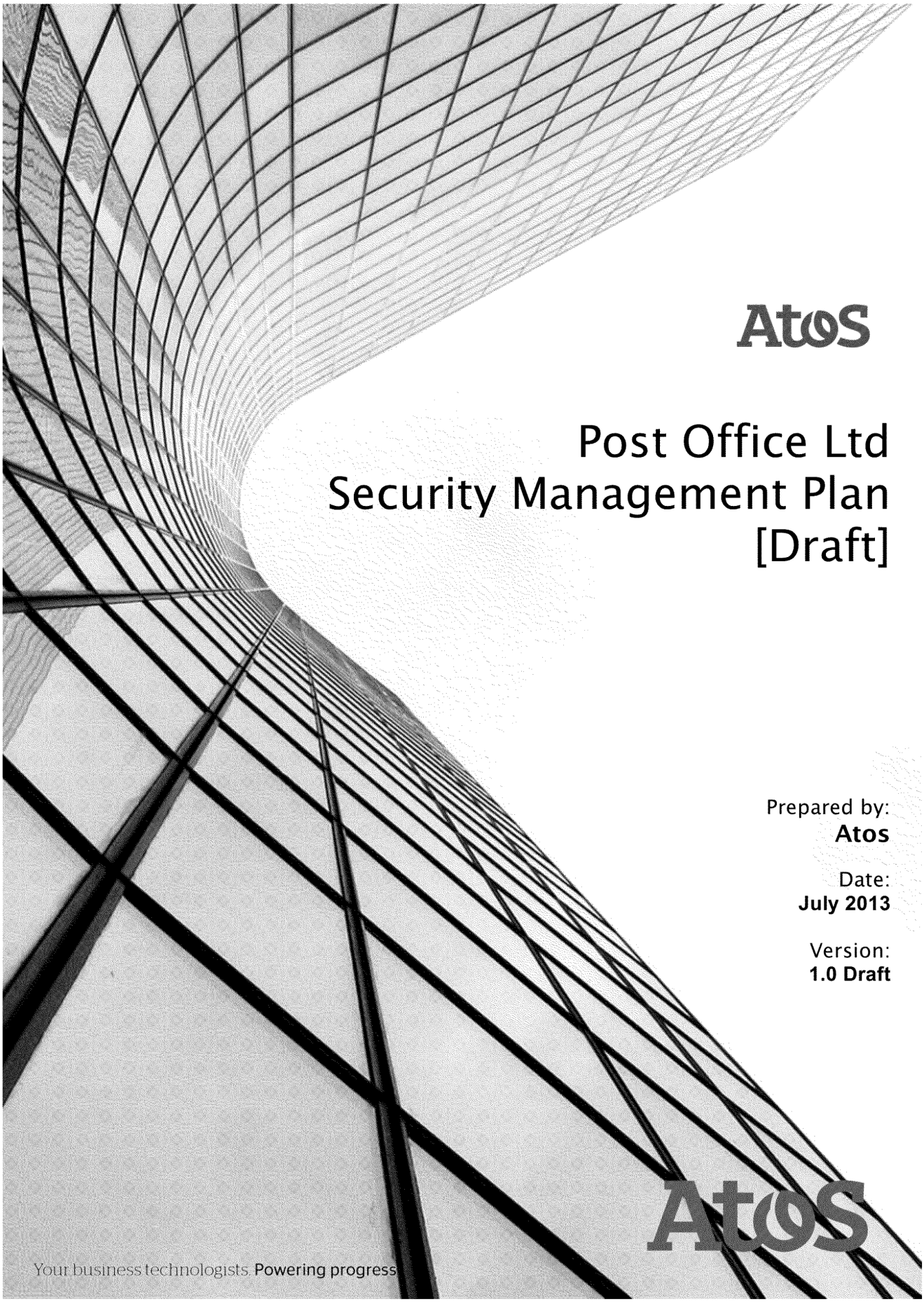
POL00401508



Post Office Ltd
Security Management Plan
[Draft]

Prepared by:
Atos

Date:
July 2013

Version:
1.0 Draft

Your business technologists. Powering progress

POL00401508

POL00401508

Contents

1. Executive Summary 7

2. Document Control 8

2.1 Version History 8

2.2 Changes since Last Version 8

2.3 Issue Control 8

2.4 Purpose 8

2.5 Scope 9

3. Information Security Policy 10

4. Organising Atos Information Security 12

4.1 Security Management Structure and Responsibilities 12

4.1.1 Atos Post Office Ltd. Service Director 12

4.1.2 Atos Post Office Ltd. Security Operations Manager / Support Team 13

4.2 Information Security Incident and Weakness Reporting 14

4.3 Vulnerability Management 15

4.4 Agreements on External (Third) Party Access 15

4.5 Outsourcing 15

5. Asset Management 16

5.1 Inventory of Assets 16

5.2 Acceptable Use of Information and other Assets 16

5.3 Information Classification 17

6. Human Resources Security 18

6.1 Terms and Conditions 18

6.2 Information Security Awareness and Training 18

6.3 Disciplinary Process 19

6.4 Monitoring of Personnel 19

6.5 Termination of Employment 20

6.6 Security Access Cards/Building Passes 20

6.7 Physical Access to Areas/Rooms Containing Post Office Ltd. Equipment 20

7. Physical and Environmental Security 21

POL00401508

7.1 Physical and Environmental Security Control Implementation 22
7.2 Physical Security Perimeter 22
7.3 Physical Entry and Other Controls 22
7.4 Working in Key Rooms/Areas 22
7.5 Intruder Detection Alarms 23
7.6 Protection of Equipment against Theft 23
7.7 Equipment Removal 23
7.8 Hardware Access Controls 24
7.9 Tamper Detection 24
7.10 Maintenance and Repair 24
7.11 Power Security 25
7.12 Fire Security 25
7.13 Water/Liquid Security 25
7.14 Cabling and Related Item Security 25
7.15 Safety Alerts 26

8. Communications and Operations Management 27

8.1 Operational Procedures and Responsibilities 27
8.1.1 Change Control Procedures 27
8.2 Segregation of Duties and Areas of Responsibility 27
8.2.1 Separation of Development, Test and Operational Environments 28
8.3 System Planning and Acceptance 28
8.3.1 Capacity Planning 28
8.3.2 System Acceptance 28
8.4 Protection against Malicious and Mobile Code 29
8.4.1 Prevention 29
8.4.2 Detection 30
8.4.3 Recovery 31
8.4.4 Mobile Code 31
8.5 Back-up and Recovery 31
8.6 IT Component Start-up and Close Down 31
8.7 Media (including Document) Security 32
8.7.1 Management of Removable Media 32
8.7.2 Printed Output 32
8.7.3 Secure Re-use or Disposal of Media 32
8.8 Exchange of Information 33

POL00401508

8.9 Monitoring 33
8.9.1 Accounting and Audit 33
8.9.2 Clock Synchronisation 34
8.10 Operator Logs 34
8.11 Fault Logging 34
8.12 Encryption 34

9. Access Control 35
9.1 User Account Management 35
9.1.1 User Account Requests 35
9.1.2 User Account Creation 35
9.1.3 Review, Disabling and Deletion of User Accounts 35
9.2 Access Control Configuration 36
9.3 Password Management 36
9.3.1 Control and Implementation 36
9.3.2 Password Generation 36
9.3.3 Password Storage and Transmission 36
9.3.4 Changing Passwords 37
9.3.5 Review of Passwords 37
9.3.6 Maintenance Passwords (Service Accounts) 37
9.3.7 Service Accounts Passwords 37
9.3.8 Privileged User/System Management Supervisory Passwords 37
9.4 Network Access Control 38
9.4.1 General 38
9.4.2 External Connections 38
9.5 Remote Access 38
9.6 Operating System, Application and Information, Access Control 39
9.7 Mobile Computing and Teleworking 39
9.7.1 Laptop Security 39

10. Information Systems Acquisition, Development and Maintenance 40
10.1 Security of System Files 40
10.1.1 Control of Operational Software 40
10.1.2 Protection of System Test Data 40
10.1.3 Protection of Source Code 40
10.2 Security in Development and Support Processes 41

POL00401508

10.2.1 System and Application Software Integrity 41
10.2.2 Sub-Contracted/Outsourced Software Development 41
10.3 Software Maintenance 41
10.4 Software Fault Log 41
10.5 Technical Vulnerability Management 42

11. Information Security Incident Management 43
11.1 Information Security Incidents and Weaknesses 43
11.2 IT/Networking Malfunctions 43
11.3 Learning from Information Security Incidents 44
11.4 Disciplinary Process in context of Information Security Incidents 44

12. Business Continuity Management 45
12.1 Business Continuity Planning 45
12.2 Back-up Procedures 45
12.3 Emergencies and Breakdowns 46
12.3.1 Hardware Failures 46
12.3.2 Software Failures 46
12.3.3 Fire/Building Evacuation 46

13. Compliance 47
13.1 Compliance with Legal Requirements 47
13.2 Compliance with Information Security Policies and Standards, and Technical Compliance 47
13.3 Transition to Compliance 48
13.4 Protection of System Audit Tools 48

14. Document Configuration 49
14.1 Feedback 49
14.2 Changes 49

15. Document References 50

POL00401508

1. Executive Summary

The role of the Information Security Management Service Integrator function is to develop, implement and maintain Information Security across the Supply Chain.

The Atos Security Management function will fulfil a Governance and Compliance role over the Supply Chain. In the role of the Service Integrator, Atos will be designated accountability and responsibility for the security management activities requiring a hand-off with the supply chain concerning Information Security activities as defined within Schedule 2.1 and Schedule 2.5.

This Security Management Plan below is in direct response to Schedule 2.5 ref. 3.1.2 and is structured in accordance with ISO/IEC 27001/2. Atos will introduce cross-supplier procedures (CSPs) which will describe the operational interfaces between different suppliers across the supply chain to facilitate the end-to-end service levels required by the Post Office Ltd.

The security of a system/service must be planned and cover the entire life cycle of the service. The security of the Post Office Ltd. IT provision is built upon the existing:

- Atos, Post Office Ltd. policies and procedures where possible; and
- Post Office Ltd. IT provision specific policies and procedures.

Summary:

a. Security is a key component of systems/services

b. Security must be planned throughout the life cycle of the system/service

c. Security is integral and not an 'add on' to a system/service

d. Security is built upon existing Atos and EUC policies and procedures

POL00401508

2. Document Control

2.1 Version History

Version	Date	Comments
1.0	June 2013	Initial draft for inclusion with Contract

2.2 Changes since Last Version

- None, initial release.

2.3 Issue Control

Author	Carl Nightingale, Executive Consultant, Atos
Peer Review	Gavin Kenny (CLAS), Associate Partner, Atos
Approver	
Signature	
Date	
Distribution List:	
TBC	Security Manager, Post Office Ltd.
TBC	Transition and Transformation Programme Director, Atos

2.4 Purpose

The purpose of this document is to outline how the Post Office Ltd. Service provision by Atos will demonstrate that an adequate level of security will be achieved. Furthermore this document is to provide an easy to use cross reference between Schedule 2.1, Schedule 2.5, the Post Office Ltd. Information Security Policy set (as defined in Schedule 2.5) and the related documents from within Atos. It is primarily targeted at the Atos support staff involved with supporting the Post Office Ltd. environment.

POL00401508

At this stage of the contract negotiations, this is a draft example of what the Security Management Plan may contain. The formal first draft of the Post Office Ltd. Security Management Plan will be issued as per Schedule 2.5|3.2.1.

Once the contract is awarded, this document will be maintained and issued by the Atos Post Office Ltd. Security Operations Manager (SOM) for Post Office Ltd.

2.5 Scope

The scope of this document is limited to providing a Security Management Plan for the Post Office Ltd. IT Service provision.

POL00401508

3. Information Security Policy

Objective (Sec.5.1|BS ISO/IEC 27002:2005):

To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations. Management should set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organisation.

Information Security within Atos is initiated and controlled by a global Security Management Group which promotes good security practices across the organisation. There are Security Managers appointed at country level. The Chief Security Officer for the UK is also Head of the UK Security Directorate, ensuring service line responsibility for information security.

In order to meet the conditions of Schedule 2.1 and Schedule 2.5 required by Post Office Ltd., Atos shall maintain the confidentiality, integrity and availability of consuming organisations' data whilst complying with UK law, relevant industry appropriate standards, and good practice guides in accordance with the Post Office Ltd. contract.

It is the responsibility of every Atos staff member to comply with the Atos Information Security Policy and the security policies of any customers they work on behalf of:

- The Atos Global Information Security Policy [ASM-SEC-0001-EN];
- The Atos UK Information Security Policy [UKSEC-POL0501]; and
- Post Office Ltd. Information Security Policy [IS01].

In the case of any conflict between Post Office Ltd. and Atos information security documentation, the following will apply (in descending order of precedence):

- Post Office Ltd. Schedule 2.1 & Schedule 2.5;
- Post Office Ltd. Information Security Policy [IS01]; and,
- Atos policies and standards.

POL00401508

The availability of quality information security documentation that is always up-to-date is one key component of a correct Post Office Ltd. information security management infrastructure for ensuring information security is implemented and maintained for the Post Office Ltd. and Atos support infrastructures. The other key components are the:

- Institution, and regular review, of a clear information security management organisation;
- Conducting of regular updates of information security risk assessment and management review results;
- CHECK ISHC Testing which is conducted on the Post Office Ltd. IT service provision across the Supply Chain and the reliant supporting data centre environment infrastructure.

The Atos Post Office Ltd. Security Operations Manager will be responsible for ensuring all related Information Security Policies and processes are communicated and validate the adherence to as part of the Post Office Ltd. Service Integrator role.

POL00401508

4. Organising Atos Information Security

Objective (Sec.6.1|BS ISO/IEC 27002:2005):

To manage information security within the organisation.
A management framework should be established to initiate and control the implementation of information security within the organisation.
Management should approve the information security policy, assign security roles and co-ordinate and review the implementation of security across the organisation.
If necessary, a source of specialist information security advice should be established and made available within the organisation. Contacts with external security specialists or groups, including relevant authorities, should be developed to keep up with industrial trends, monitor standards and assessment methods and provide suitable liaison points when handling information security incidents.
A multi-disciplinary approach to information security should be encouraged.

4.1 Security Management Structure and Responsibilities

The Atos Post Office Ltd. Security Operations Manager has overall responsibility for IT and Information Security and its implementation for the Post Office Ltd. IT service provision. The Atos Post Office Ltd. Security Operations Manager will liaise with and report to the Atos Post Office Ltd. Service Director, who has overall responsibility for information security and its implementation within Post Office Ltd.

Day to day operational issues are the responsibility of the Atos Post Office Ltd. Security Operations Manager (SOM), who will ensure and validate that all managers and staff are aware of, and comply with the appropriate policies and procedures.

A summary of the responsibilities of the Atos team is detailed below:

4.1.1 Atos Post Office Ltd. Service Director

The Atos Post Office Ltd. Service Director (SD) will be accountable for the day-to-day maintenance and implementation of the Post Office Ltd. SISD environment, along with the Atos support, infrastructure (i.e. the connections to and between Atos locations) from which, and/or via remote support is provided to Post Office Ltd. Atos is also responsible for ensuring the type and level of information security required for Post Office Ltd. is implemented and maintained for the IT and associated networking etc. and the Atos support, infrastructures. Overall, Atos responsibility rests with the Atos Post Office Ltd. Service Director. Day-to-day activities are delegated to the Atos Post Office Ltd. Security Operations Manager (SOM) and Atos Post Office Ltd. Support Team members (see below).

POL00401508

4.1.2 Atos Post Office Ltd. Security Operations Manager / Support Team

The Atos Post Office Ltd. Security Operations Manager (SOM) reports to the Atos Post Office Ltd. Service Director for the operation of the Post Office Ltd. SISD environment, and the Atos support, infrastructures. The Atos Post Office Ltd. SOM will be responsible for:

- Atos will develop, implement, operate, maintain and certify a cross Supply Chain Member Information Security Management System (ISMS).
- To validate that each Supply Chain Members' Information Security Management System (ISMS) is meeting its contracted security requirements.
- Atos will develop and maintain a Security Management Plan in accordance with Schedule 2.5 within 20 working days after the Effective Contract Date.
- To validate that the IT services meet all applicable Security Requirements (as specified within Schedule 2.1 and Schedule 2.5).
- To coordinate and deliver an annual cross Supply Chain Member threat assessment report.
- Create and maintain a record of Assets, including their business impact assessment, classification and ownership across the Supply Chain Members.
- Provide annual reporting over user accounts and permissions for all users and service recipients.
- Develop, maintain and deliver a cross Supply Chain Member information risk register.
- Providing evidence of cross Supply Chain Members security governance to the Post Office on a monthly basis.
- Ensuring that Atos employees providing services to the Post Office have been vetted appropriately. Furthermore, Atos will validate that Supply Chain personnel involved in the providing services to the Post Office receive annual security awareness training (report nonconformities) and obtain and validate a list of appropriately vetted Supply Chain personnel (report nonconformities).
- Design, implement and maintain the cross Supply Chain Member Security Incident Management process, furthermore, to ensure its integration into the Post Office Incident Management process.
- Establish operating procedures across the Supply Chain Members to monitor and control access to the Post Office data, Infrastructure, Software and Equipment.
- Validate that processes and procedures specified by Atos are adhered to by the Supply Chain Members.
- Collaborating with the Post Office to set Technical Standards and validate that the security controls specified as part of the agreed Technical Standards are implemented across the Supply Chain.
- Establishing a Supply Chain Member organisation structure to deploy, operate and maintain the Post Office Information Security Management processes, tools and policies.

POL00401508

- Validate in-scope PCI systems are judged compliant, by the Post Office Qualified Security Assessor, and report any non-compliance to the Post Office.
- Provide advice and recommendations to the Post Office concerning forensic investigative requests and report on findings where appropriate.
- Atos will be responsible for validating the adherence to and the maintenance of the Information Security Health Check process and remediation activities across the IT Services as defined within Schedule 2.5.

Atos Post Office Ltd. Support Team staff will report to the SOM for the operation of individual services, including the provision of Service Desk. Certain aspects, such as coordinating the creation of new users, may be delegated to these individuals.

Changes to the Post Office Ltd. are only permissible through a valid and approved change request.

All members of Atos staff and all contractors working within the Post Office Ltd. environment are responsible for adhering to Post Office Ltd. Information System Security Standards, including its supporting documentation (including information security guidelines) where appropriate. The Atos UK Vetting team will support the Post Office Ltd. account and are responsible for the verification and validation of all Atos personnel associated to the account. They will ensure appropriate security clearance is obtained and maintained whilst providing services to the Post Office Ltd. account. Furthermore, the Atos UK Vetting team will also coordinate with the appropriate Security Vetting departments across the Supply Chain to verify appropriate clearance of personnel providing services to the Post Office account is in place.

4.2 Information Security Incident and Weakness Reporting

Objective (Sec.13.2|BS ISO/IEC 27002:2005):

To ensure a consistent and effective approach is applied to the management of information security incidents. Responsibilities and procedures should be in place to handle information security events and weaknesses effectively once they have been reported. A process of continual improvement should be applied to the response to, monitoring, evaluating, and overall management of information security incidents. Where evidence is required, it should be collected to ensure compliance with legal requirements.

Any suspected Information Security incident or weakness associated with the Post Office Ltd. Service which is identified/suspected by Atos staff will be reported to the contract Service Desk who will then follow the escalation procedures for the Incident and Problem Management, whilst ensuring reporting is escalated to both Atos, Post Office Ltd. and the Supply Chain, where appropriate.

All security incidents must be reported to the Atos Post Office Ltd. Security Operations Manager and Post Office Ltd. following the Post Office Ltd. Security Incident Management Procedures [to be defined as part of Schedule 2.1|3.6.17].

POL00401508

4.3 Vulnerability Management

Objective (Sec.15.2|BS ISO/IEC 27002:2005):

To ensure compliance of systems with organisational security policies and standards. The security of information systems should be regularly reviewed. Such reviews should be performed against the appropriate security policies and the technical platforms and information systems should be audited for compliance with applicable security implementation standards and documented security controls.

The Post Office Ltd. ICT assets should be patched in a manner compliant with both the Post Office Ltd. Technical Standards and the appropriate Supply Chain Patching Policy. Atos will validate the adequacy of the technical security controls in operation (e.g. malware protection, firewalls, IDS/IPS, vulnerability management, patch management etc.) and report against to the Post Office Ltd.

The Atos Post Office Ltd. Security Operations Manager will work with the Post Office Ltd. Information Security to address any vulnerability identified through the annual CHECK ITHC Testing.

4.4 Agreements on External (Third) Party Access

The Atos Post Office Ltd. SOM will be responsible for ensuring all Atos staff comply with Atos and Post Office Ltd. Information Security Policies and supporting documentation in the provision of services to the Post Office Ltd. as defined within Schedule 2.1 and Schedule 2.5.

The Atos Post Office Ltd. SOM will ensure all arrangements involving external (third) party sub-contracted access (as stated in Schedule 2.5) are based on a formal contract, containing at least the following information security requirements:

- The contractor must comply with the Post Office Ltd. and Atos Information Security Policy and associated documents;
- The contractor must obtain appropriate clearance as required by the Post Office; and
- The contractor must comply with relevant legislation and regulation.

4.5 Outsourcing

Not applicable.

POL00401508

5. Asset Management

Objective (Sec.7.1|BS ISO/IEC 27002:2005):

To achieve and maintain appropriate protection of organisational assets.
All assets should be accounted for and have a nominated owner.
Owners should be identified for all assets and the responsibility for the maintenance of appropriate controls should be assigned. The implementation of specific controls may be delegated by the owner as appropriate but the owner remains responsible for the proper protection of the assets.

5.1 Inventory of Assets

The Atos Post Office Ltd. SOM will have overall responsibility to create and maintain a record of Assets (including information assets). The inventory of assets will include the following:

- Information Assets (including information processing devices);
- Business Impact Assessment;
- Classification [as per Post Office Policy SISD ISO4]; and,
- Owner.

5.2 Acceptable Use of Information and other Assets

The Atos Global Information Security Policy [Doc Ref: ASM-SEC-0001]; Atos UK Information Security Policy [Doc Ref: UKSEC-POL0501]; Atos Global IT Acceptable Use Policy [Doc Ref: ASM-SEC-0013]; the Atos UK Computer Usage Policy [Doc Ref: UKSEC-POL0902] and Post Office Ltd. Acceptable Use Policy require all employees to handle information in a manner appropriate to its classification. The Atos Post Office Ltd. SOM will be responsible for ensuring this is adhered to by all Atos staff.

The Atos Computer Usage Policy [Doc Ref: UKSEC-POL0902], states the employee's responsibilities in all aspects of computer usage. These policies provides the overall framework for a number of more detailed specific policies and applies to all permanent and temporary employees whether employed directly by Atos or sub contracted. [Refer to section 6.2 – Security Awareness]

Breach of these Policies will be considered a disciplinary issue.

POL00401508

5.3 Information Classification

Objective (Sec.7.2|BS ISO/IEC 27002:2005):

To ensure that information receives an appropriate level of protection.
Information should be classified to indicate the need, priorities, and expected degree of protection when handling the information.
Information has varying degrees of sensitivity and criticality. Some items may require an additional level of protection or special handling. An information classification scheme should be used to define an appropriate set of protection levels and communicate the need for special handling measures.

Atos Global Information Classification Policy [ASM-SEC-0003] and the Atos UK Information Classification Policy [UKSEC-POL0702] ensure that the appropriate level of protection is given to Post Office information, according to the potential harm that might be caused by its loss or unauthorised disclosure (as specified in Schedule 2.5|2.2.13).

All relevant policies and processes referred to in this document will cover all classifications of data prescribed by the Post Office in Schedule 2.5. Defined process will apply the appropriate governance and control over the Government data classified by the Post Office as 'Confidential' (with a potential impact of the Government data type being up to and including IL4).

POL00401508

6. Human Resources Security

Objective (Sec.8|BS ISO/IEC 27002:2005):

To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.
Security responsibilities should be addressed prior to employment in adequate job descriptions and in terms and conditions of employment.
All candidates for employment, contractors and third party users should be adequately screened, especially for sensitive jobs.
Employees, contractors and third party users of information processing facilities should sign an agreement on their security roles and responsibilities.

The Atos UK Security Control guidelines document [Doc Ref: UKSEC-STD0502] provides guidelines for security activities within Atos UK in line with the Global and UK policies which Atos UK uses to protect its information assets, derived from the International Standard for Information Security Management Systems – ISO/IEC 27001-2: 2005.

The Security Control guidelines document covers the areas listed below in its guidelines for line managers. Additional controls/procedures will be developed as required in conjunction with Post Office Ltd. to ensure that Atos employees fully comply with Atos and Post Office Ltd. human resources security requirements.

All HR Related Policies and Processes are available in the HR portal for all Atos employees to read and understand.

6.1 Terms and Conditions

The Atos Post Office Ltd. Service Manager will ensure appropriate terms and conditions relating to the job; role descriptions for Atos staff working on the Post Office Ltd. will be clearly defined.

6.2 Information Security Awareness and Training

Objective (Sec.8.2|BS ISO/IEC 27002:2005):

To ensure that employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organisational security policy in the course of their normal work, and to reduce the risk of human error.
Management responsibilities should be defined to ensure that security is applied throughout an individual's employment within the organisation.
An adequate level of awareness, education, and training in security procedures and the correct use of information processing facilities should be provided to all employees, contractors and third party users to minimise possible security risks. A formal disciplinary process for handling security breaches should be established.

POL00401508

The Atos Global Safety and Security guidelines [Doc Ref: ASD-SEC-0008] and the Atos UK Security Awareness and Training Policy [Doc Ref: UKSEC-POL0502] documents the standard Atos awareness and training requirements around information security. Where specific security training is required, this will be provided by the Atos Post Office Ltd. Security Operations Manager.

Awareness and training will cover requirements in the following documents:

- Post Office Ltd. User Security Operating Procedures (SyOPs) [Doc Ref: TBC];
- Post Office Ltd. Security Operating Policy (SyOPs) [Doc Ref: IS05 Security Operating Policy v0.3]; and
- Post Office Ltd. Privileged User Security Operating Procedures (SyOPs) [Doc Ref: TBC].

In accordance with Schedule 2.1 and Schedule 2.5 requirements, Atos will ensure its own personnel undertake appropriate security and awareness training and will have obtained the appropriate security clearance levels before engaging in the provision of services. Furthermore, Atos will validate on an annual basis that the Supply Chain personnel receive annual security awareness briefings and escalate any non-compliance accordingly.

6.3 Disciplinary Process

The Atos Post Office Ltd. Service Manager (as appropriate) will invoke the HR related processes regarding disciplinary proceedings as part of the Post Office Ltd. account. These may result in disciplinary action, up to and including termination of employment.

The Atos UK HR Disciplinary Policy and Procedure [Doc Ref: UKM-HR-0029] documents the details of the Atos disciplinary process.

6.4 Monitoring of Personnel

The Atos Post Office Ltd. Service Manager will follow appropriate management and HR process (the Group HR Policy on Performance Management [Doc Ref: TBC]) to ensure all staff working on the Post Office Ltd. maintain the appropriate level of skills, as well as ensuring the working environment is in keeping with personal goals and development.

Although staff may expect privacy of email, and other related usage of IT equipment, where necessary and following approved HR procedures (Atos UK Computer Usage Policy [Doc Ref: UKSEC-POL0902]) investigations may be carried out where required.

POL00401508

6.5 Termination of Employment

The Atos Post Office Ltd. Service Manager will follow standard HR procedures (see document referenced below) as part of staff termination. This will cover the removal of access, suspension of accounts, and any other Post Office Ltd. specific access that needs to be revoked. Terminations will be communicated to appropriate Post Office Ltd. service consumer and Atos personnel via the Atos Post Office Ltd. OSM as needed.

The Atos UK Leavers Procedures [Doc Ref: Atos HR Guide to Leavers Process] documents the processes for when an Atos Employee leaves the organisation, and a similar Post Office Ltd. Leavers Procedures [Doc Ref: Atos HR Guide to Leavers Process] will cover both Atos personnel as well as Post Office Ltd. users.

6.6 Security Access Cards/Building Passes

All Atos employees are issued with an identity card to enter corporate office locations. Only those Atos employees with a requirement to enter data centres are issued with security passes. All other Atos, Post Office Ltd. or contractor employees require a change request to enter the computer room and are escorted at all times if they are not cleared to SC or above.

The Atos UK Physical Access Control Policy [Doc Ref: UKSEC-POL0901] details the processes for restricting and gaining physical access to Atos owned and managed locations.

6.7 Physical Access to Areas/Rooms Containing Post Office Ltd. Equipment

Access to Post Office Ltd. equipment is limited to those Atos employees with appropriate clearance and an operational requirement to enter to the computer room.

POL00401508

7. Physical and Environmental Security

Objective (Sec.9|BS ISO/IEC 27002:2005):

To prevent unauthorised physical access, damage, and interference to the organisation's premises and information.
Critical or sensitive information processing facilities should be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They should be physically protected from unauthorised access, damage, and interference.
The protection provided should be commensurate with the identified risks.

Each Atos location has a nominated site manager who ensures appropriate action is taken to prevent or react to any information security incidents.

The Atos Post Office Ltd. Security Operations Manager will also ensure, on behalf of the UK Security Directorate, the following site specific items are performed:

- Information security awareness and training
- Site security procedures
- Information security risk assessments
- Information security incident reporting and handling
- Site security reviews
- Business continuity planning and testing; and
- Internal audits in support of the Atos ISO/IEC 27001 certification.

The Information Security Management Business manual [Doc Ref: UKSEC-ISD0101] details these and other responsibilities.

Further documentation is found in Baseline Physical and Environmental Security Standard [Doc Ref: UKSEC-STD0902], Physical Access Control [Doc Ref: UKSEC-POL0901], CCTV Policy [Doc Ref: UKSEC-STD0904], Management of Security Systems and Procedures [Doc Ref: **Error! Unknown document property name.**]. These documents detail the various physical security controls in place at Atos locations, along with standard site requirements such as access control processes, entry point protection, equipment logging and controls. These documents are available from the ISMS and Property and Facilities Management (PFM) portals.

Sites that process Post Office Ltd. data will be assessed in accordance with the following:

- Post Office Ltd. Physical Security Requirements [Doc Ref: TBC].

POL00401508

7.1 Physical and Environmental Security Control Implementation

Atos employs various physical security controls at all its sites, in the form of either Radio-frequency Identification (RFID) or swipe access, additionally where appropriate Personnel Identity Number (PIN) number entry systems (i.e. all Data Centres have RFID and PIN Systems). There must also be a sanctioned change request to gain entry to any Atos data centre.

7.2 Physical Security Perimeter

Atos Facilities Management will take steps to ensure the site perimeters of its locations are controlled and monitored in a manner suitable to the buildings operations. This covers features such as CCTV implementations, 24/7 security guard monitoring and regular patrols and monitoring of all boundaries and entry points.

The Atos Global Physical Environmental Security Policy [Doc Ref: ASM-SEC-0011] and the Baseline Physical Environmental Security [Doc Ref: UKSEC-STD0902] documents the requirements for Atos owned and managed locations.

7.3 Physical Entry and Other Controls

Physical access controls are in place at Atos sites to restrict access to key areas based on an individual's requirements and clearance levels. This is controlled at Atos sites by keypads, proximity access tokens and mantraps (mantraps are limited mainly to Data Centres, but are also deployed where needed for other secure sites).

The Atos Global Physical Environmental Security Policy [Doc Ref: ASM-SEC-0011] and the Baseline Physical Environmental Security [Doc Ref: UKSEC-STD0902] documents the requirements for Atos owned and managed locations.

7.4 Working in Key Rooms/Areas

This is achieved by standard Atos procedures, requiring change approvals for access, as well as signing for token access and approval to enter the restricted area. The Atos Global Physical Environmental Security Policy [Doc Ref: ASM-SEC-0011] and the Baseline Physical Environmental Security [Doc Ref: UKSEC-STD0902] documents the requirements for Atos owned and managed locations.

POL00401508

7.5 Intruder Detection Alarms

Atos Facilities Management will ensure Atos locations have a combination of 24/7 security guard patrols, CCTV and intruder alarms. These controls are standard as part of the Baseline Physical Environmental Security [Doc Ref: 15] requirements.

The Atos Global Physical Environmental Security Policy [Doc Ref: ASM-SEC-0011] and the Baseline Physical Environmental Security [Doc Ref: UKSEC-STD0902] documents the requirements for Atos owned and managed locations.

7.6 Protection of Equipment against Theft

Atos (managed by asset members in various groups) will maintain an inventory of all assets, and clearly label assets as Atos property. Equipment will be secured in restricted areas, access to these areas and removal of equipment is controlled, documented and requested as part of the change control process. The Atos Post Office Ltd. Service Manager has overall responsibility for ensuring this is accomplished for Post Office Ltd. and Post Office Ltd. related assets.

The Atos Global Physical Environmental Security Policy [Doc Ref: ASM-SEC-0011] and the Baseline Physical Environmental Security [Doc Ref: UKSEC-STD0902] documents the requirements for Atos owned and managed locations.

7.7 Equipment Removal

Atos will ensure (through department managers and onsite guard force) processes are in place to ensure equipment is not removed from site without prior approval. Checks in this area will be carried out as part of regular site audits. Permission for equipment removal will be logged as part of a change process; any additional controls required by the Post Office Ltd. will be co-ordinated by the Atos Post Office Ltd. Security Operations Manager. The Atos Post Office Ltd. Service Manager has overall responsibility for ensuring this is accomplished for Post Office Ltd. related equipment.

The Atos Global Physical Environmental Security Policy [Doc Ref: ASM-SEC-0011] and the Baseline Physical Environmental Security [Doc Ref: UKSEC-STD0902] documents the requirements for Atos owned and managed locations.

POL00401508

7.8 Hardware Access Controls

Atos (network, support, and facilities teams) will take steps to ensure all access panels, cabinets, and racks as well as entry points to these areas are controlled and secured. Any instances identified as being different to this will be reported to the Atos Post Office Ltd. Security Operations Manager for remediation and investigation (this could be part of the Site Security Advisor audits). The Post Office Ltd. Security Operations Manager has overall responsibility for ensuring this is accomplished for Post Office Ltd. office related equipment and areas and the Atos Post Office Ltd. Service Manager has overall responsibility for ensuring this is accomplished for Post Office Ltd. hosted assets related equipment and areas i.e. the data centre.

Server Room Security Guideline [Doc Ref: PFM-XX-G9013] gives information on checking access controls are in place and logged which are specific to the Atos Data Centre environments.

7.9 Tamper Detection

Atos (Site Security Advisors, Support Teams, and Facilities Management) will undertake regular Atos site audits; this is in addition to the onsite security guard force carrying out regular patrols. As part of these audits and patrols, any evidence or suspicion of tampering will be reported and actioned accordingly. The Atos Post Office Ltd. Security Operations Manager will also ensure awareness of tampering is covered as part of the information security awareness programmes. The Atos Post Office Ltd. Service Manager has overall responsibility for ensuring this is accomplished in relation to Post Office Ltd. related equipment and areas provided as part of the service:

- Site Security Advisor Audits [Doc Ref: TBC] document details the Atos audit scope and checks that take place;
- Audit Report Template [Doc Ref: TBC]; and
- Audit Improvement Plan Template [Doc Ref: TBC].

7.10 Maintenance and Repair

All access to facilities, server, patching and other restricted areas will require the change control process to be followed for access to be granted. The Atos Post Office Ltd. Security Architect will form part of the change board, and will ensure appropriate controls are in place for both Atos, 3rd Party Staff and Supply Chain personnel as required. All work will be logged and recorded as part of standard change and maintenance processes by the Change Management Team on the Service Desk Manager.

POL00401508

7.11 Power Security

Atos Facilities Management will take steps to implement appropriate redundant power supplies based on the function of the locations in scope. These solutions are based on industry best practice and customer requirements. These controls will be routinely inspected as part of site audits, and tested as part of BCP testing:

- Service requirements within Schedule 8.6 [Doc Ref: Schedule 8.6]; and
- Post Office Ltd. Information Security Policy [Doc Ref: IS01].

7.12 Fire Security

Atos locations are no smoking locations. Atos Facilities Management will also take steps to ensure environments operate in a structured, secure and tidy manner to reduce possible fire risks, even though fire protection systems are in place. These will also be checked as part of site audits:

- Post Office Ltd. Information Security Policy [Doc Ref: IS01]; and
- Checklist Physical Environmental Security [Doc Ref: AOA-FOR-0005 Checklist - Physical and Environmental Security].

7.13 Water/Liquid Security

Atos Facilities Management will implement controls appropriate to the risk of water flooding and liquid related issues in the related Atos facilities and locations based on specific risk assessments. All equipment installed will be maintained and installed to the supplier's documented procedures:

- Post Office Ltd. Information Security Policy [Doc Ref: IS01]; and
- Checklist Physical Environmental Security [Doc Ref: AOA-FOR-0005 Checklist - Physical and Environmental Security].

7.14 Cabling and Related Item Security

Atos Facilities Management and network teams will ensure all Atos power and telecommunications cabling carry data and supporting IT services are protected from tampering and damage. Checklists will be in place to assist in the verification of these controls, and they will also be reviewed as part of the routine audits:

- Checklist Physical Environmental Security [Doc Ref: 24]; and
- Server Room Security Guidelines 2.7 [Doc Ref: PFM-XX-G9013].

POL00401508

7.15 Safety Alerts

Atos (via the UK Security Directorate and line managers) will operate a very security aware organisation, with all staff understanding the responsibility to question anything that appears different to the norm or suspicious. Instructions on the procedures for reporting incidents will be explained at induction along with the appropriate evacuation procedures.

Baseline Physical Environmental Security [Doc Ref: UKSEC-STD0902] documents the requirements for Atos owned and managed locations.

POL00401508

8. Communications and Operations Management

Objective (Sec.10|BS ISO/IEC 27002:2005):

To ensure the correct and secure operation of information processing facilities.
Responsibilities and procedures for the management and operation of all information processing facilities should be established. This includes the development of appropriate operating procedures.
Segregation of duties should be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse.

The Atos Global Information Security Policy [Doc Ref: ASM-SEC-0001] covers various aspects around change control procedures, segregation of duties and other key operational areas. Requirements specific to the Post Office Ltd. services will be reviewed and co-ordinated by the Atos Post Office Ltd. Service Manager to ensure all additional requirements are covered.

8.1 Operational Procedures and Responsibilities

8.1.1 Change Control Procedures

For systems provided by Atos as part of the service, the Atos change management team will ensure all systems have documented operating procedures and all changes to systems are strictly controlled by documented change control procedures. These procedures will be documented and controlled from within the Post Office Ltd. Service Desk system.

8.2 Segregation of Duties and Areas of Responsibility

Atos (HR and line managers) will create job descriptions to cover each individual's job specification and responsibility. Steps will also be taken where appropriate to separate roles, tasks and responsibilities to prevent individuals subverting company or customer critical processes:

- Post Office Ltd. Information Security Policy [Doc Ref: IS01]; and
- Post Office Ltd. Security Operating Policy (SyOPs) [Doc Ref: SISD IS05 Security Operations Policy V0.3].

POL00401508

8.2.1 Separation of Development, Test and Operational Environments

Atos will adhere to Post Office Ltd. specific and good security practices by ensuring different environments exist for different activities, such as, production and non-production. Segregation between these environments will be introduced to prevent data leakage and also to ensure strict access controls to each of these environments. The Atos Post Office Ltd. Security Operations Manager and Atos Post Office Ltd. Service Manager will work in conjunction with the development and support teams to ensure the appropriate environments exist and are in use.

- Post Office Ltd. Information Security Policy section [Doc Ref: IS01].

8.3 System Planning and Acceptance

Objective (Sec.10.3|BS ISO/IEC 27002:2005):

To minimise the risk of systems failures. Advance planning and preparation are required to ensure the availability of adequate capacity and resources to deliver the required system performance. Projections of future capacity requirements should be made, to reduce the risk of system overload. The operational requirements of new systems should be established, documented, and tested prior to their acceptance and use.

8.3.1 Capacity Planning

The Atos capacity planning team will ensure adequate facilities are in place to monitor and forecast capacity requirements, to ensure appropriate storage and processing power is available. Post Office Ltd. will be made aware of issues relating to capacity requirements as part of the service provided by Atos:

- Capacity Management Process [Doc Ref: TBD] documents the process.

8.3.2 System Acceptance

Atos (via the Atos Post Office Ltd. Service Manager, Support and Transition Teams) will take steps to ensure rigorous acceptance testing is undertaken internally and with the customer to ensure the systems function as proposed. Testing and vulnerability assessments will be co-ordinated for the Post Office Ltd, and all findings will be reported and communicated via the appropriate channels. Atos will also be responsible for managing the remediation effort as a result of a health check across the Supply Chain.

POL00401508

8.4 Protection against Malicious and Mobile Code

Objective (Sec.10.4|BS ISO/IEC 27002:2005):

To protect the integrity of software and information. Precautions are required to prevent and detect the introduction of malicious code and unauthorised mobile code. Software and information processing facilities are vulnerable to the introduction of malicious code, such as computer viruses, network worms, Trojan horses, and logic bombs. Users should be made aware of the dangers of malicious code. Managers should, where appropriate, introduce controls to prevent, detect, and remove malicious code and control mobile code.

8.4.1 Prevention

The Atos Post Office Ltd. Service Manager will ensure that all Atos equipment (e.g. PCs/workstations, laptops, servers, etc.) is using authorised software and that controls are in place to prevent unauthorised changes and alterations by malicious code (Viruses, Trojans, Spam etc.). The Atos Post Office Ltd. Security Operations Manager will also be responsible to detail the risks and steps to be taken regarding malicious code.

Atos Post Office Ltd. Support Team staff must ensure:

- System access controls are configured to prevent modification of the boot and partition sector of hard disks;
- All media to be loaded on the Post Office Ltd. environment is subject to malicious code, including virus, checking before loading;
- Only licensed software is loaded on to the Post Office Ltd. environment;
- The use of Open Source, shareware, external software on removable media items (CDs and memory sticks), by any individual is formally authorised, in line with Post Office guidance, after it has been checked for malicious code, including virus scanned;
- Regular checks are made that no games software, free software obtained from magazine disks, and software and information originating from suspect web sites, has been installed;

Specifically for internet facing servers:-

- All servers included those within the internet facing firewall system have malicious code detection installed, including virus software loaded and operating; and
- Malicious code detection software definition files are updated at least daily, and more frequently when new malicious code is reported.

POL00401508

The following policies and procedures will be produced to ensure the security posture of the Post Office Ltd. environment:

- Post Office Ltd. Privileged User Security Operating Procedures (SyOPs) [Doc Ref: TBC];
- Post Office Ltd. Security Operating Policy (SyOPs) [Doc Ref: IS05 Security Operating Policy v0.3]; and
- Post Office Ltd. Email and Internet Policy [Doc Ref: TBC].

8.4.2 Detection

The Atos Post Office Ltd. Service Manager will ensure all systems relating to Post Office Ltd. will have approved and adequate controls in place to mitigate against the risk of malicious code and aid detection and removal. This will be verified by audits co-ordinated / conducted by the Atos Post Office Ltd. Security Operations Manager.

The Atos Post Office Ltd. Service Manager will ensure:

- Approved anti-malicious code detection, including virus detection software packages, are in place on the Post Office Ltd. servers and (including memory resident malicious code (including virus) protection), are configured to be used at start-up, and are operational at all times;
- All mail systems servers have malicious code (including virus checking software) implemented, and in particular all external mail gateways are equipped with online malicious code, including virus checking software, operational at all times, to sweep all incoming mail and attachments;
- All anti-malicious code (including virus checking) software is updated with the latest versions/service packs, including virus, definition files at least daily, or more regularly if it is required (e.g. due to a new malicious code, including virus, that requires immediate action to eradicate);
- In conjunction with the Atos Post Office Ltd. Service Manager, procedures to reduce the risk from, detect an occurrence of and recover from malicious code are fully documented, maintained and promulgated – as for use by only authorised and appropriately skilled personnel.

Users must report *immediately* any suspicions of malicious code to the IT Service Desk, which must then immediately inform the SOM and relevant support team.

POL00401508

Procedures to reduce the risk from, detect an occurrence of, and recover from malicious code will be documented, maintained and promulgated by Atos – as for use by only authorised and appropriately skilled personnel:

- Post Office Ltd. Patching Policy [Doc Ref: TBC];
- Post Office Ltd. Privileged User SyOps [Doc Ref: TBC];
- Post Office Ltd. Malicious Code Policy [Doc Ref: TBC]; and
- Post Office Ltd. Protective Monitoring Policy [Doc Ref: TBC].

8.4.3 Recovery

The Post Office Ltd. Service Desk will provide initial support to users who suspect infection of malicious code, and will provide steps to resolve the incident, and block access to malicious sites\domains.

8.4.4 Mobile Code

Where mobile code has been approved, the Atos Post Office Ltd. Service Manager and the Atos Post Office Ltd. Security Operations Manager will ensure that the configuration will operate as defined and documented in agreement with the Post Office Ltd. Accreditor.

8.5 Back-up and Recovery

Objective (Sec.10.5|BS ISO/IEC 27002:2005):

To maintain the integrity and availability of information and information processing facilities. Routine procedures should be established to implement the agreed back-up policy and strategy (see also 14.1) for taking back-up copies of data and rehearsing their timely restoration

The Atos Post Office Ltd. Service Manager will take steps to suitably backup all critical systems, and transport and store the media securely. This process is verified as part of routine audits and backup verification testing.

- Post Office Ltd. Information Security Policy [Doc Ref: IS01].

8.6 IT Component Start-up and Close Down

The Atos Post Office Ltd. Service Manager will ensure the hardware is built and operates based on agreed builds reviewed and approved by the Post Office Ltd. Lead Architect as part of service delivery. These will feature best practice processes, vendor configuration guidance and where appropriate Post Office Ltd. specific requirements as part of the supported build.

POL00401508

8.7 Media (including Document) Security

Objective (Sec.10.7|BS ISO/IEC 27002:2005):

To prevent unauthorised disclosure, modification, removal or destruction of assets, and interruption to business activities. Media should be controlled and physically protected. Appropriate operating procedures should be established to protect documents, computer media (e.g. tapes, disks), input/output data and system documentation from unauthorised disclosure, modification, removal, and destruction.

8.7.1 Management of Removable Media

The Atos Post Office Ltd. Service Manager will ensure all staff working on the Post Office Ltd. account, are aware of the appropriate controls and methods that should be used, particularly around any media containing business critical information.

Further information can be found in the following Atos and CESG documents:

- Media Handling and Disposal Policy [Doc Ref: UKSEC-POL1005];
- Removable Media Disposal and Destruction of Sensitive Data [Doc Ref: TBD]; and
- IS5 – Secure Sanitisation of Protectively Marked or Sensitive Information [Doc Ref: TBC].

8.7.2 Printed Output

The Atos Post Office Ltd. Service Manager will ensure all staff working on the Post Office Ltd. account, are aware of the appropriate controls and methods that should be used to ensure the printed output is handled and stored in accordance with its protective marking. Destruction must take the form of, shredding, pulping or incineration, to prevent reconstruction in line with CESG IS5 [Doc Ref: TBC].

8.7.3 Secure Re-use or Disposal of Media

The Atos Post Office Ltd. Security Operations Manager will ensure media and hardware will be securely disposed of, or recycled for use in line with Atos and Post Office Ltd. policies, and HMG/CESG policy (where appropriate) when Re-Using and Disposing of Media.

Further information can be found in the following Atos and CESG documents:

- Removable Media Data Encryption Procedure [Doc Ref: TBD];

POL00401508

- Removable Media Disposal and Destruction of Sensitive Data [Doc Ref: TBD]; and
- IS5 – Secure Sanitisation of Protectively Marked or Sensitive Information [Doc Ref: TBC].

8.8 Exchange of Information

Objective (Sec.10.8|BS ISO/IEC 27002:2005):

To maintain the security of information and software exchanged within an organisation and with any external entity. Exchanges of information and software between organisations should be based on a formal exchange policy, carried out in line with exchange agreements, and should be compliant with any relevant legislation.

The Atos Post Office Ltd. Security Operations Manager will ensure staff are made aware of appropriate email usage and etiquette; these are communicated through awareness and documentation Messaging Policy [Doc Ref: TBD] and Email Etiquette Policy [Doc Ref: TBD] and any specific Post Office Ltd. requirements.

Furthermore, Atos recognises the sensitivities concerning the sharing of potentially sensitive information between suppliers and as such has developed the Secure Exchange of Information Policy (Doc Ref: UKSEC-POL1006) to ensure that Atos employees abide by a cross supply chain procedure in agreement with the Post Office Ltd.

8.9 Monitoring

Objective (Sec.10.10|BS ISO/IEC 27002:2005):

To detect unauthorised information processing activities. Systems should be monitored and information security events should be recorded. Operator logs and fault logging should be used to ensure information system problems are identified. An organisation should comply with all relevant legal requirements applicable to its monitoring and logging activities. System monitoring should be used to check the effectiveness of controls adopted and to verify conformity to an access policy model Procedures and standards should be established to protect information and physical media containing information in transit.

8.9.1 Accounting and Audit

Atos regularly carries out internal and external audits by various accrediting bodies. Internal audits are the responsibility of the Security Site Advisor as documented in Site Security Advisor Audits [Doc Ref: 41]. In addition to these more physical audits, logical logs are recorded and monitored on all critical systems.

POL00401508

The Atos Post Office Ltd. Security Operations Manager will review physical and logical logs in order to meet service consumer requirements. Furthermore, as defined within Schedule 2.5, Atos will conduct compliance reviews across the Supply Chain where appropriate to ensure service levels are maintained:

- Post Office Ltd. Information Security Policy [Doc Ref: IS01]; and
- Site Security Advisor Audits [Doc Ref: TBD].

8.9.2 Clock Synchronisation

Atos will synchronise all computer clocks with a recognised central time source as standard to ensure log timing accuracy exists when reviewing logs and carrying out investigations. In this instance this will be the GSi/PSN (or equivalent) time source as provided by the Post Office Ltd. Network Service Tower (to be confirmed).

The Atos Post Office Ltd. Service Manager will ensure a clock re-synchronisation and check takes place after every change to daylight saving hours.

8.10 Operator Logs

The Atos Post Office Ltd. Service Manager will ensure operator activities will be logged through a combination of change controls and tickets within the Post Office Ltd. Service Desk for all Post Office Ltd. related activities.

8.11 Fault Logging

The Atos Post Office Ltd. Service Manager will ensure that all faults are recorded in the Service Desk.

8.12 Encryption

Where appropriate, inter-site traffic must be encrypted in a manner compliant with the Post Office Ltd. Cryptographic Policy [Doc Ref: TBC] for support office locations.

The general rule is that removable media and Full Desk Encryption (FDE) of assets that leave any Post Office Ltd. office location must be encrypted in a manner compliant with the Atos Removable Media Policy and Post Office policy, except where the SIRO has given an exemption for business purposes.

POL00401508

9. Access Control

Objective (Sec.11|BS ISO/IEC 27002:2005):

To control access to information. Access to information, information processing facilities, and business processes should be controlled on the basis of business and security requirements. Access control rules should take account of policies for information dissemination and authorisation.

9.1 User Account Management

This section relates to Atos staff providing support on the Post Office Ltd. account.

9.1.1 User Account Requests

Accounts created for use by Post Office Ltd. are covered by the following processes and procedures:

- Post Office Ltd. Logical Access Control [Doc Ref: IS06]
- Atos Password Policy [Doc Ref: UKSEC-POL1102_Password_Policy].

All account requests must be raised as a ticket in Post Office Ltd. Service Desk.

9.1.2 User Account Creation

The Atos Post Office Ltd. Security Operations Manager will be responsible for the requesting of Privileged accounts for Atos staff and the Post Office Ltd. This will ensure the least privilege access for the user, along with recording of access permissions granted.

Post Office Ltd. Service Desk accounts for employees will be subject to review and approval via a change request:

- Post Office Ltd. Password Policy [Doc Ref: TBC]
- Atos Password Policy [Doc Ref: UKSEC-POL1102_Password_Policy].

9.1.3 Review, Disabling and Deletion of User Accounts

The Atos Post Office Ltd. Security Operations Manager will ensure regular reviews are conducted on user account usage and requirements in accordance with the Schedule 2.1 and Schedule 2.5 requirements. Reporting will include failed access attempts, accounts that have not been used for significant amounts of time along with enabling and disabling of appropriate service accounts:

- Post Office Ltd. Routine Compliancy Review [Doc Ref: TBD]; and
- Post Office Ltd. Account User Maintenance Guidance [Doc Ref: TBC].

POL00401508

9.2 Access Control Configuration

The Post Office Ltd. Password Policy outlines the password controls within Post Office Ltd. The Atos Post Office Ltd. Security Operations Manager will ensure the requirements are adhered to.

- Post Office Ltd. Password Policy [Doc Ref: TBC]
- Atos Password Policy [Doc Ref: UKSEC-POL1102_Password_Policy].

9.3 Password Management

9.3.1 Control and Implementation

Atos user account and password management will follow standard procedures for all accounts used in association with the Post Office Ltd. systems:

- Post Office Ltd. Password Policy [Doc Ref: TBC]
- Atos Password Policy [Doc Ref: UKSEC-POL1102_Password_Policy].

9.3.2 Password Generation

For systems provided by Atos, through support teams, will generate passwords in accordance with Post Office Ltd. Password Policy and the Atos Password Policy for access to systems used in the provision of the service with the Post Office Ltd:

- Post Office Ltd. Password Policy [Doc Ref: TBC]
- Atos Password Policy [Doc Ref: UKSEC-POL1102_Password_Policy]

9.3.3 Password Storage and Transmission

The Atos Post Office Ltd. Security Operations Manager and/or Service Desk will distribute Post Office Ltd. related user account and password information. Privileged user information relating to Post Office Ltd. will be provided and stored in accordance with the following documents:-

- Post Office Ltd. Password Policy [Doc Ref: TBC]
- Post Office Ltd. Information Security Policy [Doc Ref: IS01]
- Atos Password Policy [Doc Ref: UKSEC-POL1102_Password_Policy]

POL00401508

9.3.4 Changing Passwords

Atos (through support teams) will manage passwords of its systems in accordance with Post Office Ltd. Password Policy [Doc Ref: TBC] and the Atos Password Policy [Doc Ref: UKSEC-POL1102]. The Atos Post Office Ltd. Service Manager has overall responsibility for ensuring this is accomplished.

9.3.5 Review of Passwords

The Atos Post Office Ltd. Security Operations Manager will take steps to monitor password change management. In the event a password has changed from the password guidelines, the manual forcing of password policy will be implemented in line with:

- Post Office Ltd. Password Policy [Doc Ref: TBC];
- Post Office Ltd. Privileged User SyOps [Doc Ref: TBC];
- Post Office Ltd. Security Operating Policy (SyOPs) [Doc Ref: IS05 Security Operating Policy v0.3];
- Post Office Ltd. Information Security Policy [Doc Ref: IS01]; and
- Atos Password Policy [Doc Ref: UKSEC-POL1102_Password_Policy].

9.3.6 Maintenance Passwords (Service Accounts)

The Atos Post Office Ltd. Security Operations Manager will ensure the disabling and enabling of maintenance passwords relating to the Post Office Ltd. on an 'as required' basis. This will be controlled and monitored though standard change controls procedures and reported against as part of the Schedule 2.1 requirements.

9.3.7 Service Accounts Passwords

The Atos Post Office Ltd. Security Operations Manager will ensure the service accounts for machine-to-machine interaction will be regularly reviewed. This will be controlled and monitored though standard Atos change controls procedures. All changes will be recorded with the Service Desk.

9.3.8 Privileged User/System Management Supervisory Passwords

The Atos Post Office Ltd. Security Operations Manager will ensure privileged accounts relating to systems and infrastructures are only held by Atos individuals assigned to support the Post Office Ltd. account for systems pertinent to the delivery of the Atos service.

POL00401508

9.4 Network Access Control

The Atos Logical Access Control Policy [Doc Ref: UKSEC-POL1101] documents the Network Connectivity requirements for services relevant to the Post Office Ltd. The Atos Post Office Ltd. Service Manager has overall responsibility for ensuring network access control requirements in relation to Post Office Ltd. service are maintained in accordance with Post Office Standards and related documents.

9.4.1 General

Atos will ensure that the all networking infrastructure is documented. This documentation will cover justifications for any diagnostic points, along with methods for ensuring the infrastructure meets Post Office Ltd. requirements. These activities will be co-ordinated by the Atos Post Office Ltd. Security Operations Manager.

9.4.2 External Connections

The Atos Post Office Ltd. Security Operations Manager will ensure all external connections under Atos supervision are configured and have the appropriate rule agreed with the Post Office Ltd. Information Security Team. (This will cover all firewalls within scope of the engagement). The main Atos external connection in relation to Post Office Ltd. will be remote access configurations, used to provide support:

- Post Office Ltd. Information Security Policy [Doc Ref: TBD]

9.5 Remote Access

Only Atos staff may connect to the Atos Private Network, and this is ensured via two factor authentication methods; once connected, security will be established via an IPSEC VPN. The Atos Post Office Ltd. Security Operations Manager will ensure any remote support / access to the Post Office Ltd. environment will follow the security requirements detailed in Post Office Ltd. and CESG security policy documents.

Any additional remote connectivity to Post Office Ltd. resources will be subject to Post Office Ltd. Accreditor security approval. All Post Office Ltd. laptops must have their hard disk encrypted with a CESG approved full disk encryption product:

- Post Office Ltd. Information Security Policy [Doc Ref: 23];
- Atos Remote Working Policy [Doc Ref: UKSEC-POL1104]

POL00401508

9.6 Operating System, Application and Information, Access Control

The Atos Post Office Ltd. Service Manager will ensure all equipment used as part of the Atos service to the Post Office Ltd. will be based on a signed off build, with appropriate controls to protect information, applications systems, and functionality.

9.7 Mobile Computing and Teleworking

9.7.1 Laptop Security

The Atos Post Office Ltd. Security Operations Manager will ensure all Post Office Ltd. related Atos users are made aware of the various risks associated with using laptops outside of the office through information security awareness and training. The main areas of focus will cover what information shouldn't be stored on the laptop, care of ownership whilst out of the office, risks of shoulder surfing, and other security risks of which users should be aware. All laptops must have their hard disk encrypted with a CESG approved full disk encryption product:

- Atos IT Acceptable Use Policy [Doc Ref: ASM-SEC-0013];
- Post Office Ltd. Data Classification and Handling Policy [Doc Ref: TBD];
- Post Office Protective Marking System Policy [Doc Ref: TBD].

POL00401508

10. Information Systems Acquisition, Development and Maintenance

Objective (Sec.12|BS ISO/IEC 27002:2005):

To ensure that security is an integral part of information systems.
Information systems include operating systems, infrastructure, business applications, off-the-shelf products, services, and user-developed applications. The design and implementation of the information system supporting the business process can be crucial for security. Security requirements should be identified and agreed prior to the development and/or implementation of information systems.
All security requirements should be identified at the requirements phase of a project and justified, agreed, and documented as part of the overall business case for an information system.

10.1 Security of System Files

10.1.1 Control of Operational Software

The Atos Post Office Ltd. Service Manager will ensure any changes to systems in support of the Atos services to the Post Office Ltd. are fully tested with a managed migration and full rollback plan, and follow change process controls.

10.1.2 Protection of System Test Data

The Atos Post Office Ltd. Service Manager will ensure the standard change control process is followed relating to all Post Office Ltd. systems data testing. As part of best practice, test data will remain separate from production environments, and is only used for the purpose of testing and development. The system will then be purged of data to ensure it conforms to Post Office requirements (TBC):

- Post Office Ltd. Information Security Policy [Doc Ref: TBC];
- Post Office Ltd. Decommissioning Policy [Doc Ref: TBC];
- Post Office Ltd. Information Classification [Doc Ref: S04 & S04a]; and

10.1.3 Protection of Source Code

The Atos Post Office Ltd. Service Manager will take steps to ensure backups cover source code related material as appropriate:

- Atos relevant documentation (TBC)

POL00401508

10.2 Security in Development and Support Processes

Objective (Sec.12.5|BS ISO/IEC 27002:2005):

To maintain the security of application system software and information.
Project and support environments should be strictly controlled. Managers responsible for application systems should also be responsible for the security of the project or support environment. They should ensure that all proposed system changes are reviewed to check that they do not compromise the security of either the system or the operating environment.

10.2.1 System and Application Software Integrity

The Atos Post Office Ltd. Service Manager will ensure any changes to Atos systems and application software in support of the service follow standard change control procedures, and any updates will be tested as appropriate.

- Post Office Ltd. Information Security Policy [Doc Ref: IS01].

The Atos Post Office Ltd. Support Team will:-

- Only install system software from original master media supplied by the Manufacturer/supplier;
- Only load the master media onto the processors when write-protected;
- Keep the master media secured when not in use; and
- Make a record of the media and its location in a Media Register.

10.2.2 Sub-Contracted/Outsourced Software Development

The Atos Post Office Ltd. Service Manager will ensure Post Office Ltd. contract requirements are met in the event software development is sub-contracted/ outsourced outside of Atos.

10.3 Software Maintenance

The Atos Post Office Ltd. Service Manager will ensure only authorised personnel perform any software maintenance in relation to the Post Office Ltd, and any maintenance requirements will be raised using the standard change management process. All maintenance will be carried out in the test environment and tested before moving into production.

10.4 Software Fault Log

Atos will keep appropriate logs of Post Office Ltd. software faults and the corrective actions taken to resolve any issues.

POL00401508

10.5 Technical Vulnerability Management

The Atos Post Office Ltd. Security Operations Manager will ensure the latest information on vulnerabilities (utilising the Atos ISRM Vulnerabilities Database), and vendor alerts relating to Atos provided Post Office Ltd. applications and Post Office Ltd. systems is obtained and understood on a regular basis. Vulnerabilities relating to information security will be applied immediately through appropriate change control procedures.

- Post Office Ltd. Patching Policy [Doc Ref: TBC].

POL00401508

11. Information Security Incident Management

Objective (Sec.12.5|BS ISO/IEC 27002:2005):

To ensure a consistent and effective approach is applied to the management of information security incidents.

The following documents are the Atos procedures for handling an Information Security related incident:

- Atos Security Incident Management Policy [Doc Ref: ASM-SEC-0010]
- Post Office Security Incident Management Procedure [Doc Ref: TBD]

11.1 Information Security Incidents and Weaknesses

The Atos Post Office Ltd. Security Operations Manager will be the main point of contact and co-ordinator for all Post Office Ltd. related incidents. The Atos Post Office Ltd. Security Operations Manager will be responsible for communicating with the appropriate parties, leading the investigation from an Atos and Post Office (Supply Chain) perspective and using appropriate documentation to track and report the incident response. Post Office Ltd. Service Desk is the repository for all security incidents. The Post Office Ltd. Security Working Group (SWG) is the forum for discussing security incidents.

The following documents are also relevant:

- Post Office Ltd. Security Incident Management Procedure [Doc Ref: TBD]; and
- Atos Security Incident Management Policy [Doc Ref: ASM-SEC-0010].

11.2 IT/Networking Malfunctions

The Atos Post Office Ltd. Security Operations Manager will be the main point of contact and co-ordinator for all Post Office Ltd. related incidents. The Atos Post Office Ltd. Security Operations Manager will be responsible for communicating to appropriate parties, leading the investigation from an Atos perspective and using appropriate documentation to track and report the incident response. Post Office Ltd. Service Desk is the repository for all problem incidents. The Post Office Ltd. Security Working Group (SWG) is the forum for discussing problem incidents.

The following documents are also relevant:

- Post Office Ltd. Security Incident Management Procedure [Doc Ref: SISD IS11 Information Security Incident Management Policy V0.4]; and
- Atos Security Incident Management [Doc Ref: ASM-SEC-0010].

POL00401508

11.3 Learning from Information Security Incidents

The Atos Post Office Ltd. Security Operations Manager will review the actions and results of a security incident relating to the Post Office Ltd. and identify lessons learned to reduce the possibility of recurrence. Lessons learned for other engagements will also be utilised to benefit the Post Office Ltd. by identifying any security related weaknesses. These will be raised and discussed via the SWG.

The following documents are also relevant:

- Post Office Ltd. Security Incident Management Procedures [Doc Ref: SISD IS11 Information Security Incident Management Policy V0.4];
- Atos Security Incident reporting process for users [Doc Ref: ASP-SEC-0038];
- Atos Security Incident Submission Form [Doc Ref: ASD-SEC-0039].

11.4 Disciplinary Process in context of Information Security Incidents

The Atos Post Office Ltd. Service Manager, will as appropriate, invoke HR related processes regarding disciplinary proceedings as part of the Post Office Ltd. engagement. These may result in disciplinary action, up to and including termination of employment. This process will be facilitated by the line manager:

- Post Office Ltd. Information Security Policy [Doc Ref: IS01]; and
- Atos Disciplinary Policy and Procedure [Doc Ref: TBC].

POL00401508

12. Business Continuity Management

Objective (Sec.14|BS ISO/IEC 27002:2005):

To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption. A business continuity management process should be implemented to minimise the impact on the organisation and recover from loss of information assets (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventive and recovery controls. This process should identify the critical business processes and integrate the information security management requirements of business continuity with other continuity requirements relating to such aspects as operations, staffing, materials, transport and facilities.
The consequences of disasters, security failures, loss of service, and service availability should be subject to a business impact analysis. Business continuity plans should be developed and implemented to ensure timely resumption of essential operations. Information security should be an integral part of the overall business continuity process, and other management processes within the organisation.
Business continuity management should include controls to identify and reduce risks, in addition to the general risks assessment process, limit the consequences of damaging incidents, and ensure that information required for business processes is readily available.

12.1 Business Continuity Planning

Specific Atos Site based business continuity plans are developed using the standard Security Directorate approved Template, Site Business Continuity Plan. The Service Desk has full DR capabilities:

- ATF DR procedures [Doc Ref: TBC]

12.2 Back-up Procedures

The Atos Post Office Ltd. Service Manager will take steps to ensure Atos Post Office Ltd. support staff suitably backup all critical systems, and transport and store the media securely. This process is verified as part of routine audits and backup verification testing. Any specific Post Office Ltd. backup requirements will be followed as documented in the work instructions:

- Post Office Ltd. Information Security Policy [Doc Ref: IS01].

POL00401508

12.3 Emergencies and Breakdowns

12.3.1 Hardware Failures

In the event of hardware failure, the Atos Post Office Ltd. Service Manager will follow the appropriate Post Office Ltd. steps in order to resume service in line with predefined SLAs (TBC). The steps taken will be recorded in the appropriate logs, and support staff will be notified as required.

12.3.2 Software Failures

In the event of software failure, the Atos Post Office Ltd. Service Manager will follow the appropriate Post Office Ltd. steps in order to resume service in line with predefined SLAs. The steps taken will be recorded in the appropriate logs, and support staff will be notified as required.

12.3.3 Fire/Building Evacuation

Where appropriate, as part of the induction process, Atos staff will be given instructions and briefings regarding fire and building evacuation. Staff working on the Post Office Ltd. account will comply with Atos evacuation procedures as appropriate. The Atos Post Office Ltd. Service Manager will ensure appropriate inductions are initiated. Where onsite presence is required, then it is assumed that the Post Office will provide the appropriate induction for Atos staff visiting Post Office locations.

POL00401508

13. Compliance

Objective (Sec.15|BS ISO/IEC 27002:2005):

To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements. The design, operation, use, and management of information systems may be subject to statutory, regulatory, and contractual security requirements. Advice on specific legal requirements should be sought from the organisation's legal advisers, or suitably qualified legal practitioners. Legislative requirements vary from country to country and may vary for information created in one country that is transmitted to another country (i.e. trans-border data flow).

13.1 Compliance with Legal Requirements

The Atos Post Office Ltd. Security Operations Manager will ensure appropriate compliance with legal, regulatory and contractual requirements are met as described in the Post Office Ltd. Schedule 2.1 and Schedule 2.5 requirements. This will include conducting Supply Chain reviews and making appropriate information available for Post Office Ltd. information security compliance reviews.

- Schedule 2.1;
- Schedule 2.5;
- ISO27001;
- PCI-DSS (where appropriate);
- Post Office Ltd. Information Security Policy [Doc Ref: IS01].

13.2 Compliance with Information Security Policies and Standards, and Technical Compliance

Atos ensures compliance with various regulations through its use of internal and external audits against published policy. Where appropriate, the Atos Post Office Ltd. Security Operations Manager will assist Post Office Ltd. to meet compliance requirements documented in the Post Office Ltd. Security Standards where responsibility lies with Atos:

- Schedule 2.1;
- Schedule 2.5;

POL00401508

- ISO27001;
- PCI-DSS (where appropriate);
- Post Office Ltd. Information Security Policy [Doc Ref: IS01].

13.3 Transition to Compliance

Atos will develop and introduce a cross-supplier procedure (CSP) specifically for the development of the ISMS across the supply chain. The procedure will ensure the appropriate transition of current security activities across the supply chain to be incorporated into a single ISMS, across the service. Atos will manage the transition period for each supplier and monitor their progression to achieving certification within a 12 month period from the contract effective date.

13.4 Protection of System Audit Tools

The Atos Post Office Ltd. Security Operations Manager will ensure system audit related tools are not installed and operational on a permanent basis in the Post Office Ltd. environment. Any access and usage is controlled and approved through appropriate change control procedures.

POL00401508

14. Document Configuration

14.1 Feedback

The Atos Post Office Ltd. Security Operations Manager will be responsible for informing the Post Office Ltd. Information Security Team (via the SWG) in relation to any changes, and/or recommendations to this document and those documents referenced from this document.

14.2 Changes

The Atos Post Office Ltd. Security Operations Manager will ensure any appropriate changes to this document and those documents referenced from this document are understood and communicated to the Post Office Ltd. project staff (via the SWG under the governance of Change Control procedures).

POL00401508

15. Document References

Reference ID	Doc Ref	Title	Version	Date
1	TBC	Post Office Ltd. Organisational Terms of Reference		
2	IS11	Post Office Ltd. Security Incident Management Procedures		
3	IS09	Post Office Ltd. Patching Policy		
4	N/A	Post Office Ltd. Code of Connection		
5	SEC0001	Atos UK Information Security Policy		
6	TBC	Atos Computer Usage Policy		
7	TBC	UK Security Control guidelines		
8	TBC	Security Awareness and Training Policy		
9	TBC	Post Office Ltd. Security Operating Policy (SyOPs) [Doc Ref: IS05 Security Operating Policy v0.3];		
10	TBC	Post Office Ltd. Privileged User Security Operating Procedures (SyOPs)		
11	TBC	Performance Management Guidelines		
12	TBC	Atos Leavers Procedures		
13	TBC	Physical Access Control		
14	TBC	The Information Security Management Business manual		
15	TBC	Baseline Physical Environmental Security		
16	STD0904	CCTV Policy		

POL00401508

Post Office Ltd. – Security Management Plan

Reference ID	Doc Ref	Title	Version	Date
17	P9046	Management of Security Systems and Procedures		
18	G9013	Server Room Security Guidelines		
19	0005	Site Security Advisor Audits		
20	TBC	Audit Report Template		
21	TBC	Audit Improvement Plan Template		
22	TBC	Service Specification Utilities		
23	IS01	Post Office Ltd. Information Security Policy		
24	TBC	Checklist Physical Environmental Security		
25	TBC	Capacity Management Process		
26	IS03	Post Office Ltd. Acceptable Use Policy		
27	TBC	Post Office Ltd. Malicious Code Policy		
28	TBC	Post Office Ltd. Protective Monitoring Policy		
29	TBC	Removable Media Data Encryption Procedure		
30	TBC	Removable Media Disposal and Destruction of Sensitive Data		
31	IS5	Secure Sanitisation of Protectively Marked or Sensitive Information		
32	TBC	Messaging Policy		
33	TBC	Email Etiquette Policy		
34	TBC	Post Office Ltd. Cryptographic Policy		
35	TBC	Atos Global Information Security Policy		

POL00401508

Post Office Ltd. – Security Management Plan

Reference ID	Doc Ref	Title	Version	Date
36	TBC	Post Office Ltd. Access Control Policy		
37	TBC	Post Office Ltd. Password Policy		
38	TBC	Post Office Ltd. Routine Compliancy Review		
39	TBC	Post Office Ltd. Leavers Procedures		
40	CESG Memo 26	CESG Memo 26 – Passwords for Identification and Authentication		
41	TBC	Site Security Advisor Audits		
42	IAS6	Protecting Personal Data		
43	TBC	Post Office Ltd. Patching Policy		
44	GPG10	Good Practice Guide – Remote Working		
45	TBC	Client Policy		
46	TBC	Laptop Code of Conduct		
47	Government Protective Marking System Policy February 2010	Government Protective Marking System Policy February 2010		
48	TBC	Post Office Ltd. Account User Maintenance Guidance		
49	TBC	Post Office Ltd. Decommissioning Policy		
50	TBC	PSN Code of Connection		
51	TBC	Serious Incident Management Security Directorate		
52	TBC	Security Serious Incident Procedure Checklist		

POL00401508

Post Office Ltd. – Security Management Plan

Reference ID	Doc Ref	Title	Version	Date
53	TBC	Security Incident Report		
54	TBC	Business Continuity Planning Checklist		
55	TBC	Business Continuity Management		
56	TBC	Site Business Continuity Plan		
57	TBC	Post Office Ltd. RMADS		
58	TBC	Post Office Ltd. Cardinal RMADS		
59	IS4	Communications Security & Cryptography Management of Cryptographic Systems		
60	TBC	Post Office Ltd. Data Classification and Handling Policy		
61	TBC	Post Office Ltd. Physical Security Requirements		
62	TBC	Post Office Ltd. Security Operating Procedures (SyOPs)		
63	TBC	Post Office Ltd. Post Office Ltd. Security Aspects Letter (SAL)		
64	TBC	Atos Disciplinary Policy and Procedure		