FUJ00080298

Document Title:	POA Operations Incident Management Procedure
Document Type:	Procedure Definition
Release:	Not applicable
Abstract:	This document describes the POA Operations Incident Management Procedure
Document Status:	APPROVED This document contains sections that have been identified to POL as comprising evidence to support the assessment of named Acceptance Criteria by Document Review. These sections must not be changed without authority from the FS Acceptance Manager
Author & Dept:	Tony Wicks – POA Operations
Internal Distribution:	Peter Thompson, Tony Atkinson, Steve Bansal, Steve Gardiner, Steve Parker, Leighton Machin, Steve Evans, Changdev Pawashe, Andy Hemingway, Gaby Reynolds, Simon Edmondson, Yannis Symvoulidis, Roger Stearn, Catherine Obeng, Kumudu Amaratunga, Sandie Bothick, Bill Membery, Chris Harrison
External Distribution:	Rebecca Barker, POL Business Continuity Manager Dave King, POL Security Manager
Security Risk Assessment Confirmed:	Yes

Approval Authorities:

Name	Role	See Dimensions for record
Steve Bansal	POA Tower Lead BAS (Interim)	
Sandie Bothick	POA MAC Team Manager	

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

FUJ00080298

0 Document Control

0.1 Table of Contents

FUJ00080298

FUJ00080298

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 Paul Halliden	
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.	

FUJ00080298

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
		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 Brand incident (PCI)	
7.0	17-Jul-14	Incorporates minor amendments	

0.3 Review Details

Review Comments by :	
Review Comments to :	Tony Wicks
Mandatory Review	
Role	Name
POA Tower Lead BAS (Interim)	Steve Bansal
POA MAC Team Manager	Sandie Bothick
POA Acceptance Manager	Steve Evans
Optional Review	
Role	Name
POA Infrastructure Operations Manager	Andy Hemingway
POA Business Continuity Manager	Changdev Pawashe,
POA Lead SDM Managed Infrastructure Services	Leighton Machin
POA POLSAP and Online Services SDM	Gaby Reynolds
POA Credence and Sales force SDM	Simon Edmondson
POA SDM Networks	Roger Stearn
POA SMC Manager	Catherine Obeng
POA Security Manager	Kumudu Amaratunga
POA Quality Compliance and Risk Manager	Bill Membery
POA Lead SDM Online Services	Yannis Symvoulidis
POA Problem Manager	Steve Gardiner
POA Engineering SDM	Chris Harrison
Post Office Ltd	
Security Manager	Dave King
Business Continuity Manager	Antonio Jamasb

(*) = Reviewers that returned comments

FUJ00080298

0.4 Acceptance by Document Review

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

POL NFR DR Acceptance Ref	Internal FS POL NFR Reference	Document Section Number	Document Section Heading
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
CS/PRO/110			POA Problem Management Database Procedures	PVCS
PA/PRO/001			Change Control Process	PVCS
CS/QMS/001			Customer Service Policy Manual	PVCS
SVM/SDM/SD/0001			Service Desk – Service Description	Dimensions
SVM/SDM/SD/0023			POA Call Enquiry Matrix and Incident Prioritisation	Dimensions
CS/REQ/025			Horizon HSD / SMC: Requirements Definition	PVCS
SVM/SDM/PRO/0001			POA Customer Service Major Incident Process	Dimensions
SVM/SDM/PLA/1048			SMC Business Continuity Plan	Dimensions
SVM/SDM/SD/0002			Engineering Service Description	Dimensions
SVM/SDM/PLA/0031			Security Business Continuity Plan	Dimensions
C-MSv1.3			Manage Incidents Process	BMS
C-MSv_roles			Service Management Process Roles and Responsibilities	BMS

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

FUJ00080298

0.6 Abbreviations

Abbreviation	Definition
A+G	Advice & Guidance
BCP	Business Continuity Plan
BMS	Business Management System
CISO	Chief Information Security Officer
CPP	Common Point of Purchase
FI	Forensic Investigator
HDI	Help Desk Interface (between Atos SDM12 and TfS incident management systems)
ICR	Initial Case Report
ISO	International Standards Organisation
ITIL	Information Technology Infrastructure Library
KA	Knowledge Article also known as KEL
KEDB	Known Error Database
KEL	Known Error Log (in the context of this document, this is a workaround and diagnostic database) (Theses are also known as Knowledge Articles.)
MAC	Major Account Controllers (MAC team)
MSU	Management Support Unit
OLA	Operational Level Agreement
OMDB	Operational Management Database
ORF	Operational Review Forum
OTI	Open Teleservice Interface
PCI	Payment Card Industry
PCI DSS	Payment Card Industry Data Security Standard
PO	Post Office
POL	Post Office Limited
PSE	Product Support Engineers
RFC	Request For Change
POA	Post Office Account
SAN	Storage Area Network
SAP	Systems, Applications and Products (in Data Processing)
SDM(s)	Service Delivery Manager(s)
SDU	Service Delivery Unit
SISD	Service Integrator Service Desk (Atos Service Desk)
SLT	Service Level Targets

FUJ00080298

Abbreviation	Definition
SMC	Systems Management Centre
SMT	Service Management Team
SRRC	Service Resilience & Recovery Catalogue
SSC	System Support Centre
TfS	Triole for Services
UNIRAS	Unified Incident Reporting & Alerting System
VIP	VIP Post Office, High Profile Outlet

0.7 Glossary

Term	Definition
Common Point of Purchase	A location identified by card schemes as a single point where a number of stolen cards were used before the card was involved in fraudulent activity.
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 TfS call management system.

0.8 Changes Expected

Changes

0.9 Accuracy

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

0.10 Copyright

FUJ00080298

1 Introduction

1.1 Owner

The owner of the Incident Management process at the local POA account level is the Fujitsu POA Service Delivery Manager responsible for Incident Management within the POA account.

1.2 Objective

The objective of this document is to define the procedure for Incident Management in the POA environment. The procedure is the local implementation of the Fujitsu corporate Incident Management process (C-MSv1.3). Reference to process in this document is within the context of the corporate document C-MSv1.3. 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 Atos Service Desk are transferred/ referred from POA MAC / SMC to Atos Service Desk.

For clarity; Post Office Limited (the customer) appointed Atos as their Service Integrator including the primary service desk function (Atos Service Desk, which may also be referred to as SISD).

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

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 (C-MSv1.3)

- 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

1.3 Process Rationale

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

FUJ00080298

service quality and availability. Normal service operation is defined here as service operation within Service Level Targets (SLT).

Demonstrating a professional approach to Atos, the Service Integrator contracted to POL, and Post Office Limited (the customer) and their clients.

1.4 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 Atos 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.

FUJ00080298

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 the Atos 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
  - Logging via HNG-X web interface
- 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 3, and are not subject to steps 1 & 2 of this process.

FUJ00080298

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.
- 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 Atos Service Desk.
- Non-availability of the OTI links to core & external service desk tools.
- Lack of information given to the MAC / SMC regarding changes, Atos or 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
- Unavailability of sufficient tools for Incident diagnosis
- Non-availability of KEL or call management systems
- 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 of desk agents.
- 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 ORFs, 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

FUJ00080298

4 Resources

The resources required for this process are:

- Process Owners
- Major Account Controllers team
- Service Management Team
- System Management Centre team
- SSC
- SDUs
- Triole for Service incident management system
- Peak
- SDM12 (within Atos) and the HDI interface into TfS.
- Despatch 1
- TIVOLI
- Additional remote Management, Operational and Diagnostic tools
- Detailed Process and Procedure documentation

4.1 Roles

The main roles required by the process are:

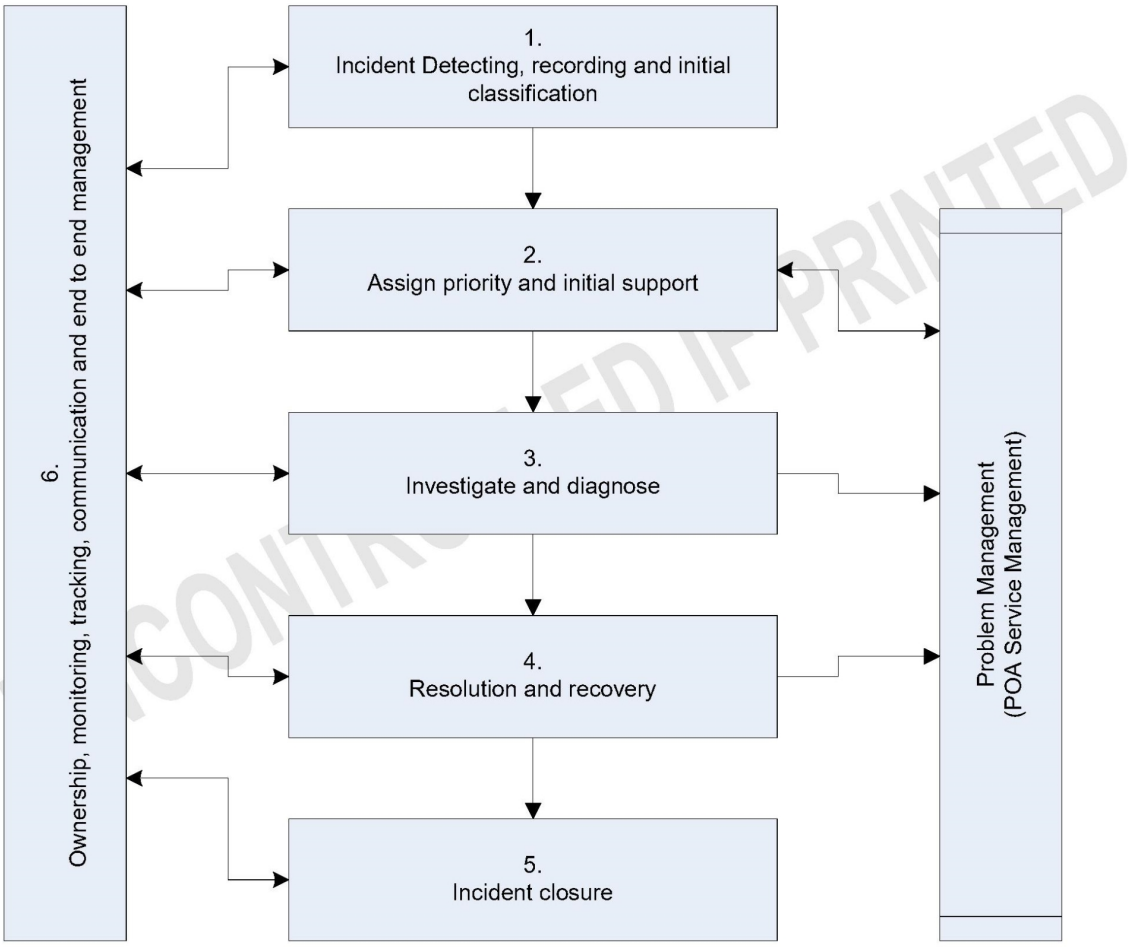
- Incident Manager - To drive the Incident Management process, monitor its effectiveness and make recommendations for improvement. The key objective is to ensure that service is improved through the efficient resolution of Incidents.
- Service Desk Agent - To provide a single point of contact for users, dealing with the management of routine and non- routine Incidents, Problems and requests
- Incident Resolver - To accurately diagnose and resolve Incidents and Problems within SLA, 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.

Detailed definitions of each role include activities and key performance indicators are in the Fujitsu "Service Management Process Roles and Responsibilities" (C-MSv_roles).

FUJ00080298

5 Process Flow

5.1 Level 1 Incident Management Process

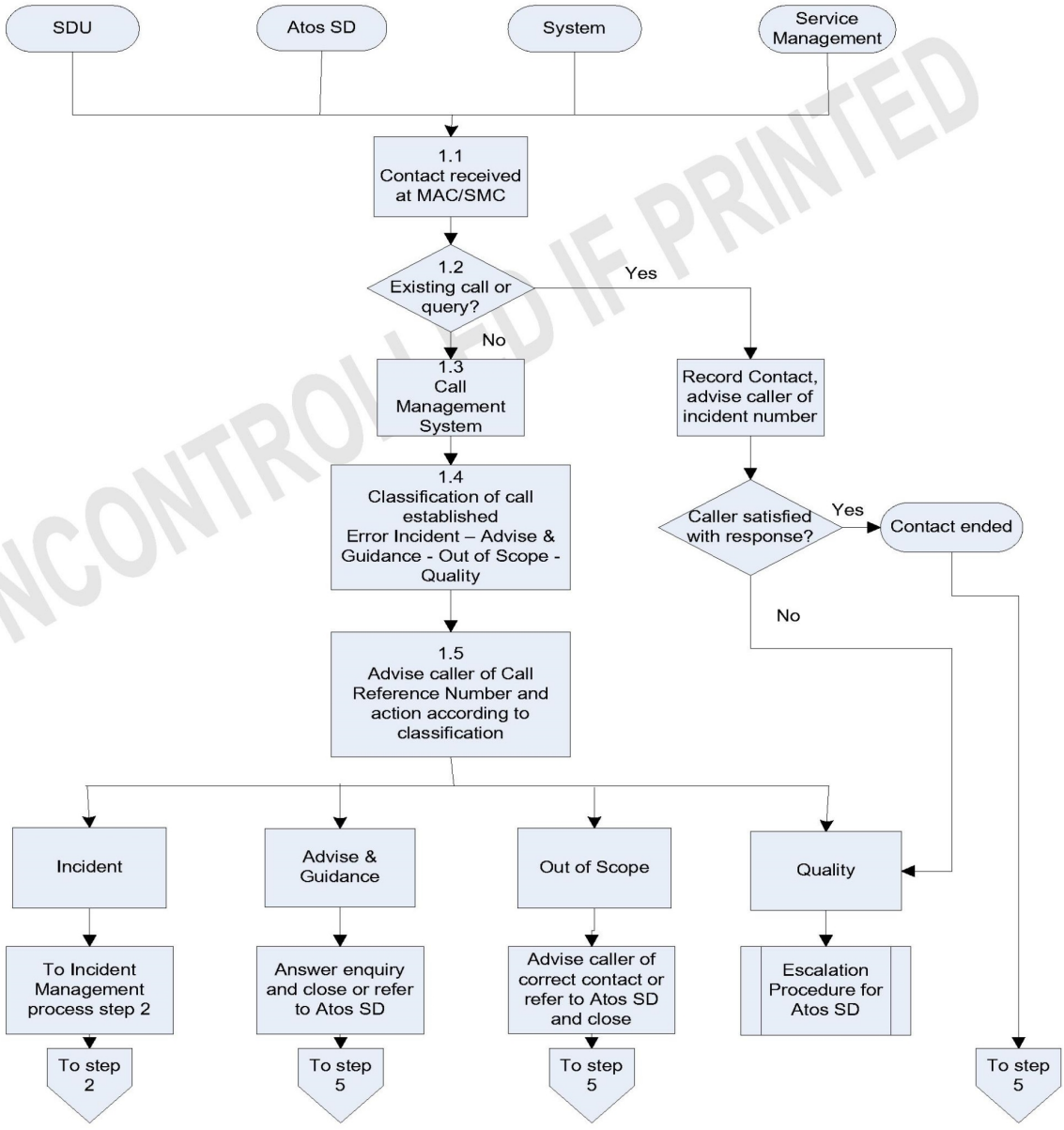


FUJ00080298

5.2 Level 2 Incident Management Processes

5.2.1 Step 1: Incident Detecting, Recording and Initial Classification

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



FUJ00080298

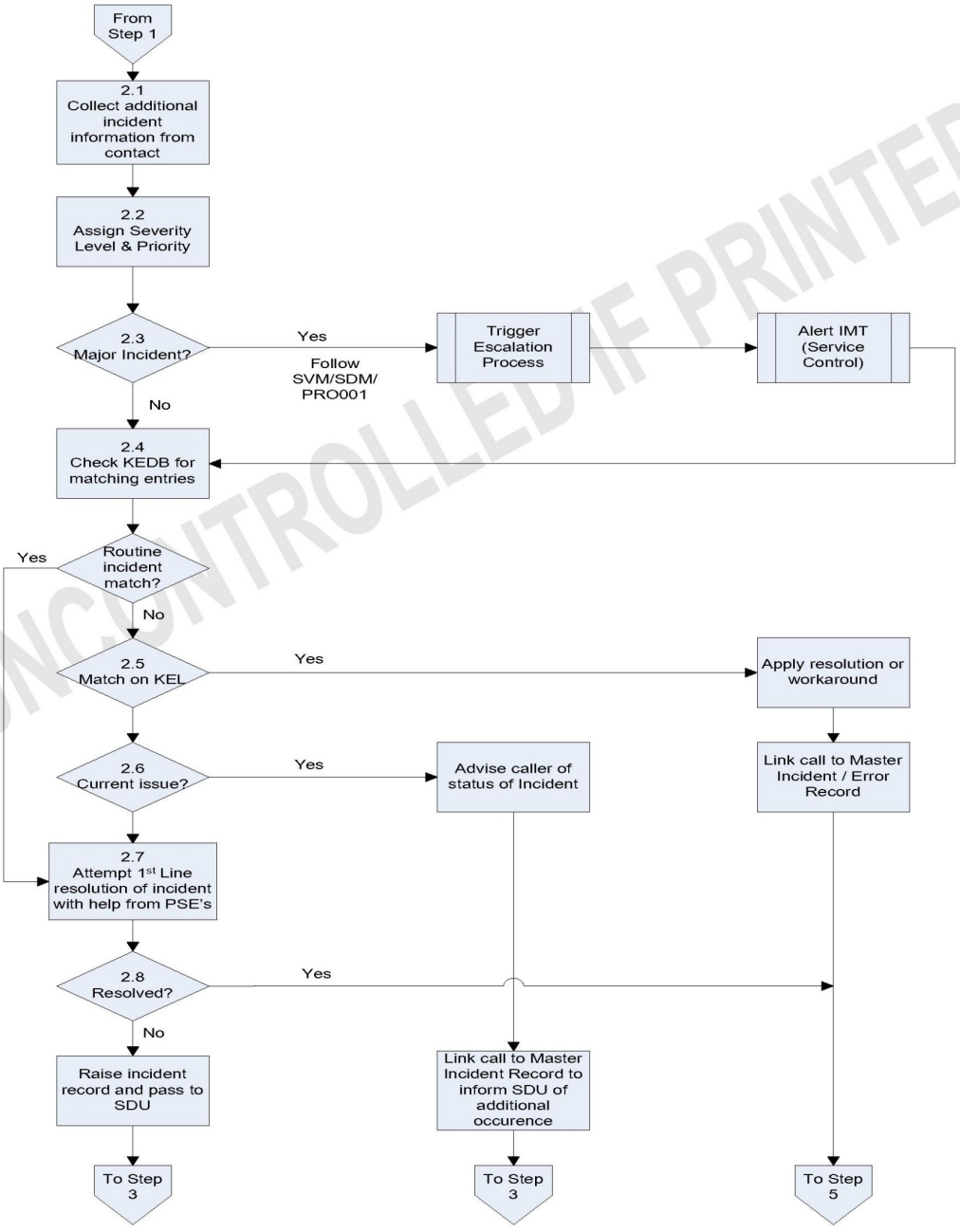
1	Incident Detecting, Recording and Initial Classification			
Step No	**Current Situation/Input**	**Activities**	**Accountability Responsibility**	**Next Step**
1.1	Incident information provided	An Incident is received through contact (see definition in Section 2.0 above) with the MAC / SMC from: Atos SD Fujitsu SDUs POA IT Service Management Third Parties Fujitsu Service Delivery Management Post Office Ltd, including POL Information Security For Ownership, Monitoring, Tracking and Communication by the MAC/SMC/SSC see section 5.2.6 below	See specifics under Activities	1.2
1.2	Incident information / details provided	The caller may be enquiring about an existing Incident. Details are provided and if the response is satisfactory, contact is ended, moving the incident to step 5. If the caller is not satisfied with the response, the relevant Escalation Procedure is invoked. In cases of Incidents that are either taking an above average time (for this type of Incident) to resolve or involve multiple SDU's, the MAC / SMC alerts the relevant Service Delivery Manager to provide focused management of the Incident.	MAC, SMC	1.3 or 5
1.3	New incident details from Incident Initiator	For a new Incident, Contact details are recorded if not system generated, e.g., an Atos SD SDM12 incident. Details taken are dependent upon the error reported. Typically they may include: The user's name and unique ID number Location and contact details Alternative contact details (where appropriate) Hardware details as appropriate Software error details, including application use at point of failure where known Business and User Impact Description of Incident Location access times Caller assessment of the priority of the incident.	MAC, SMC	1.4
1.4	Classify the incident	Classification of Call determined as one of the following: Error Incident – invoke Incident Management Process Step 2 Quality – record details of complaint or compliment and invoke the relevant Escalation Procedure. Advice & Guidance – Cold Transfer to Atos SD. Out of scope – if the call is not within scope for the services provided by Fujitsu advise the caller of the correct number or refer to Atos SD and close incident.	MAC, SMC	1.5
1.5	Provide Incident	The caller is advised of call reference number and the incident follows the process as appropriate for the nature of the call.	MAC, SMC	2

FUJ00080298

	Reference			

5.2.2 Step 2: Assign Priority and Initial Support

Responsible: MAC / SMC



FUJ00080298

2	Assign Priority and Initial Support			
Step No	**Current Situation /Input**	**Activities**	**Accountability/ Responsibility**	**Next Step**
2.1	Further incident information requested	The MAC / SMC agent collects additional information in order to determine the nature, impact and urgency of the Incident.	MAC, SMC	2.2
2.2	Severity and Priority allocated	Call Severity is assigned based on the impact and urgency as per the criteria in the table below. Call Priority for Hardware and Network calls is assigned in accordance with the Priority matrix as detailed in Engineering Service Description (SVM/SDM/SD/0002), a copy of which each agent should have on their desk. (See the following table in this section.)	MAC, SMC	2.3
2.3	Is Major Incident trigger met?	If the incident is considered a Major Incident as defined in SVM/SDM/PRO/0001 Major Incident Process, the Major Incident Procedures are invoked.	MAC, SMC	2.4
2.4	Check Known Error Database or is there a known resolution?	The MAC / SMC agent then attempts to resolve the Incident using the resources available. This starts by interrogating the MAC / SMC knowledge database to find all information related to the Incident symptoms. If the Incident is routine, i.e. there is a predetermined route for resolution, then the Incident is resolved on the call or referred to the relevant SDU using the MAC / SMC Support Matrix.	MAC, SMC	2.5
2.5	Provide user with KEL details if applicable	If the Incident is not routine, the MAC / SMC agent checks for Known Errors listed in the SSC KEL against records relating to the Incident symptoms. If a match is found, the agent informs the caller of the workaround or resolution available.	MAC, SMC	2.6
2.6	Check for Parent incident?	If there is no match in MAC / SMC knowledge database or the SSC KEL, the MAC / SMC Incident Management System stack is checked for current incidents outstanding. If a match is made, the caller is then advised of the status of the incident and the master record is updated to reflect the current occurrence.	MAC, SMC	2.7
2.7	Liaise with PSE to seek incident resolution	If no match is made against the MAC / SMC Incident Management System stack, the MAC / SMC continues with first line resolution of the Incident assisted by the Product Support Engineers (PSE's). MAC are appraised of the position.	MAC, SMC	2.8
2.8	Refer to Support Matrix and transfer to appropriate SDU	If the PSE's cannot resolve the Incident, it is referred to the relevant SDU using the MAC / SMC Support Matrix. MAC are appraised of the position. For Hardware calls, the caller is given an indication of engineer arrival time, based on the SLA associated with the priority of the call.	MAC, SMC	3

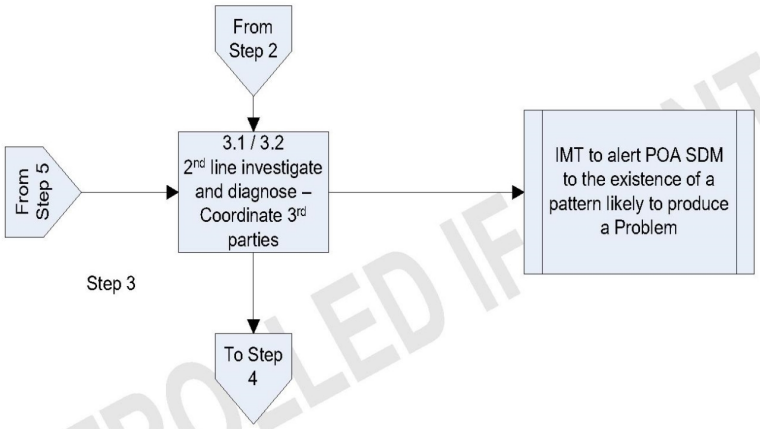
FUJ00080298

Severity	Importance	Definition
1	Critical	• BUSINESS STOPPED, a Post Office unable to trade (where engineering cover available), unable to process any business, or central system failure which will result in a number of Post Offices being unable to process work. • Causes significant financial loss (as agreed between POL and POA Operations) • Results in data corruption or unrecoverable data loss.
2	Major	• BUSINESS RESTRICTED, a Post Office restricted in its ability to transact business e.g. 50% of counters unable to trade or trading with restricted business capability. • Has an adverse impact on the delivery of service to a number of end users. • Causes a financial loss that impacts POL and/or POA reputation (as agreed between POL and POA Customer Services) • If a PCI Major Incident process is invoked
3	Medium	• NON-CRITICAL, a Post Office working normally but with a known disability, e.g. an interim solution (workaround) has been provided. • If a PCI Minor Incident process is invoked • Has a minor adverse impact upon the delivery of service to a small number of end users
4 or 5	Low	• Non-urgent • Insignificant and usually cosmetic error, either a trivial documentation error or spelling error on the system.

FUJ00080298

5.2.3 Step 3: Investigation and Diagnosis

Responsible: SDU's



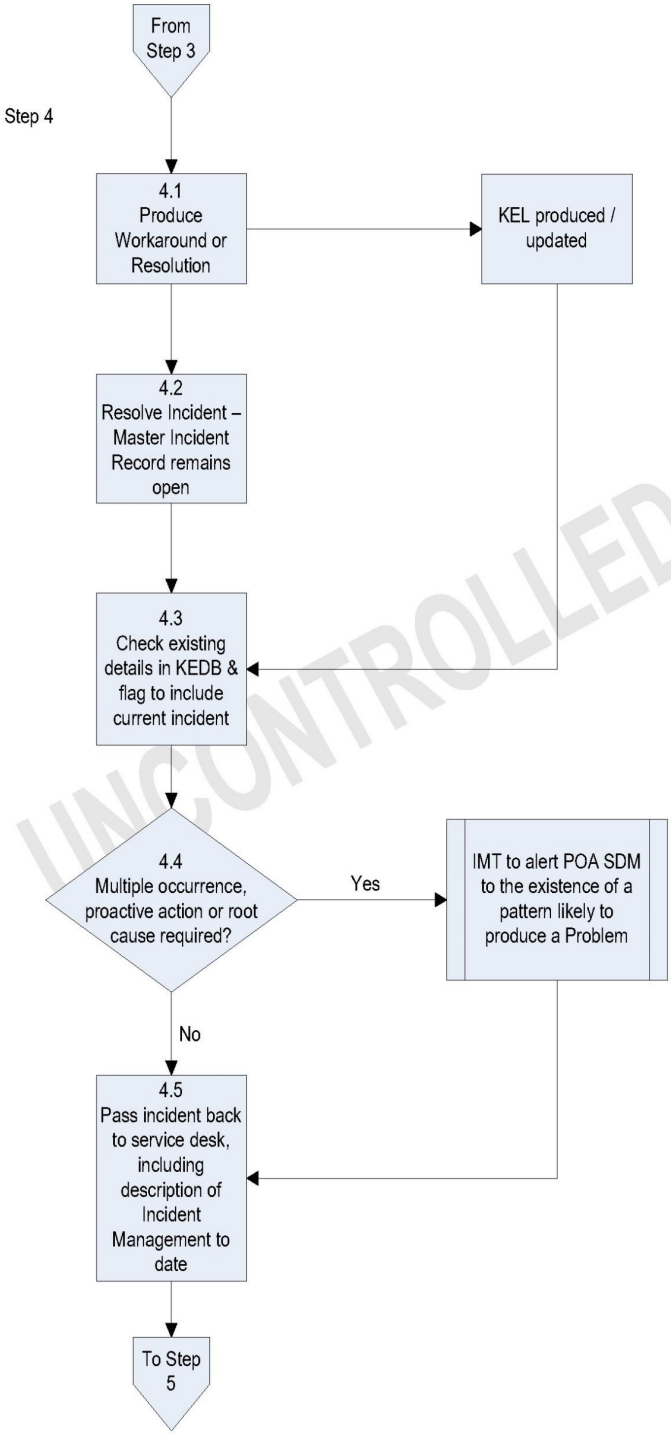
FUJ00080298

3	Investigation and Diagnosis			
Step No	**Current Situation/Input**	**Activities**	**Accountability/ Responsibility**	**Next Step**
3.1	Second line support stage. SDU investigation	The referred SDU investigates and diagnoses the Incident, based on information already taken by the MAC / SMC, together with any new information. The SDU also coordinates where sub-contract third parties are involved. If the Incident has no associated KEL, or it is complex and involves multiple SDU's, or if it has been unresolved for an extended period, the MAC will alert the POA Service Delivery Manager to the existence of a pattern likely to produce a Problem.	Second Line SDU	4
3.2	Out of hours Support SMC	SMC should check the OLA documentation to determine if out of hours support is available for the Service impacted. In the event that out of hours support is available, SMC will discuss incidents with the Duty Manager, who in turn will discuss incidents with the line of business SDM.	SMC	4

5.2.4 Step 4: Resolution and Recovery

Responsible: SDU's

FUJ00080298



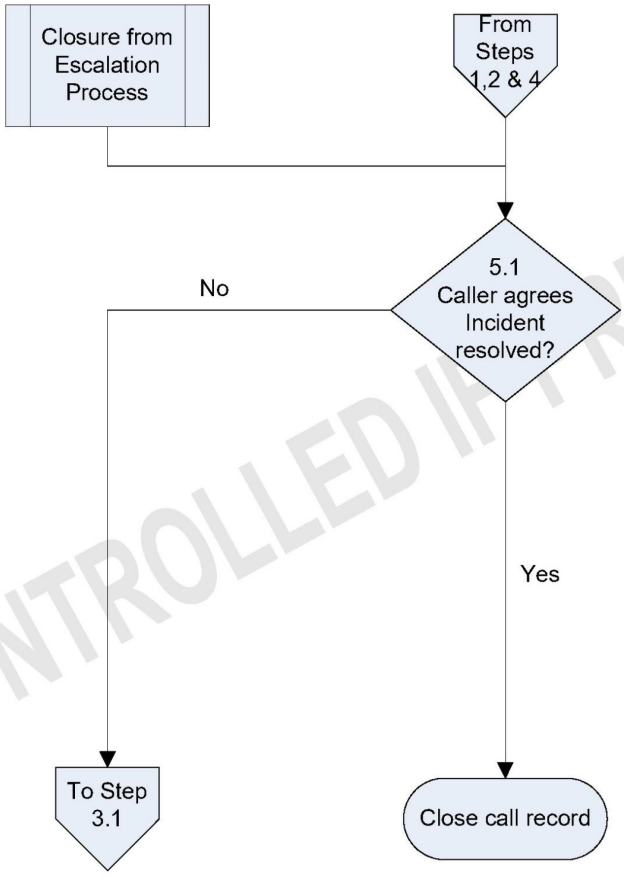
FUJ00080298

4	Resolution and Recovery			
Step No	**Current Situation/Input**	**Activities**	**Accountability/ Responsibility**	**Next Step**
4.1	SDU investigates incident following local processes	SDU investigates the incident, diagnose the cause and possibly identify and produce either a workaround or resolution.	SDU	4.2
4.2	Provide resolution	The SDU then either applies the workaround or resolution or passes it to the MAC/ SMC to implement. The Master Incident Record (if one exists) remains open at this point.(The incident should be set to resolved in this step (awaiting the User's agreement it can be closed in section 5.1)	SDU and MAC , SMC	4.3
4.3	SDU seek confirmation of resolution update KELs if applicable.	The SDU checks the workaround or resolution has been successful. MAC / SMC are responsible for updating details recorded in MAC / SMC knowledge database, from details supplied via the KEL created by SSC. MAC / SMC knowledge database should be identical to SSC KEL in relation to Application Software, but may also contain additional information.	SDU and MAC, SMC	4.4
4.4	MAC looks for Child Incidents or incident trends	If this is a Parent Incident, i.e., it has a number of child incidents linked to it, or where there is a probability that proactive action is required to prevent further occurrences of this Incident the MAC will alert the POA SDM to the existence of a pattern likely to produce a Problem	MAC	4.5
4.5	Invoke incident closure processes	The Incident is then passed to the MAC / SMC to manage the closure	MAC, SMC	5.1 or 5.2

FUJ00080298

5.2.5 Step 5: Incident Closure

Responsible: MAC / SMC



5

5	INCIDENT CLOSURE			
Step No	**Current Situation/ Input**	**Activities**	**Accountability / Responsibility**	**Next Step**
5.1	MAC managed incidents	For incident raised by the MAC for the Atos SD the MAC will liaise with the Atos SD and POA Duty Manager on the closure of the incident. If closure is not agreed the incident shall be returned to the SDU to be reworked.	MAC	End
5.2	MAC/SMC managed incidents	The incident may now be closed with the agreement of the originator. If closure is not agreed the incident shall be returned to the SDU to be	MAC, SMC	End

FUJ00080298

		reworked.		

5.2.6 Step 6: Ownership, Monitoring, Tracking and Communication

Responsible: MAC / SMC, SSC

Throughout the Incident, the MAC / SMC retains ownership for monitoring and keeping the call raiser informed of progress, unless the incident is specifically software related, in which case SSC hold the responsibility for confirming details of closure.

The MAC / SMC manages the complete end-to-end Incident process.

Activities include:

Regularly monitoring the status and progress towards resolution of all open Incidents
Note Incidents that move between different specialist support groups, indicative of uncertainty and possibly a dispute between support staff
Give priority for Incident monitoring to high-impact Incidents
Keep affected users informed of progress without waiting for them to call, thus creating a pro-active profile
Monitors SLT and escalates accordingly. If an Incident has no associated KEL or, it is complex and involves multiple SDU's, or if it has been unresolved for an extended period, MAC will alert the POA SDM to the existence of a pattern likely to produce a Problem.
Updating MAC / SMC TfS Knowledge Articles from information supplied from SSC KEL. This may be applied as a direct copy or amended for use by the agents, dependant upon the technical complexity of the update.

FUJ00080298

6 Outputs

The outputs from this process are:

- A Problem referred to the Service Delivery Manager with line of business responsibility, where there have been one or more Incidents for which the underlying cause is unknown
- 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
- ICR (Initial Case Report)
- Record in the Incident Security Log

FUJ00080298

7 Standards

This Process conforms to:

- Process Management and Control PA/PRO/038
- ITIL Best Practice
- BS15000
- BS9001
- BS/ISO IEC 27001
- IEC 17799:2005
- PCI DSS version 1.2

FUJ00080298

8 Control Mechanisms

The contractual measures that apply to this service are described in the Service Desk Service Description (SVM/SDM/SD/0001)

This covers service availability, service principles, service definition, incident prioritisation, service targets and limits and MAC / SMC performance reporting.

In addition, internal measures may apply for specific productivity and service improvement activities.

FUJ00080298

9 Appendix A: Security Incident Reporting

9.1 Scope

This annex outlines the process regarding the investigation, and reporting of all security incidents concerning the HORIZON Network and all IT equipment, and any Payment Brand incident (PCI).

9.2 Aim

The aim of these instructions is to ensure that details of all IT related security incidents are reported to one central point and that any follow up investigations are managed in an efficient and auditable manner.

9.3 Changes

These work instructions are primarily for use by the MAC team, the POA Security Team, the POL Security Team, and SSC staff. Approval from POL is to be gained before any significant changes to the work instructions are implemented. All readers are encouraged to propose changes to Work Instructions, in writing, to the POA Security Manager.

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 lays down the POA framework under which the work is carried out.

9.5 IT Incidents

9.5.1 Incident Definition

9.5.1.1 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.

FUJ00080298

9.5.2.1 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:

- 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.

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.
- Attacks on Fujitsu Services Post Office Account personnel via Information Systems. (I.e. Harassment, Duress

FUJ00080298

- 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.

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.

FUJ00080298

9.6 Reporting

9.6.1.1 Anyone reporting a security Incident should be encouraged to notify their Line Manager in the first instance. The Line Manager will gather as much detail of the incident as possible, following company procedures. He or she will undertake an initial local investigation into the incident, ensuring that in the case of missing equipment or materials that they have not just been misplaced. Information gathered will be entered into the initial case report template (ICR).

9.6.1.2 If the severity of the Incident is considered as Minor but warrants further investigation the Line Manager should immediately log a call with the MAC team, stating that they are reporting a security incident, giving brief details. Please note that in certain cases there may be circumstances where no details of a sensitive nature should appear on the call log. Having logged the call and obtained a call reference number, the Line Manager may then continue with the investigation, and act as a liaison between the person reporting and all concerned parties. Once logged, the investigation will thereafter be referred to by the Call Number.

9.6.1.3 All Incidents reported to the MAC team with a call reference and even when classified as Minor should still be forwarded to POA Security Management to determine if there is a Security Impact. 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

9.6.1.4 If the severity of the Incident is considered as Major the Incident details must be reported directly to the POA Security Manager immediately. Contact details are available on Café VIK. Depending on the type of Incident and the severity of the incident POA Security will make the decision to escalate the details to the POL Security. In the case of Data Centre incidents specifically Security will also inform the Data Centre Manager if this has not already been done. Regardless of the severity of the incident, when a compromise in card data occurs the incident must be reported to POL Security so that POL can comply with it's contractual obligations with it's card acquirer.

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

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

9.6.1.6 In all cases relevant details should only be recorded and discussed as necessary between the person investigating or Line Manager dealing with it and any relevant parties who need to be included in the investigation. Information on any incident must not be passed to anyone who is not directly involved with the investigation without the authority of POA Security Manager and the POL Head of Information Security.

9.6.1.7 Once a call is raised with the SSC the call will then be placed on the call stack of the POA Security Team, who will monitor the incident, assist or advise the Line Manager if required, and be available to take over the investigation should the need arise, but always be able to respond, within 2

FUJ00080298

hours of the initial call being made. (Minor Incidents (during normal working hours of between 9am and 5pm) and Major Incidents at all times.)

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, all details of the investigation, and final outcome or reference details, should be recorded on the initial case report (ICR) and details will be recorded in the security Incident Log. 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 Manager takes ownership of an investigation, he will report the results to POL Head of Information Security and POL's Business Continuity Manager.

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 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.

FUJ00080298

9.7.3 External Investigator

9.7.3.1 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 incidences 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.

FUJ00080298

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 his nominated deputy. POA and 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.

9.7.5.2 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.

9.8.3 UNIRAS Reporting

On call closure, the POA Security Team will complete and notify UNIRAS where required. Thereafter the incident will be reviewed to identify the lessons learnt and the processes and relevant documentation will be updated as appropriate.

FUJ00080298

9.9 TRENDS & AUDITING

9.9.1 Frequency

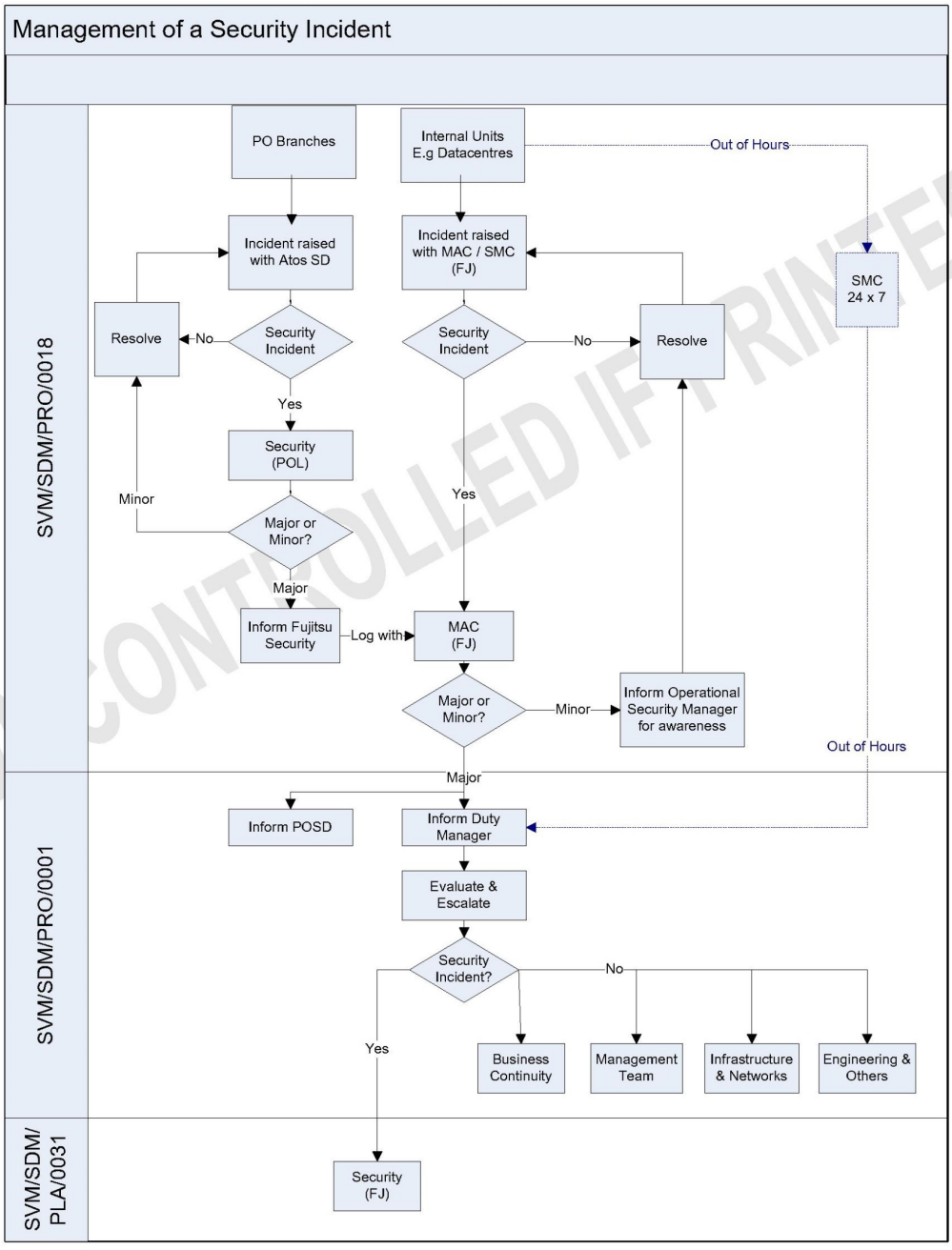
9.9.1.1 POA Security Team will carry out a monthly check of all investigations and create a summary report highlighting all incidents to the POL Head of Information Security.

9.9.1.2 The report will highlight any trends or weaknesses which may need to be raised at future Information Security Management Forums (ISMF).

9.9.1.3 Details from the monthly reports may also be considered suitable for Line Managers.

FUJ00080298

Appendix B Security Incident Process flow



Note: This diagram has only been provided an overview of the relationship between incident processes and the HNG-X Business Continuity Security Plan. **Included for guidance purposes only.**

FUJ00080298

Appendix C Security Incident Report Template

Identification						
Transition:				**Incident ID**		
Period:	**From:**		**To:**		**Reported:**	
Manager:					**Date:**	
Operational Security Report					**Overall Status:**	
Incident Details						
Further Action						
Lessons Learnt & Recommendations for Future Actions						

FUJ00080298

Appendix D Contacts

Security Incidents

- Kumudu Amaratunga – GRO **(Operational Security Manager)**

Major Incident Manager Contact Details

- Steve Gardiner – GRO
- Steve Bansal – GRO
- Tony Wicks – GRO

Out of Hours Duty Manager Contact Details

OOH Duty Manager Pager GRO between the hours:

17.30 - 09.00 Monday PM to Thursday AM

17.00 - 09.00 Friday PM to Monday AM

Outside these times, please contact the Major Incident Manager

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.

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*