admissible in court, if required.

Following the initial investigation and where considered appropriate, the appropriate senior manager within POL liaises with the local Police or other external agencies.

When an investigation is closed the POA Security Manager seeks to ensure that details of the investigation have been recorded and can be made available for Route Cause Analysis, trending & lessons learned.

9.7 Investigation

9.7.1 Policy

Although all security incidents will initially be reported to the POA Security Manager in order to have one point of contact for all parties, some or all of the investigation requirements may be passed to one or more of the following for further action. The decision of delegation will be determined by the POA Security Manager in association with POL Information Security Incident Manager.

9.7.2 POL Security / Investigation Team

9.7.2.1

In the event that the reporting of an incident is passed to POL Security or the Investigation Team, details of the investigation, and final outcome or reference details, should be added to the TfSNow call which can be communicated to POL. It is important that for any incident investigated the correct procedures are adopted regarding evidence, as the information collected and recorded may be used for evidential purposes at a later date.

9.7.2.2

In the event that the POA Security Team takes ownership of an investigation, they will report the results to POL and Fujitsu Security team.

9.7.2.3

During any investigation the Investigator must comply with the appropriate legislation and compliance requirements and regulatory or standard requirements.

9.7.2.4

FUJ00234983

All initial investigations should be carried out at the earliest opportunity and any queries should be directed to POA Security Manager. Investigation must be reliable, stand up to scrutiny and potential cross-examination and evidence must be properly obtained, recorded and time stamped.

9.7.3 External Investigator

Should it be considered necessary the incident might be passed to an external Investigator or forensics team, who will ensure that any data required for evidential purposes is captured and investigated using a systematic approach which ensures that an auditable record of evidence is maintained and can be retrieved. In some cases, where a compromise to card data is involved, two Forensic Investigation teams may be involved. One team operating on behalf of POL gathering the required audit logs to use to analyse and investigate the problem. A second Forensic Investigations team may be imposed to investigate on behalf of the card acquirer and card schemes. In all incidents where a Forensic Investigation is involved, the Forensic Investigators will be shadowed by POL's Legal and Security Teams.

9.7.4 Evidence Rules

9.7.4.1 Rules of Evidence

Before undertaking security incident investigation and computer forensics it is essential that investigators have a thorough understanding of the Rules of Evidence. The submission of evidence in any type of legal proceedings generally amounts to a significant challenge, but when computers are involved the problems are intensified. Special knowledge is needed to locate and collect evidence, and special care is required to preserve and transport evidence. Evidence in computer crime cases differs from traditional forms of evidence in as much as most computer related evidence is intangible and is in the form of electronic pulse or magnetic charge, hence the need to use specialist teams. That said the information collected and recorded from the Operational areas is equally important and must be recorded with due care and diligence.

9.7.4.2 Types of Evidence

Many types of evidence can be offered in court to prove the truth or falsity of a given fact.

The most common forms of evidence are Direct, Real, Documentary and Demonstrative.

Direct Evidence

Direct evidence is oral testimony whereby the knowledge is obtained from any of the witness's five senses and is in itself proof or disproof of a fact in issue. Direct evidence is called to prove a specific act such as an eye witness statement.

Real Evidence

Real evidence also known as associative or physical evidence is made up of tangible evidence that proves or disproves guilt. Physical evidence includes such things as tools used in the crime, and perishable evidence capable of reproduction etc. The purpose of physical evidence is to link the suspect to the scene of the crime. It is that evidence that has material existence and can be presented to the view of the court and jury for consideration.

Documentary Evidence

Documentary evidence is presented to the court in forms of business records, manuals, printouts etc. Much of the evidence submitted in a computer crime case is documentary evidence.

Demonstrative Evidence

Demonstrative evidence is evidence used to aid the jury. It may be in the form of a model, experiment, chart or an illustration offered as proof.

FUJ00234983

9.7.5 Process

In most cases response to a reported incident the initial investigation will be carried out by a nominated investigator normally the POA Security Manager or a member of the SecOps team. POL Security Teams will be on hand to provide backup and assistance if required. When seizing evidence from a computer related crime the investigator will collect any and all physical evidence such as the personnel computer, peripherals, notepads and documentation etc., in addition to computer generated evidence.

There are four types of computer generated evidence:

- Visual output on a monitor.
- Printed evidence on a plotter.
- Printed evidence on a printer.
- Film recordings on such digital media as disc, USB stick, log files, tape or cartridge, and optical representation on either CD or DVD.

The investigator will endeavour to obtain as much original evidence as possible. In the event of a court appearance the court prefers the original evidence rather that a copy but will accept a duplicate if the original is lost or destroyed or is in the possession of a third party who cannot be subpoenaed.

9.7.5.1

Following the initial investigation and where considered appropriate, the investigator will report to/ liaise with the local Police and/or other external Agencies; this will only be done following consultation with the POL Head of Security and POL Head of Information Security or substitute.

Copies of the initial and follow up reports will be submitted to relevant authorities and details of all investigations will be held on file by the POA Security to aid any subsequent trend analysis.

9.8 Remedial Action

9.8.1 On Completion of report

When the final report of an investigation has been completed, it should be passed to the relevant authority for follow up action, the results of which should be referred back to the POA Security Manager.

9.8.2 Completion of Investigation

When an investigation is closed the POA Security Manager will ensure all details of the investigation have been recorded and can be made available for subsequent future analysis.

9.9 Trends & Auditing

9.9.1 Frequency

9.9.1.1

POA Security Team carries out a monthly check of investigations and creates a summary report highlighting incidents to the POL Head of Information Security.

The report highlights trends or weaknesses which may need to be raised at future Information Security Management Forums (ISMF). POA will also submit a quarterly report to the Fujitsu Security Management Forum, to ensure that Fujitsu Security Incident trends can be reviewed in the round.

FUJ00234983

10 Appendix B Contacts

10.1.1 Security Incidents

- Jason Muir – GRO (POA Information Security Manager)

10.1.2 Major Incident Manager Contact Details

- Matthew Hatch – GRO
- Sandie Bothick – GRO
- Sonia Hussain – GRO
- Steve Bansal – GRO

10.1.3 Out of Hours Duty Manager Contact Details

Please refer to Account Call Out Rota for the applicable OOH Duty Manager

- Sandie Bothick – GRO
- Andy Hemingway – GRO
- Ramana Ravula – GRO
- Matthew Hatch – GRO

17.30 - 09.00 Monday PM to Thursday AM

17.00 - 09.00 Friday PM to Monday AM

Outside these times, please contact the Major Incident Manager

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

10.1.4 POA Service Delivery Manager Contact Details

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