WITN11070110

Document Title:	**HNG-X Security Business Continuity Plan**
Document Reference:	SVM/SDM/PLA/0031
Document Type:	**CONTINGENCY PLAN**
Release:	As applicable
Abstract:	This Security business continuity plan has been produced to meet the requirements of ISO 27001 and should be used in conjunction with the HNG-X Services, Support Services and Engineering Services business continuity plans. This document details the planned actions which can be taken to minimise the risk of one or more components of the HNG-X Service or Support Services not being available due to security violations.
Document Status:	DRAF
Author & Dept:	Changdev Pawashe POA Business Continuity Manager
Internal Distribution:	
External Distribution:	Rebecca Barker, Business Continuity Manager, Post Office Limited. APPROVED Versions only

Approval Authorities:

Name	Role	Signature	Date
Alex Kemp	Post Office Account Senior Operations Manager		
Keith Smith	Post Office Account Chief Information Security Officer		

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

WITN11070110

0 Document Control

0.1 Table of Contents

WITN11070110

WITN11070110

0.2 Document History

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
0.1	15/07/2008	First draft for HNG-X	None
1.0	12/08/09	Incorporated section 10.1 for RTO and RPO requirements.	None
1.1	24/04/09	To reflect organisational changes Minor update to Figure One. Incorporated new internet access preventative measures N20, N21 and I31	None
1.2	12/05/09	Added Jim Sweeting, Vince Cochrane and Adam Parker to the Reviewer lists.	None
1.3	14/07/2014	Updated document to send for review to Reviewers. Included- MAC team details, Edited contact details of 'Normal Processes & Escalation Process.	None
1.4	22/09/2014	Updated reviewer comments. Issuing for an approval	None
2.0	23-Sep-2014	Approval version	

0.3 Review Details

Review Comments by :	
Review Comments to :	Changdev Pawashe & PostOfficeAccountDocumentManagement[redacted] GRO

Mandatory Review	
Role	Name
Infrastructure Operations Manager	Andy Hemingway
Post Office Account, Senior Operations Manager	Alex Kemp
HNG-X System Owner (DR and Continuity)	Ed Ashford
Post Office Account Chief Information Security Officer	Keith Smith
Post Office Account Security Operations Manager	Kumudu Amaratunga
Post Office Account Security Architect	Dave Haywood
Optional Review	
Role	Name

WITN11070110

Network Delivery Manager	Roger Stearn
Post Office AccountService Delivery Manager MAC Team	Sandie Bothick
Post Office Account Service Technical Manager Unix Team	Fiona Lennox
Post Office Account Service Problem Management	Steve Bansal; Tony Wicks
HNG-X System Owner	Paul Stewart
Fujitsu Services Core Services System Owner and Operations Manager	Andrew Gibson
Principal Customer Solution Architect	Jason Clark
Systems Management & Global Cloud	Catherine Obeng
SMC Team Manager	Jacob Cherian
Quality and Compliance Manager	Bill Membery
Application SDM and Risk Manager	Yannis Symvoulidis
Issued for Information – Please restrict this distribution list to a minimum	
Position/Role	Name

(*) = Reviewers that returned comments

0.4 Associated Documents (Internal & External)

Reference	Version	Date	Title	Source
PGM/DCM/TEM/0001 (DO NOT REMOVE)	2.0	16-Apr-07	POA HNG-X Generic Master Document Template	Dimensions
SVM/SDM/SIP/0001			HNG-X Business Continuity Framework	Dimensions
SVM/SDM/PLA/0001			HNG-X Support Services Business Continuity Plan	Dimensions
SVM/SDM/PLA/0002			HNG-X Services Business Continuity Plan	Dimensions
SVM/SDM/PLA/0030			HNG-X Engineering Business Continuity Plan	Dimensions
SVM/SDM/PLA/0003			HNG-X Business Continuity Test Plan	Dimensions
SVM/SDM/PRO/0028			Fujitsu Services Post Office Account HNG-X Business Continuity Management Process	Dimensions
SVM/SDM/PRO/0001			POA (POA) Customer Service Major Incident Process	Dimensions
SVM/SEC/PLA/0009			PCI Incident Management Plan	Dimensions

WITN11070110

CS/MAN/012			Post Office Account Crisis Management Quick Reference Guide	PVCS
SU/MAN/018			Operations Procedures Manual Index	PVCS

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

0.5 Abbreviations

Abbreviation	Definition
ACL	Access Control List
AV	Anti-virus
BIOS	Basic Input/Output System
BCM	Business Continuity Manager
BRA01	Bracknell01
CA	Computer Associates
CHAP	Challenge-Handshake Authentication Protocol
CMT	Crisis Management Team (POA)
DCS	Debit Card System
DMZ	De-Militarised Zone
DSA	Digital Signature Algorithm
DVLA	Department of Vehicle Licensing Authority – Post Office MOT Enquiry
FTP	File Transfer Protocol
HSD	Horizon Service Desk
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IDS	Intruder Detection System
IMT	Incident Management Team
IPSEC	IP Security
ISO	International Standards Organization
LAN	Local Area Network
MAC	Major Account Controllers.
MBCI	Major Business Continuity Incident
NDC	National Distribution Centre
NEU	National Exchange Unit
OOH	Out Of Hours
OS	Operating System
OTI	Open Transport Interface
PAN	Primary Account Number

WITN11070110

PCI	Payment Card Industry
PIN	Personal Identification Number
POL	Post Office Limited
POA	Post Office Account
RPO	Recovery Point Objectives
RSA	A public-key-encryption technology developed by RSA Data Security, Inc. The acronym stands for Rivest, Shamir, and Adelman, the inventors of the technique.
RTO	Recovery Time Objectives
SDM	Service Delivery Manager
SMC	System Management Centre
SSC	Support Service Centre (Third Line Support)
TfS	Triole for Service
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network

0.6 Glossary

Term	Definition

0.7 Changes Expected

Changes
As an operational document, it is expected this will also be amended for numerous reasons including: 1, new risks are identified; 2, improved or new contingency actions are identified; 3, In 7.2 Section: Infrastructure Security Control: In Item I26, Risk need to be addressed & will need to be updated in the document.

0.8 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.

WITN11070110

1 Introduction

This Security business continuity plan has been produced to meet the requirements of ISO 27001 and should be used in conjunction with the HNG-X Services, Support Services and Engineering Services business continuity plans.
This document details the planned actions which can be taken to minimise the risk of one or more components of the HNG-X Service or Support Services not being available due to security violations.

Section 11, the Business Impact and Risk assessment lists the perceived potential security violations and defines the action to be taken in the event the risk occurs. In many cases this calls for the Security Operations Manager to make an initial assessment of the situation and report the findings to the POA Crisis Management Controller. For some perceived risks the Crisis Management Team should already be informed of the potential incident. CS/MAN/012 defines the members of the Crisis Management Team and their support teams. As the specific action to be taken for each of these risk can be so varied, i.e., ranging from, software virus infections, threatened terrorist attacks to an actual terrorist attack, the follow-up actions are not defined here but are to be managed through exception management depending upon the situation, but in accordance with Fujitsu Services Group/Corporate policies and processes defined on Café Vik.

Note: HNG-X operational business continuity, operational security and penetration testing, are to be conducted.

2 Scope

The scope of this Security business continuity plan is to define the measures taken to prevent security violations in the HNG-X solution and to define the actions to be taken if security violations are identified.

This plan does not detail the functionality of the Key Management Service or other security function as this are detailed in SVM/SDM/PLA/0001.

WITN11070110

3 Ownership and Operation

The POA Business Continuity Manager, who is also responsible for its maintenance and operational verification, owns this plan. Contact details are shown below.

Name	Position	Office Contact No.	Out of hours No.
Changdev Pawashe Post Office Account	Fujitsu Services, Post Office Account, Business Continuity Manager.	GRO	GRO
Kumudu Amaratunga	Fujitsu Services, Post Office Account, Security Operations Manager.	GRO	GRO

A copy of this plan Business Continuity plan is available on the Dimensions server for reference.

4 Service Functionality

4.1 Services Overview

SVM/SDM/PLA/0002 the HNG-X Services business continuity plan and SVM/SDM/PLA/0001 the Support Services business continuity plan provide full details on the HNG-X Service and the HNG-X Support Services. The operation of the security service is documented within the Support Services business continuity plan SVM/SDM/PLA/0001.

This Security business continuity plan has been produced to meet the requirements of ISO 27001 and should be used in conjunction with the HNG-X Services, Support Services and Engineering Services business continuity plans.
This document details the planned actions which can be taken to minimise the risk of one or more components of the HNG- Service or Support Services not being available due to security violations.

This document specifically covers the preventative measures that have been taken to minimise the risk of security violations, see section 7 and the business impact analysis table in section 11 defines the actions to be taken in the event a security incident is escalated to the POA Duty Managers.

Figure one provides an overview of all the HNG-X Services for which POA has partial or full responsibility. The diagram also provides details of the support applications and services covered within the HNG-X Support Services Business Continuity Plan SVM/SDM/PLA/0001.

WITN11070110

HNG-x Services Overview

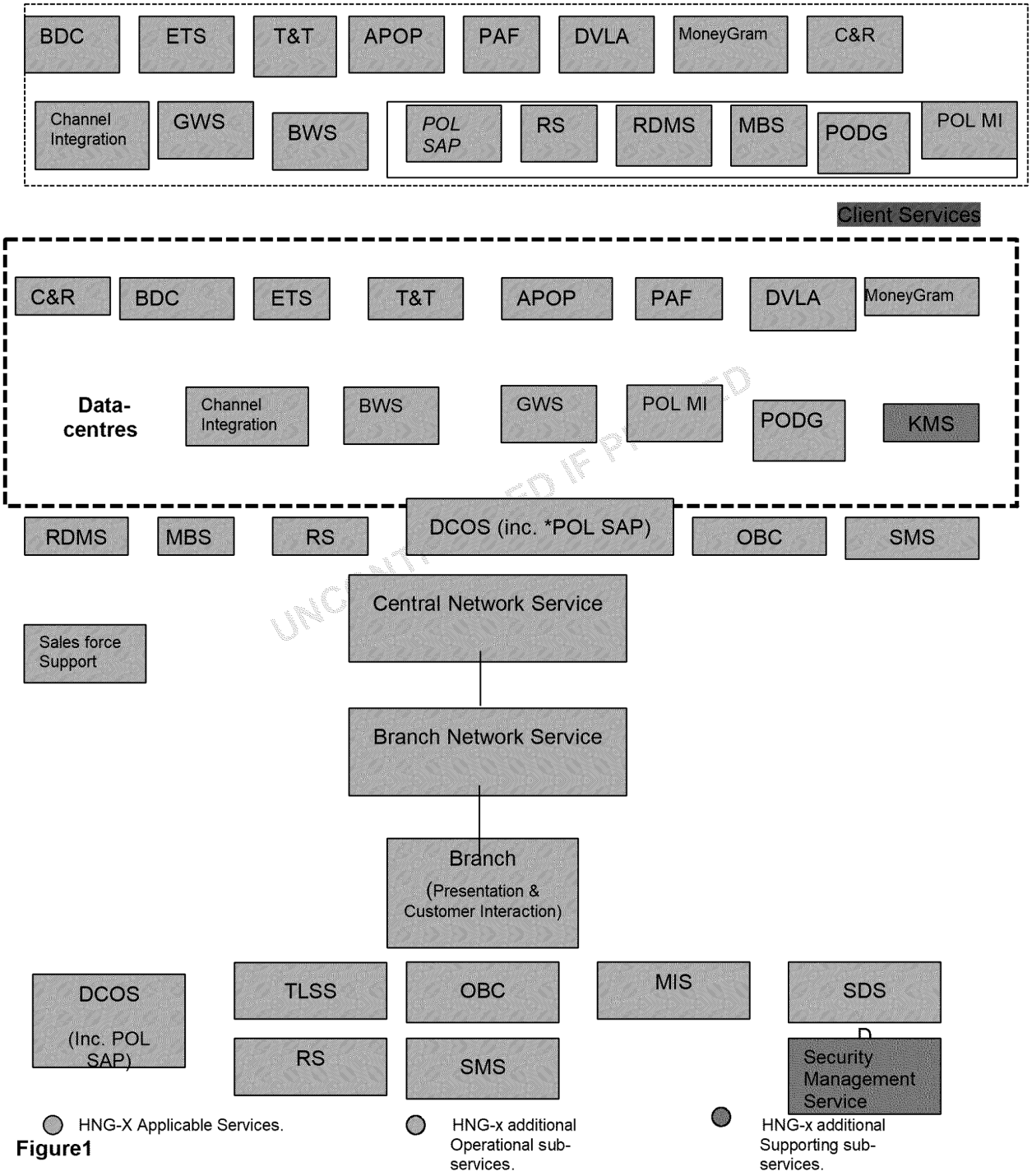

Figure1

WITN11070110

5 Security Service

The POA Security Service can be considered to cover a number of functions:

1; Data-centre security, e.g., physical and personnel – See SVM/SDM/PLA/0002

2; HNG-X infrastructure security – individual services - See SVM/SDM/PLA/0002

3; the operation of the HNG-X Key Management Service - See SVM/SDM/PLA/0001

This business continuity plan specifically details the planned actions which can be taken to minimise the risk of one or more components of the HNG-X Service or Support Services not being available due to a security violation.

6 Testing Strategy

6.1 Initial Testing

The testing of the security service is documented in SVM/SDM/PLA/0013 and some testing is contained within the HNG-X data-centre fail-over test script in SVM/SDM/PLA/0005. The testing of security services documented in SVM/SDM/PLA0013 & SVM/SDM/PLA/0005 has been tested in 2013.

6.2 Ongoing Test Strategy

This refers to how the contingency measures in place for the Security Service will be periodically tested to ensure they are current and reflect the service model for those services as they mature.

This is provided by an ongoing series of business continuity tests at a predetermined frequency for the duration.

WITN11070110

7 Preventative Measures

The following sections define the measures that have been taken to minimise the potential risk of security violations.

7.1 Network Security Controls

	Risk(s) Addressed	Implemented Preventative Measures
N1	Attempted unauthorised access from a client connections (banks, DVLA, HSBC Merchant Services (HMS), e-pay)	Client DMZ Firewalls Inner Firewall for HSBC Merchant Services (HMS) (DCS)
N2	Attempted unauthorised access from the internet	Data centre DMZ Firewalls A DMZ is provisioned that provides network separation, data isolation and content inspection of traffic going to and from the Internet. This is achieved through a combination of tight firewall controls and proxy services for interactive access and for content inspection. The proxy service is a Secure Computing Webwasher appliance configured to inspect http, https and ftp traffic, depending on the requirements of the service. This service will initially only be used to support outbound HTTPS connections for the Moneygram Test Web Service and for the Kahala/Telecoms Broadband Service. All services requiring access to or from the Internet will use this service. Third party penetration testing
N3	General attempted unauthorised access	Network Segmentation. Within each Data Centre, the HNG-X network is segmented in accordance with a Security Domain model. This ensures that the flow of data around the network is controlled using the principle of Least Privilege Access Control. The network segmentation is achieved using a combination of physical and virtual controls. Dependent on the Security Domain and any specific contractual agreements with third parties, the network segmentation is enforced using VLANs, Stateful Inspection Firewalls, ACLs and physical separation. Each different network media type is authenticated using a dedicated RADIUS server for network

WITN11070110

		device access, with the Branch Router using different CHAP credentials per interface, and each human support user accessing a network device is authenticated using the Identity and Access Management Service.
N4	Attempted unauthorised access from a wireless LAN	No wireless LAN access (Wi-Fi) allowed in solution
N5	Attempted unauthorised access from the Royal Mail intranet network.	Post Office DMZ Firewalls
N6	Attempted unauthorised access from the branch network.	VPN Security layer implemented. Active logging of Intrusion Detection Alerting and reporting mechanism configured. Update mechanism to be implemented.
N7	Exposure to non-counter staff/kit. Limits number of end points that can attack the solution.	Closed user Group on branch network Make properly closed for Dialled access.
N8	Exposure to non-counter staff/kit. Network end point requires valid username and password to attach to network	Strong CHAP Password for branch network authentication
N9	Attempted unauthorised access from branch network.	The Branch Router to be configured with access lists to restrict traffic flows to the Data centre. Branch router configured with layer 2 MAC filters to limit which devices can connect and pass traffic to the Router. A high availability pair of Firewalls configured at each Data centre to manage traffic flows from the service provider network to HNG-X edge Routers.
N10	Unauthorised devices being plugged into branch LAN trying to gain access into the HNG-X Data centre.	HNG-X branch router to be configured with the appropriate access lists to further restrict traffic flow from the branch to the Data Centre.
N11	Attempted unauthorised access from the Fujitsu support community.	At each Data Centre create a Support DMZ with appropriate support DMZ Firewalls
N12	Confidentiality and integrity of data while in transit.	Network encryption to banks and e-pay
N13	Confidentiality and integrity of data while in transit.	Network encryption to support sites updated to use IPSEC
N14	Confidentiality and integrity of data while in transit.	Network encryption to Royal Mail sites
N15	Confidentiality and integrity of bulk data while in transit to/from HSBC Merchant Services (HMS).	MPPE (Microsoft Point to Point Encryption) protection of files to/from streamline
N16	Access to management functions from	Separate management LAN and 'live' traffic in data

WITN11070110

	exposed networks.	centre for server console and routers wherever possible.
N17	Detection of unauthorised access attacks that breach inner firewalls.	Intrusion Detection implemented on the central Data-centre network
N18	Security breach of one network type could compromise other network types.	Radius servers segregated by logical network type
N19	Limit risk of unauthorised access.	Uses Private IP addresses which are not exposed across the system boundary
N20	Limit risk of from unauthorised Internet access.	The Internet access design provides for a single non-resilient Internet access in each of the IRE11 and IRE19 data centres. Although non-resilient, redundancy of access between sites is provided and services can be manually restored between sites. There are two layers of firewall protection for Internet access. DMZ LANs are to be established on the inner firewall tier for the Internet Services Hub, Hosting DMZ and for the Webwasher/DXI proxy servers.
N21	Limit risk of from unauthorised Internet access from EMC via Remote Support.	A DMZ is to be established on the outer firewall tier specifically for the EMC Remote Services Gateway (RSG). This will prevent EMC initiated connections through the inner tier firewall which will then only accept incoming traffic from the RSG platform.

7.2 Infrastructure Security Controls

	Risk(s) Addressed	Control Name
I1	Prevent alien code being loaded.	No plug and play, floppy disk, CD etc in counter
I2	Intrusion by non-authorised staff	Physical Controls on data centre access
I3	General Intrusion Prevention by non-authorised staff	Platform foundation builds used for HNG-X have been hardened through the use of specialist scripts and build instructions. This hardening reduces the 'surface area' for attack and thereby reduces the level of vulnerability of each individual system. This hardening removes unnecessary services and software as well as applying a base set of platform file permissions.
I4	Intrusion Prevention and Detection - vulnerability management	The McAfee Foundstone vulnerability scanning appliance has been deployed into each Data Centre. This appliance is configured to scan all systems, (including network devices), on a regular basis.

WITN11070110

		The scanner has been configured to run non-destructive scans, with appropriate credentials, on the scanned platform, to enable in-depth Operating System scanning. Reports are produced from the vulnerability scanning server as input to the audit process and for analysis by the CS Security Team.
I5	Intrusion Prevention and Detection	Network-Based Intrusion Prevention is deployed in the HNG-x infrastructure at the interface between the Branch Network and the Data Centre network. This is to prevent malicious traffic from the Branch estate from entering the Data Centre and to provide notification of any occurrence to the Security Event and Information Management service. Network-based intrusion detection is also deployed throughout the HNG-X Data Centre infrastructure. This provides notification of an attempted compromise of systems within the Data Centre, through malicious activity or malicious code. In addition to raising alerts of malicious activity, the IDS sensors will send feed event logs into the secure event management service, to provide an audit trail and to enable additional event correlation with Firewall, Router and other network device logs.
I6	Exposure of system to non-authorised users	Access controls for support/operational staff – Secure Access Servers, secure logon etc.
I7	Unauthorised access or programme drops from counters into the data centre	Counter and Branch router locked down (no access by branch staff to underlying OS)
I8	Stop sensitive data being exposed	Implement clear security policy and procedures, e.g., for support teams etc. Degauss disks /tapes before leaving the Data centre
I9	Unauthorised access or programme drops attempts on local LAN. Limit spread of machine to machine viruses	Counter firewall
I10	Risk of virus infection with Data-centres	Anti Virus for all data centre platforms, i.e., Ensure the systems are hardened and patched appropriately. Configure AV on those systems that will support it or protect via an inline AV appliance. Current AV solution only been deployed to limited number of servers (Only PCI platforms).
I11	Reduce implications of Unauthorised access or programme drops attacks.	Create secure build standard and secure builds for servers.

WITN11070110

		Turn off unused features. Remove unwanted/unused services. Ensure access controls correct, implement minimum setting permissions for users, applications and file system.
I12	Access to keys by non-authorised staff	Physical Controls on access to key management functions and key handling
I13	Access to full keys by Fujitsu staff	Two-person controls on access to key material
I14	Address vulnerabilities in OS to stop unauthorised access or programme drops/viruses	Patching of Data centre platform operating systems Physical Controls on access to support workstations In conjunction with the configuration management system, implement a system to receive notification of vulnerability alerts. Patch systems using change control Test patches for latest vulnerabilities in test environment.
I15	Prevent system being booted into a uncontrolled operating system	BIOS is locked down and only bootable from primary storage on counter
I16	Fraud by Fujitsu staff	Auditing of all support staff actions related to change of business data
I17	Limit any data from being retained in the counter hard disk.	Clear page file on shut down at counter
I18	Prevent unauthorised code from being installed	Code signing
I19	Prevent unauthorised changing of ref data	Ref data signing
I20	Address vulnerabilities in operating system to stop unauthorised code and viruses	Patching of counter OS
I21	Access by non-authorised staff to support functions	Physical Controls on access to support workstations
I22	Stop machine to machine viruses, limit access to servers from unexpected sources.	Server firewalls
I23	Ensure if an application is bypassed in someway, the user hasn't got sufficient privilege to perform unauthorised actions or changes to the machine.	Counter Application are run in non-privileged user mode.
I24	Stop unauthorised counters being added	Counters have to be centrally configured before they can be used by the application
I25	Stop users spoofing a branch to access its accounts from remote location.	Counters are configured to only allow login to a given branch

WITN11070110

I26		VPN upgraded to 128bit Key + POLO Process + Disk Encryption to protect keys in pagefile
I27	Information exposure. Loss of confidentiality or integrity.	Encryption
I28	Information exposure. Loss of integrity.	Update DSA public/private keys to RSA + increase strength.
I29	General attempted unauthorised access from a client, PO, Branch or support connections	Four separate DMZs have been implemented in the HNG-X Data Centre. (See SVM/SDM/PLA/0002 for further details.)
I30	General attempted unauthorised access into HNG-X general servers	A three tier security model with 11 separate security domains has been implemented for HNG-X. (See SVM/SDM/PLA/0002 for further details.)
I31	Malware delivered via the internet access or suspicious activities	The Webwasher (DXI) appliance shall act as a proxy for HTTP, HTTPS, FTP, SMTP protocols and inspects these protocols for malware and suspicious activity. The external (Internet facing) IP address is seen as the source IP address by the Internet for all traffic that goes through the DXI.

WITN11070110

7.3 Application Security Controls

#	Risk(s) Addressed	Control Name
A1	Application Vulnerabilities	A vulnerability management service ensures security patches and updates are maintained at the appropriate level. The service provides secure platform builds that have been hardened to reduce the vulnerability of the standard platform. The service provides protection against malware in the form of Viruses, Trojans, and Worms etc. and detects and prevents malicious code and malicious activity on the network. This service supplies the assurance that possible platform and application vulnerabilities have been reduced to a minimum. The following facilities are supplied by the service; • Provides system hardening. • Provides vulnerability management. • Provides patch management. • Provides malware management. • Controls vulnerabilities within HNG-X. The vulnerability management service consists of a number of components that work together to identify and reduce vulnerabilities in HNG-X. This includes vulnerabilities caused by configuration errors as well as software bugs.
A2	Application Vulnerabilities	HNG-X uses the ESET anti-virus product. current AV protection is provided by ESET AV. Updates of virus signatures and of the anti-virus engine are obtained using the Patch Management Server. The signatures and updates are put through LST testing to ensure their integrity and are applied using the Tivoli software distribution system rather than the ESET management tools, thereby ensuring consistency of delivery to system-managed platforms. Only PCI platforms got AV running not all servers
A3	Application Vulnerabilities	To reduce vulnerability to exploitation and to ensure that all systems within the HNG-X environment have the relevant and appropriate Microsoft Products, Solaris 10, Red Hat Linux 4.x

WITN11070110

		and Oracle. patches applied within a reasonable timeframe, a patch management system has been implemented. This system provide mechanisms for; Gathering patches and updates to major operating systems and applications, Evaluating and filtering the patches and updates Testing the patches and updates Deploying the patches and updates. A patch management server is deployed within the HNG-X infrastructure, which obtains patches and updates from the relevant Vendors, using the Internet as a transport medium, and store them in an appropriate location. The CS Security Team is responsible, along with platform owners, for establishing the relevance and priority of each patch or update. The filtered patches are LST tested and are distributed to the target platforms using the Tivoli software distribution mechanism. Data integrity of each patch or update, (and of software distribution in general), is assured using a file hashing mechanism.
A4	Prevent exposure of PAN	PAN not printed in full on receipts
A5	Fraud – used for litigation support, FSA requirement.	Auditing of branch staff transactions and events
A6	Exposure of customer's Personal Identification Numbers (PIN).	Hardware encryption of PIN at counter and data centre, using Pinpads and Atalla HSMs PINs are held encrypted except when within tamper-resistant physical devices
A7	Exposure of system to unauthorised users	Logon/Logoff of branch staff to application
A8	Authentication of transactions to/from counter	Authentication of transactions to/from counter
A9	Prevent wide scale exposure of Sensitive Authentication Data	Deleting Sensitive Authentication Data (see definitions) from audit and diagnostic records before written
A10	Confidentiality of such data in transit (e.g. Track 2)	Encryption of Sensitive data between counter and data centre. (VPN to make 128bit)

WITN11070110

A11	Minimise risk of malware.	No email access for branch staff
A12	Minimise risk of malware.	No internet browsing capability for branch staff
A13	Exposure of system to non-authorised users	CA for certifying counter/app server keys Update key length – move from DSA to RSA
A14	Replay of banking transactions	MAC of banking transactions Add MAC to deposit transactions
A15	Proof of data in case of dispute or fraud investigations.	Auditing of data passed across interfaces to external systems (e.g. banks)
A16	Higher privilege functions not provided to low privilege users.	Users of Branch application are allocated role(s) to determine the functions to which they have access.
A17	Allows staff to lock screen while away from the counter to stop unauthorised users from using the application.	Branch Application provides facility to “lock screen”
A18	Allows staff to logout quickly if threatened	Branch Application provides facility for user to quickly and simply logout in a clean manner.

WITN11070110

8 Preparedness Measures

Preparedness may be defined as, those measures taken to ensure the technical solution and business processes supporting that solution deliver the service that they are designed to deliver, in such a way as to meet and exceed the service level.

8.1 Testing

From a technical standing, functionality is proven by testing the solution at a unit, system and business integration level.

This functional testing has been complemented by performance and security testing to ensure that the solution is both scalable and secure. HNG-X infrastructure has also been subjected to third party security penetration testing

Additionally, the Security Service for HNG-X has been the subject of operational business continuity tests.

8.2 Service Management & Delivery

From a business perspective, this process starts by establishing very exacting and specific security requirements. The POA Customer Services Security Team is specifically responsible for the operational security relating to HNG-X infrastructure, network, applications and physical facilities.

This business continuity plan instructs the POA Duty Managers of the process to be followed in the event a security violation is identified. This document is further supported by operational documentation for all aspects of the HNG-X service delivery.

8.3 Risk Analysis

The business impact analysis table in section 11 details the Risk Analysis undertaken at a Business Continuity level for HNG-X and it defines the actions to be taken in the event a security incident is escalated to the POA Duty Managers.

This BIA table identifies potential risks to the service, the assessed probability of that risk occurring, the impact of that risk becoming a reality and the contingency activity or plans necessary to contain such an occurrence with minimum impact to HNG-X service overall.

9 Contingency Measures

Contingency measures are defined as the actions to be performed in the event of a service break, in this case a security violation, to manage the impact to the HNG-X service and the business operations.

Contingency measures will include the recognition, activation, incident management and initiation of recovery procedures.

WITN11070110

9.1 Recognition

9.1.1 System Management Recognition

The HNG-X solution includes a Systems management capability to monitor and report on events that occur upon all the platforms involved in the service delivery and counters.

The process of monitoring and managing the Network components and Routers is performed by a combination of the products ***HP OpenView and CISCO works***.

TWS (Tivoli Work Scheduler) provides scheduling facilities for the Host and Agent processes.

Tivoli ITM is used to manage and monitor the Sun Solaris Servers, UNIX and Windows NT platforms directly to provide a comprehensive management view of the entire solution at any time. Tivoli ITM covers all of the functionality.

9.1.2 Security Violation Recognition

Within the overall HNG-X solution a number of different security monitoring and reporting facilities have been implemented. These include the following:

Close Circuit TV and recording of Data-centres, operational Security facilities, and Fujitsu Services and suppliers buildings.

Recognition and recording on door access systems.

Infrastructure intruder detection software

Anti-virus software

Secure Access System audit logs

Transaction audit logs and data.

External sources, e.g., detection within Post Office Limited systems.

9.2 Activation

Once a security violation event has recognised, detected, or reported a TfS incident will be raised with the SMC/MAC (Major Account Controllers) teams. (For security reasons it is imperative that only the minimum information is provided and this is treated with discretion).

WITN11070110

9.3 Incident Management

Personnel at the MAC (Major Account Controllers) will carry this out. If the incident cannot be resolved by the MAC at the time of the call it will be routed to the appropriate support unit for resolution. At the same time if the incident meets the MAC escalation criteria, it will be escalated to the Fujitsu Services POA Duty Manager.

If the criteria for Cross-Domain Business Continuity Management are satisfied the Duty Manager will escalate the problem to the POA Business Continuity Manager who will own the problem as a Business Continuity event.

The POA Duty Managers and the POA Business Continuity Manager will inform the POA Security Operations Manager of all incidents reported to then as potential security violations or events.

Note: Post Office Limited may also escalate Business Continuity events, including security related incidents, directly to the POA Duty Manager.

9.4 Initiation of Recovery Procedures

Where this is a POA only incident, this would usually be instigated by the support team charged with supporting the equipment upon which the failure has occurred, as soon as possible, and certainly with intent to resolve the incident within the relevant Service Level Agreement.

Depending on the severity of the incident, there may be some dialogue between the Duty Manager and the support function to agree on the most appropriate course of action.

Wherever there is a Cross Domain incident, the resolution would be instigated at the time when all parties affected had agreed the course of action:

In the case of a Business Continuity incident, this would be after the Business Continuity Team had agreed a plan of action, see Section 11, Plan Activation.

10 Recovery of Normal Service

An Operations Procedures Manual containing the operational and recovery processes and procedures for all possible failures in the end to end HNG-X Service.

Thus in its simplest form, normal service could be resumed by the Duty or Problem Manager liaising with the support team, agreeing when the recovery action should be run, and then carrying that activity out.

Where the recovery action is dependent upon a third party the support dialogue would take place between the support teams, and the problem management dialogue would take place between the appropriate management.

WITN11070110

10.1 Recovery Time Objectives and Recovery Point Objectives

As detailed in section 2 Scope, this plan does not detail the functionality of the Key Management Service or other security function as this is detailed in SVM/SDM/PLA/0001. The Recovery Time Objectives and Recovery Point Objectives for the Key Management Service are detailed within that plan. The Recovery Time Objectives and Recovery Point Objectives for the loss of the Data-centre or Data-centre fail-over, if required, due to a forensic investigation is detailed within SVM/SDM/PLA/0002.

11 Impact & Risk Assessment

11.1 Risks Identified Against the Horizon Services

The matrix below details the identified risks and impacts of security violations to the HNG-X Service.

As a matter of normal operational practice, an incident would be placed with the Service Desk if any of the identified risks materialised.

The intention is that the list identified can act as a guide to personnel assessing and managing any incident affecting the Engineering service.

The matrix contains a column identified as probability with a range of 0 to 4. These estimate the probable risk of the define security violation. It must be emphasised that these are not percentages and should be considered simple weighting factors.
As a guideline the following occurrence ratings have been allocated:

Rating	
0	Less than one violation is predicted per year
1	One violation is predicted per year
2	Two violations are predicted per year
3	Approximately three violations are predicted per year
4	Approximately four violations are predicted per year

WITN11070110

11.2 Risks

The risk assessment identifies the Critical Time Factors for activation of contingency measures for the potential security risks.

No	Area of Risk or Incident Type	Risk	Probability	Critical Time Factor	Impact	Action
1.	**Data-centre Security**	The IRE11 or IRE19 computer room has been penetrated by unauthorised access – no indications of tampering of systems.	**1**	**immediate**	**No Impact**	Incident to be passed to Security Operations Manager.
2.		The IRE11 or IRE19 computer room has been penetrated by unauthorised access –there is evidence of physical tampering of systems.	**0**	**immediate**	Incident to be passed to Security Operations Manager. Undertake an immediate investigation of the infrastructure which has been tampered and report findings. **Potential Business Impact POL POA**	**Treat as MBCI** **Inform CMT Controller and invoke Crisis Management Team** CMT to use report to decide which subsystems, if any, should be shutdown. Retain all evidence
3.		The IRE11 or IRE19 computer room has been penetrated by unauthorised access –there is evidence of unauthorised equipment, including monitoring devices, connected to the HNG-X infrastructure.	**0**	**immediate**	Incident to be passed to Security Operations Manager. Undertake an immediate investigation into the sub-systems which have been penetrated. **Potential Business Impact POL POA**	**Treat as MBCI** **Inform CMT Controller and invoke Crisis Management Team** CMT to use report to decide which subsystems, if any, should be shutdown.

						Retain all evidence
4.		The IRE11 or IRE19 computer room has been penetrated by unauthorised access –there is evidence of unauthorised intrusion into the HNG-X infrastructure/service.	**0**	**immediate**	Incident to be passed to Security Operations Manager. Undertake an immediate investigation into the sub-systems which have been penetrated. **Potential Business Impact POL POA**	**Treat as MBCI** **Inform CMT Controller and invoke Crisis Management Team** CMT to use report to decide which subsystems, if any, should be shutdown. Retain all evidence
5.	**Operations Facilities Security**	IRE11 or IRE19 SOS operations room penetrated by unauthorised access – no indications of tampering of systems	**1**	**immediate**	**No Impact**	Incident to be passed to Security Operations Manager.
6.		IRE11 or IRE19 SOS operations room has been penetrated by unauthorised access –there is evidence of physical tampering of systems	**0**	**immediate**	Incident to be passed to Security Operations Manager. Undertake an immediate investigation of the infrastructure which has been tampered and report findings. **Potential Business Impact POL POA**	**Treat as MBCI** **Inform CMT Controller and invoke Crisis Management Team** CMT to use report to decide which subsystems, if any, should be shutdown. Retain all evidence
7.		IRE11 or IRE19 SOS operations room has been penetrated by unauthorised access –there is evidence of unauthorised equipment, including monitoring devices, connected to the HNG-X infrastructure.	**0**	**immediate**	Incident to be passed to Security Operations Manager. Undertake an immediate investigation into the sub-systems which have been penetrated. **Potential Business Impact POL POA**	**Treat as MBCI** **Inform CMT Controller and invoke Crisis Management Team** CMT to use report to decide which subsystems, if any, should be shutdown.

						Retain all evidence
8.		IRE11 or IRE19 SOS operations room has been penetrated by unauthorised access –there is evidence of unauthorised intrusion into the HNG-X infrastructure/service.	**0**	**immediate**	Incident to be passed to Security Operations Manager. Undertake an immediate investigation into the sub-systems which have been penetrated. **Potential Business Impact POL POA**	**Treat as MBCI** **Inform CMT Controller and invoke Crisis Management Team** CMT to use report to decide which subsystems, if any, should be shutdown. Retain all evidence
9.	**SSC Facilities Security**	BRA01 or LEW02 SSC Room has been penetrated by unauthorised access – no indications of tampering of systems.	**1**	**immediate**	**No Impact**	Incident to be passed to Security Operations Manager.
10.		BRA01 or LEW02 SSC Room has been penetrated by unauthorised access –there is evidence of physical tampering of systems.	**0**	**immediate**	Incident to be passed to Security Operations Manager. Undertake an immediate investigation of the infrastructure which has been tampered and report findings. **Potential Business Impact POL POA**	**Treat as MBCI** **Inform CMT Controller and invoke Crisis Management Team** CMT to use report to decide which subsystems, if any, should be shutdown. Retain all evidence
11.		BRA01 or LEW02 SSC Room has been penetrated by unauthorised access –there is evidence of unauthorised equipment, including monitoring devices, connected to the HNG-X infrastructure.	**0**	**immediate**	Incident to be passed to Security Operations Manager. Undertake an immediate investigation into the sub-systems which have been penetrated. **Potential Business Impact**	**Treat as MBCI** **Inform CMT Controller and invoke Crisis Management Team** CMT to use report to decide which subsystems, if any,

					POL POA	should be shutdown. Retain all evidence
12.		BRA01 or LEW02 SSC Room has been penetrated by unauthorised access –there is evidence of unauthorised intrusion into the HNG-X infrastructure/service.	**0**	**immediate**	Incident to be passed to Security Operations Manager. Undertake an immediate investigation into the sub-systems which have been penetrated. **Potential Business Impact POL POA**	**Treat as MBCI** **Inform CMT Controller and invoke Crisis Management Team** CMT to use report to decide which subsystems, if any, should be shutdown. Retain all evidence
13.	**POA Security Facilities.**	BRA01 or LEW02 Security Room has been penetrated by unauthorised access –there is no evidence of physical tampering of systems	**1**	**immediate**	**No Impact**	Incident to be passed to Security Operations Manager.
14.		BRA01 or LEW02 Security Room has been penetrated by unauthorised access –there is evidence of unauthorised equipment, including monitoring devices, connected to the HNG-X infrastructure.	**0**	**immediate**	Incident to be passed to Security Operations Manager. Undertake an immediate investigation of the infrastructure which has been tampered with and report findings. **Potential Business Impact POL POA**	**Treat as MBCI** **Inform CMT Controller and invoke Crisis Management Team** CMT to use report to decide which subsystems, if any, should be shutdown. Retain all evidence
15.		BRA01 or LEW02 Security Room has been penetrated by unauthorised access –there is evidence of unauthorised intrusion into the HNG-X infrastructure/service.	**0**	**immediate**	Incident to be passed to Security Operations Manager. Undertake an immediate investigation into the sub-systems which have been penetrated.	**Treat as MBCI** **Inform CMT Controller and invoke Crisis Management Team** CMT to use report to decide

WITN11070110

					Potential Business Impact POL POA	which subsystems, if any, should be shutdown. Retain all evidence
16.		BRA01 or LEW02 Security Room has been penetrated by unauthorised access –there is evidence of physical tampering of systems.	**0**	**immediate**	Incident to be passed to Security Operations Manager. Undertake an immediate investigation into the sub-systems which have been penetrated. **Potential Business Impact POL POA**	**Treat as MBCI** **Inform CMT Controller and invoke Crisis Management Team** CMT to use report to decide which subsystems, if any should be shutdown. Retain all evidence
17.	**SMC Facilities Security**	SMC IND49 Room has been penetrated by unauthorised access –there is evidence of unauthorised intrusion into the HNG-X infrastructure/service.	**0**	**immediate**	Incident to be passed to Security Operations Manager. Undertake an immediate investigation into the sub-systems which have been penetrated. **Potential Business Impact POL POA**	**Treat as MBCI** **Inform CMT Controller and invoke Crisis Management Team** CMT to use report to decide which subsystems, if any, should be shutdown. Retain all evidence
18.	**SOS Operations Out Of Hours laptop.**	Unauthorised HNG-X infrastructure/service intrusion via an SOS Operations Out Of Hours laptop.	**0**	**immediate**	Incident to be passed to Security Operations Manager. Undertake an immediate investigation into the sub-systems which have been penetrated. **Potential Business Impact POL POA**	**Treat as MBCI** **Inform CMT Controller and invoke Crisis Management Team** CMT to use report to decide which subsystems, if any, should be shutdown. Retain all evidence

19.	**SSC Operations Out Of Hours laptop.**	Unauthorised HNG-X infrastructure/service intrusion via an SSC Operations Out Of Hours laptop.	**0**	**immediate**	Incident to be passed to Security Operations Manager. Undertake an immediate investigation into the sub-systems which have been penetrated. **Potential Business Impact POL POA**	**Treat as MBCI** **Inform CMT Controller and invoke Crisis Management Team** CMT to use report to decide which subsystems, if any, should be shutdown. Retain all evidence
20.	**Payment Card Industry Incident**	Post Office Limited report a minor PCI incident affecting HNG-X. (I.e., less than n cards affected).	**0**	**immediate**	Incident to be passed to Security Operations Manager. **Potential Business Impact POL POA**	**Potential MBCI and Inform CMT Controller** CMT Controller to use report to decide which subsystems if any should be shutdown. Retain all evidence
21.		Post Office Limited report a Major PCI incident affecting HNG-X. (I.e., greater than n cards affected).	**0**	**immediate**	Incident to be passed to Chief Information Security Officer. Undertake an immediate investigation into the sub-systems which have been penetrated. **Potential Business Impact POL POA**	**Treat as MBCI** **Inform CMT Controller and invoke Crisis Management Team** CMT to use report to decide which subsystems, if any, should be shutdown. Retain all evidence
22.		Fujitsu Services detect a minor PCI incident on HNG-X. (I.e., less than n cards affected)	**0**	**immediate**	Incident to be passed to Security Operations Manager. **Potential Business Impact POL POA**	**Potential MBCI and Inform CMT Controller** CMT Controller to use report to decide which subsystems, if any, should be shutdown. Retain all evidence

23.		Fujitsu Services detect a major PCI incident on HNG-X. (I.e., greater than n cards affected)	**0**	**immediate**	Incident to be passed to Chief Information Security Officer. Undertake an immediate investigation into the sub-systems which have been penetrated. **Potential Business Impact POL POA**	**Treat as MBCI** **Inform CMT Controller and invoke Crisis Management Team** CMT to use report to decide which subsystems if any should be shutdown. Retain all evidence
24.	**Infrastructure Intruder Detected**	Evidence of attended system intrusion, i.e., abnormal processes, port access, etc. No evidence of actual system penetration.	**<5**	**immediate**	**No Impact**	Incident to be passed to Security Operations Manager.
25.		Evidence of attended system intrusion, i.e., abnormal processes, port access, etc. Evidence of actual system penetration.	**0**	**immediate**	Incident to be passed to Chief Information Security Officer. Undertake an immediate investigation into the sub-systems which have been penetrated. **Potential Business Impact POL POA**	**Treat as MBCI** **Inform CMT Controller and invoke Crisis Management Team** CMT to use report to decide which subsystems, if any, should be shutdown. Retain all evidence
26.	**Malicious Programme/Software /Virus Detection**	Virus detected which can be cleaned by existing anti-virus software	**0**	**immediate**	Incident to be passed to Security Operations Manager. Copies of virus to be sent for specialist analysis **Potential Business Impact POL POA**	To be treated as normal security incident process.
27.		Virus detected which cannot be	**0**	**immediate**	Incident to be passed to	**Treat as MBCI**

		cleaned by existing anti-virus software			Security Operations Manager. Virus specialist company to be employed to conduct analysis. **Potential Business Impact POL POA**	**Inform CMT Controller and invoke Crisis Management Team** CMT to use report to decide which subsystems, if any, should be shutdown. Retain all evidence
28.		Malicious Programme adversely affecting HNG-X infrastructure performance.	**0**	**immediate**	Incident to be passed to Security Operations Manager. Undertake an immediate investigation into the sub-systems which have been penetrated. **Potential Business Impact POL POA**	**Treat as MBCI** **Inform CMT Controller and invoke Crisis Management Team** CMT to use report to decide which subsystems, if any, should be shutdown. Retain all evidence
29.		Malicious Programme adversely affecting network infrastructure performance.	**0**	**immediate**	Incident to be passed to Security Operations Manager. Undertake an immediate investigation into the network which is adversely affected; involve Vodafone, Core ISP as applicable. **Potential Business Impact POL POA**	**Treat as MBCI** **Inform CMT Controller and invoke Crisis Management Team** CMT to use report to decide which subsystems, if any, should be shutdown. Retain all evidence
30.	**Unavailability of Audit Data**	Unavailability or loss of Audit Data (System)	**0**	**immediate**	Incident to be passed to Security Operations Manager. Undertake an immediate investigation into the loss of audit data.	**Treat as Potential MBCI** **Inform CMT Controller and invoke Crisis Management Team** CMT to use report to decide

					Potential Business Impact POL POA	which subsystems, if any, should be shutdown. Retain all evidence
31.		Unavailability or loss of Audit Data for Support access	**0**	**immediate**	Incident to be passed to Security Operations Manager. Undertake an immediate investigation into the loss of audit data. **Potential Business Impact POL POA**	**Treat as Potential MBCI** **Inform CMT Controller and invoke Crisis Management Team** CMT to use report to decide which subsystems, if any, should be shutdown. Retain all evidence
32.	**Loss of Restricted, Confidential or Personal Data**	Loss of Restricted, Confidential or Personal Data computer files	**0**	**immediate**	Incident to be passed to Security Operations Manager. **Potential Business Impact POL POA**	**Treat as Potential MBCI** **Inform CMT Controller**
33.		Loss of Restricted, Confidential or Personal Data hard copies	**0**	**immediate**	Incident to be passed to Security Operations Manager. **Potential Business Impact POL POA**	**Treat as Potential MBCI** **Inform CMT Controller**
34.		Loss of Personal Computers, i.e., SOS and SSC OOH Laptops	**0**	**immediate**	Incident to be passed to Security Operations Manager. **Potential Business Impact POL POA**	To be treated as normal security incident process initially.
35.	**Terrorist Activity**	Threatened or actual terrorist attack (Data-centres, IRE11, IRE19, SDC01, TCY01, TCY02)	**0**	**immediate**	Incident to be passed to Crisis Management Team, and FJS Corporate Management. **Potential Business Impact POL POA**	**Treat as MBCI** **Inform CMT Controller and invoke Crisis Management Team**

WITN11070110

36.		Terrorist Attack (Utility Infrastructure – i.e. Power)	**0**	**immediate**	Incident to be passed to Crisis Management Team, and FJS Corporate Management. **Potential Business Impact POL POA**	**Treat as MBCI** **Inform CMT Controller and invoke Crisis Management Team**
37.		Terrorist Attack (WAN fibre infrastructure)	**0**	**immediate**	Incident to be passed to Crisis Management Team, and FJS Corporate Management. **Potential Business Impact POL POA**	**Treat as MBCI** **Inform CMT Controller and invoke Crisis Management Team**
38.		Suspect Parcels (potential mail bombs)	**0**	**immediate**	Incident to be passed to Security Operations Manager. **Potential Business Impact POL POA**	**Treat as MBCI** **Inform CMT Controller and invoke Crisis Management Team**

WITN11070110

12 Plan Activation

This plan is activated by the Major Account Controllers (MAC) personnel raising a 'P1' priority incident with the POA Duty Manager and providing them with sufficient detail of the incident to compare the event with the risks defined in section 11.

In the event that the incident is to be treated under the normal security incident process they should contact and inform the POA CS Security Operations Manager using the contact details defined in section 13.

In the event that the incident is defined as a Potential MBCI or Major Business Continuity Incident the POA Duty Manager is to inform the POA BCM of the incident. The POA Business Continuity Manager is to ensure that where applicable the POA CS Chief Information Security Officer or the Security Operations Manager is made aware of the incident for initial investigation and escalated to the Crisis Management Team Controller using the contact details defined in section 13.

If the Joint BCM processes are invoked, the next steps will be to agree who from the BCMT owns the MBCI.

The BCMT will then agree a plan of action and agree upon the recovery and contingency activities to be carried out. Again, this will be done in conjunction with Senior Managers, relevant Business Units and Expert Domains as appropriate.

The agreed plan will then be monitored and reviewed until such time as the MBCI impacting the HNG-X has been resolved, and the MBCI closed.

It should be noted that in the event the Crisis Management Team process is invoked it is potentially likely that the incident will be jointly managed by the POA CMT and POL Business Protect Team.

WITN11070110

13.0 Contact List

13.1 Normal Processes

Organisation	Contacts	Telephone Number
FUJITSU SERVICES POA	Duty Manager Or Office Hours applicable Service Delivery Manager CS Security Operations Manager Kumudu Amaratunga Chief Information Security Officer Keith Smith Operations Director (CMT Controller)	Pager: Mobile Mobile Mobile
(MBCI Contacts)	Business Continuity Manager Changdev Pawashe	Office: Mobile:
FS Core Services **Networks**	Network Manager Roger Stearn Fujitsu Network Operations centre: GRO	Office: Mobile: Office:
FS Core Services System Ops Service	SOS NT and UNIX Manager Andrew Gibson Technical Support Manager Fiona Lennox	Office: Mobile: Office: Mobile:
FS Core Services Systems Mgt Centre	SMC Manager Jacob Cherian	Office: Mobile:
FS Core Services MAC/CMT.	MAC/CMT (STE04) Operations Manager Sandie Bothick Business Stream Manager Sandie Bothick	Mobile: Mobile:
Post Office Limited	ATOS IT Service Continuity management team GRO GRO	

GRO

WITN11070110

	ATOS IT Service Continuity management team GRO GRO	

WITN11070110

13.2 Escalation Processes

Escalation Level	Level 1	Level 2	Level 3	Level 4
Fujitsu Services POA	Duty Manager Pager: GRO Or Office Hours applicable Day Time POA Duty Manager Via MAC team.	Problem Manager (Assigned by Duty Manager) Business Continuity Manager. Changdev Pawashe Office: GRO Mobile: GRO GRO	CS Security Operations Manager. Kumudu Amaratunga Mobile: GRO	Customer Service Operations Director. Peter Thompson Mobile: GRO GRO Chief Information Security Officer. Keith Smith Mobile: GRO GRO
FS Core Services **Networks**			Network Manager Roger Stearn Mobile: GRO	Data Networking Support Manager POA Networks Duty manager – GRO
SOS NT and UNIX			NT&UNIX Manager Andrew Gibson Office: Mobile GRO	Technical Support Manager Fiona Lennox Mobile: GRO
SMC			SMC Manager Jacob Cherian Office: Mobile: GRO	
MAC			MAC Ops Manager Sandie Bothick Mobile: GRO	Office: GRO
Post Office Limited			Business Continuity Manager	Network Support Service Manager.

WITN11070110

			ATOS IT Service Continuity management team GRO	ATOS IT Service Continuity management team GRO