POL00397087

POca Service Delivery

Security Policy

Document Reference:	AFSO EMEA-POca-0481
Issue Number:	Version 2.1
Issue Date:	30th July 2009
Template Version:	4.3

POL00397087

Document Authorisation

	Name	Signature	Date
Written by:	Mark Geldart		
Reviewed by:	Gursharan Virdi Kay Ruddeforth-Tan Dave Riley David Forster Dave Solkin Dan Carpenter Ian Fenelon Steve Hill Ian Stevenson Madeleine Ververis JPM		
Approved by:	Martin Timms Ross Craig		
Authorised by:	Mike Daley		

Amendment History

Issue	Date	Nature Of Change
1.0	April 2003	Original Security Policy released
2.a	5th June 2009	Updated for ISO27001 review
2.b	11th June 2009	Updated and issued for GV/KRT comment
2.c	23rd June 2009	Incorporated comments from review
2.d	30th June 2009	Added more comments and updated referenced items
2.e	15th July 2009	More comments from CAP added. WPR comments added. Issued for formal WPR
2.0	22nd July 2009	Issued following formal WPR (No JPM comments incorporated and will be added to next version)
2.1	30th July 2009	Added JPM comments and final tidy up

Distribution List

Name	Copy Number

POL00397087

Terminology

Abbreviation	Description
ASFO EMEA Government and Healthcare Industry Unit	Applications Services Field Operations Europe, Middle East and Africa Government and Healthcare Industry Unit
BAU	Business as usual
BPO	Business Process Outsourcing
C&W	Cable and Wireless
CMS	Content Management System
CRM	Customer Relationship Management
CSO	Client Security Officer
ISM	Information Security Manager
ITO	Infrastructure Technology Outsourcing
POca	Post Office Card Account
TCT	Thames Card Technology
TTI	Toshiba Topham IDData
USB	Universal Serial Bus
VPN	Virtual Private Network

References

EDS Security Policy	
POca Permit to Work Process	
Card Account Security Statement	
EDS Information Handling Security Policy	
EDS Information Handling Security Requirements	
EDS Code of Business Conduct	
Computer Incident Response Plan Notification and Escalation Procedures	
POca Change Management Process	
EDS Security Policy (Data centre access control)	
EDS UK Electronic Communications Policy	
EDS E-mail Etiquette Policy	
90 Day User Access Audit Process	
Electronic Benefits Transfer System Key Management For EMV Version 0.1	
EDS Records Retention Policy	
EDS Code of Practice for Privacy and Data Protection	
EDS Use of Corporate Assets Policy Protecting EDS Assets	
Use of Non-EDS Software Policy	
Global Privacy and Data Protection Policy	
Violence in the Workplace Policy	
Enterprise Security Policies and Standards	
Compliance with the United States Foreign Corrupt Practices Act	
Internal Control Policy	

POL00397087

Post Office Limited Community Information Security Policy	
Freedom of Information Act 2000	
The Data Protection Act 1998	
The Official Secrets Act 1989	
The Computer Misuse Act 1990	
The Copyright, Designs and Patents Act 1988	
Financial Services and Markets Act 2000	
Regulation of Investigatory Powers Act 2000	
Electronic Communications Act 2000 as amended by the Communications Act 2003	
Her Majesty's Government's (HMG's) Minimum Requirements for the Verification of the Identity of Individuals v4 June 2003	
Data Handling Procedures in Government: Final Report June 2008	
UK Payment Services Regulations (2009)	
Banking Code/ Banking Conduct of Business (2009)	

POL00397087

TABLE OF CONTENTS

POL00397087

POL00397087

1. Introduction

EDS is committed to providing a secure operational environment for the delivery and operation of the Post Office Card Account (POca). This environment has been designed to protect the confidentiality, integrity and availability of the information services provided for both the customer - Post Office Limited (POL), and their end users of the service.

Endorsed by the EDS Account Executive and approved by the Account Operations Manager, this document provides an overview of the security policies and procedures adopted by POca in support of these goals.

1.1 Background

The Post Office Card Account service was launched by the UK Government in April 2003. Replacing the current benefit payments system, POca allows customers to withdraw payments made by Government Agencies from Post Office branches using a smart card. EDS has been contracted on behalf of the Post Office, to provide and manage these services.

1.2 Company Security Objectives

Security is critical to protecting POca assets and providing uninterrupted, high-quality service to our client and their end users. The purpose of the POca Security Policy is to ensure the protection and availability of POca resources, including its employees, and the confidentiality and integrity of POca intellectual assets.

The policies and procedures contained within this document have been designed to achieve this objective and to minimise the impact of any identified security incidents upon the operational efficiency and provision of key business services to the customers.

In providing a world-class service for our clients, the policies defined within this document also support the requirements of defined international best practice ISO 27002 - the International Code of Practice for Information Security Management and ISO 27001 the Specification for an Information Security Management System.

Security is a moving target; additional threats and vulnerabilities emerge on a regular basis and must be managed. All policies contained within this document are subject to regular review and proposed changes to any additional policies require full management support.

The POca community must individually and together maintain the appropriate level of information security necessary for the end-to-end POca services.

1.3 Scope of the Security Policy and Principles manual

The provision and management of POca is designed around a leveraged service delivery model. Services required in support of the delivery and management of POca are drawn from a number of service providers both internal and external to the EDS organization.

The Security Policy applies to all activities involved in the delivery and management of the account. This includes the Contact Centres and Live Support activities. This policy will also be adopted by the appointed service providers – both internal and external to EDS - where equivalent policies are not in place. In addition to the Live service it should be noted that the Policy applied equally to the various Test environments used around POca.

EDS organisations/locations bound by this policy:

- Infrastructure Technology Outsourcing (ITO) are responsible for the management and monitoring of the operational environment at a server and network level. They are also responsible for management of the database administration team and for production of the Card Account stationery.
- Business Process Outsourcing (BPO) teams who have responsibility for two areas key to POca service delivery.
    - BPO Telephony team support the Leveraged IP Telephony platform used by the Contact Centres. This team are responsible for the administration, updating and amendment of the systems supporting this service.

POL00397087

  - Content Management System (CMS) support, responsible for the administration, updating and amendment of the CMS application software components.

- Customer Relationship Management System (CRM) support, responsible for the administration, updating and amendment of the CRM application software.

Third Party Service Organisations i.e. JPMorgan, Card Suppliers (TTI and Thames Card Technology), and Cable and Wireless (C&W) are also bound by the terms of this policy. They must:

- Sign into a contractual relationship with EDS and formally agree to adhere to all EDS security controls and applicable legislation where equivalent policies are not in place. This should include information security and non-disclosure agreements or other written confidentiality agreements.
- Protect the information and intellectual assets to which they have access.
- Protect physical assets, systems, and resources.

References to existing policies have been included in this policy where relevant.

POL00397087

2. SECURITY POLICY

The success of POca is dependent upon the implementation of the Corporate Information Security Policy that has been designed to protect the confidentiality (ensuring that information is accessible only to those authorised to have access), integrity (safeguarding the accuracy and completeness of information and processing methods), and availability (ensuring that authorised users have access to information and associated assets when required), of all client information as defined in ISO/IEC 27001:2005.

Based on EDS Corporate Security Policy, POca Information Security Policy has been developed to ensure that the confidentiality of information is assured, and is protected from unauthorised access ensuring that integrity is maintained at all times.
The Corporate Security Policy informs both employees and managers of their responsibilities with regard to Security and directs both at mandatory training material. Any employees who disregard any aspect of the Security Policies will be subject to formal disciplinary proceedings.

In the event of an actual or suspected Security Incident, formal processes have been established to manage and investigate any actual or suspected security incidents ensuring timely resolution and to prevent re-occurrence. In the event of a major disruption to our services, plans have been put in place to minimise the impact that this may have on our client. Compliance with the required regulatory and legislative requirements that are appropriate to our and our partner's business environment have been identified.

The Corporate Information Security Policy is formally reviewed on an annual basis or, as a direct result of any changes to current working practices and the supporting technology infrastructure.

Links: EDS Security Policy
Card Account Security Statement

2.1 Security Organisation

2.1.1 Information security infrastructure and management

Information Security is a business responsibility shared by all members of the management team. On a day-to-day basis the ISM is responsible for the implementation and co-ordination of information security policies, procedures and initiatives within the account. POca senior management will lead by example by ensuring that Information Security is given a high priority in all current and future business activities and initiatives.

The ISM is a role fulfilled by the POca Client Security Officer (CSO) although he may nominate a fully authorised representative. The ISM will regularly attend the management meetings, reporting on any issues relating to the implementation of the security policies, impending changes in legislation, security threats and vulnerabilities and audit activities. The ISM will work with external security groups, professional associations and forums to keep up to date with current developments in security and other related areas.

The ISM has overall responsibility for ensuring that the security of all information assets is managed effectively. All employees are responsible for ensuring information security is not compromised when using the assets. The purchase of, or enhancements to, information processing facilities is controlled through a formal authorisation process. A formal change management process has been implemented to manage any systems upgrades including the installation of new information processing facilities.

Where assistance is required, the ISM will seek specialist advice on specific security issues from within the relevant areas of EDS. Regular liaison with JPMorgan Risk and Compliance team, POL Security Team and EDS Corporate Security will ensure that the project is fully aware of current security issues, new threats and any concerns.

POca is committed to providing regular and relevant Information Security awareness communications to all staff by various means including electronic updates, briefings and newsletters.

To ensure that the corporate information security policy and principles are cost effective, consistent with the business risks and fit for purpose, the implementation of these policies will be independently reviewed on an annual basis.

POL00397087

As described above, all aspects of POca operation are continually assessed from a security perspective. Any areas identified which pose a security risk will be categorised and raised using the established POca Risk Management process with the effective manager of the Risk being the CSO. Information on these risks will be provided to the account leadership team during periodic updates.

2.1.2 Security Risk Management

Inputs to the overall risk management process will be from a compliance analysis of the POca system against the controls established within this document. Both issues and risks will be captured, monitored and controlled by the POca CSO, as part of the Risk Management process, as an overall risk matrix.

All risks will be assessed against the following criteria:

- Nature/Impact of the risk: on a scale of 1 though 5 (where 5 is the greatest impact).
- Likelihood of the risk occurring on a scale of 1 through 5 (where 5 is the greatest likelihood).

The overall risk will be assessed as a combination of impact and likelihood.

All risks will be assigned an owner with the responsibility of:

- Accepting the risk.
- Mitigating against the risk.
- Insuring against the risk.

The choice must be justified to the POca Management team.

Identification, assignment and management of risk will be an ongoing process, with risk assessment being undertaken when changes to the POca system occur. Newly identified risks will be added to the overall risk matrix.

2.1.3 Security of third party access

Minimal third party access to information processing facilities has been identified. Routine maintenance of facilities and systems is undertaken by EDS staff who are aware of the requirements of this Security Policy and are bound by the EDS Security Policy.

The ISM is responsible for ensuring that an appropriate risk analysis has been undertaken when considering the use of third party services and establishing the access levels required. This policy is strongly enforced where there is a business needs to connect to a third party location.

No third parties are allowed access to the organisation or its information until a formal contract has been agreed and signed by both parties addressing security issues to ensure that the confidentiality, integrity and availability of information and EDS' reputation is not compromised. An appropriate summary of POca's Information Security Policy will be formally provided to all contractors, prior to the supply of any services.

2.1.4 Outsourcing

The delivery and management of POca is dependent upon services provided both internally by EDS and also by external partners and other service providers. The key providers are identified below.

- EDS ITO - responsible for the delivery and management of information systems, management of database administrators and the production of POca stationary associated with the account.
- CRM support groups – responsible for updates and changes to the software applications.
- JPMorgan – responsible for the EBT banking system and FSA Regulatory oversight across the POCA estate
- BPO – IP Telephony team
- BPO – POca CMS input capture/scanning team
- TTI Data Systems (TTI) – responsible for Card Production.
- Thames Card Technology (TCT) – responsible for Card Production
- Cable and Wireless (C&W) – responsible for the operation and management of the POca Virtual Private Network (VPN).

POL00397087

Formal contracts have been established between EDS and the relevant service providers. These contracts specify the services to be provided, including service availability, maintenance and security of equipment data back-up, data confidentiality and business continuity planning requirements. In addition to the formal contract, initial on-site security reviews or security questionnaires were completed for each of the external service providers.

The services provided by third party providers will be reviewed on a regular basis. These reviews will include an analysis of performance against agreed service availability and security incidents reported during the review period. In addition to these reviews, independent security reviews may be conducted as specified by the ISM.

For those services provided internally by EDS, the Delivery Framework Agreement details the services that are provided, including required service levels, security controls and escalation procedures.

2.2 Asset classification and control

Records of information assets (hardware, software, and information) owned and managed by POca are recorded by the ISM and where applicable maintained by each individual support group.

The asset list clearly identifies the owner/custodian responsible for ensuring the secure maintenance and use of the asset(s).

All data must be classified in relation to its value, sensitivity or criticality

All information, data and documents are clearly labelled so that all users are aware of the sensitivity of the information, which must at all times remain confidential to POca and EDS.

Information used within EDS falls into one of three classifications as described below:

EDS Internal	Information that comprises mostly EDS business information
EDS Confidential	Information of such sensitivity and/or value that disclosure could result in damage to EDS, or an EDS client
EDS Limited Distribution	Information of such high sensitivity and/or value that disclosure could result in serious damage to EDS or an EDS client

Information used within POca shall be classified making note of guidelines from POL, EDS and other government organisations.

It has been agreed with POL that all POca data carries a classification of “EDS Confidential” and as such requires that all media is labelled accordingly.

All documentation must be classified, labelled and strictly stored by the information owner in accordance with the EDS Information Handling Security Policy as defined above.

Links: EDS Use of Corporate Assets Policy
EDS Information Handling Security Policy
EDS Information Handling Security Requirements
POca Risk Management process

2.3 Personnel security

In order to minimise the risks of security incidents caused as a direct result of human action, error, theft, fraud or misuse of facilities, security is considered at the recruitment stage, included in contracts and monitored during an individual's employment in accordance with EDS Corporate procedures.

Roles and responsibilities for all contact centre personnel including security responsibilities are discussed during induction training. .

All personnel employed by POca have access to information that is vital to the effective operation of the Card Account. To ensure that their positions are not abused, a range of verification checks are completed

POL00397087

whilst recruiting these personnel. These checks include Criminal Records Bureau (CRB) checks, reference checking, confirmation of claimed academic and professional qualifications, identity checks and confirmation of previous employment.

On acceptance of their position within POca, all employees both management and staff, must agree to and sign the terms and conditions of employment prior to commencing employment. This agreement includes statements relating to an employee's legal rights and responsibilities, security responsibilities and an undertaking not to disclose the nature or content of company information to any person or organisation outside of the company.

A formal disciplinary process has been established and will be invoked against any members of staff found to be violating the security policies and procedures and the terms and conditions of employment.

Note: The policies identified above are also extended to temporary staff including contractors and any third parties and visitors to the premises.

Links: EDS Code of Business Conduct

2.3.1 User training

Information Security Awareness training is provided for all employees upon joining EDS POca account, and updated throughout their employment, to ensure that they are educated and updated on the range of information security threats and required safeguards. Where staff change roles, their Information Security needs will be reassessed and any new training identified would be provided as a priority.

The Corporate Security Policy informs both employees and managers of their responsibilities with regard to Security and directs both at mandatory training material. Completion of these training courses is tracked at a corporate level with local management tasked with ensuring compliance is achieved.

The ISM will be expected to maintain and receive periodic training as a priority ensuring awareness of the latest threats to the business and information security techniques.

All staff are expected to remain vigilant for possible fraudulent activity at all times, as complacency could lead to financial loss or damage to EDS/POca. Where a risk assessment has identified an abnormal high level of threat to the operation of the account, employees will be notified on a “need to know” basis and reminded of the specific threats and safeguards to be employed within the bounds of their specific responsibilities.

A summary of POca’s Information Security policies will be provided to all third party contractors and temporary staff for acceptance prior to them commencing work with the company.

The POca Security Policy will be summarised into a number of Powerpoint slides and issued to other EDS groups and external service providers. It is expected that all service providers provide regular security training for their personnel.

2.3.2 Information Security Incident Management

A security incident occurs whenever EDS or customer information or resources are compromised, where there is a risk for compromise of such information, when recurring or successful attempts to obtain unauthorised access to a system are detected or where misuse of the system is suspected.

In the event of an actual or suspected Security Incident, formal processes have been established to manage and investigate any actual or suspected security incidents ensuring timely resolution and to prevent re-occurrence

All EDS personnel are required to report all observed or suspected security incidents, threats weaknesses or malfunctions to the nominated member of staff.

These incidents will be reported via the standard Incident Management reporting tool (Digital Workflow) and assigned to the Security group for POca using processes which are documented in POca Incident Management processes.

POL00397087

These cases will always be raised at Severity 2 and escalated as needed.
.
Security Incidents are classified into the following three categories:

- Severity Level One: disruption of system and business functionality
- Severity Level Two: degradation of services
- Severity Level Three: mitigation of potential disruption or degradation

The ISM will be informed of all incidents that are not reported directly

The type and nature of the security incident will influence the investigation processes as well as the potential corrective actions to be taken. All actual or suspected Incidents are reported to the POca Problem Management team who will provide a central point of contact for managing and handling of incidents. Additionally, an Incident Report will be raised by the person (or delegate) who has responsibility for the functional area where the Incident occurred. This process applies to all participants in the Card Account Live Service, including external suppliers.

Information on any POca Security Incident will be reported to the POca Account Management Team who will instruct teams on the course of action to be taken.

Based on the nature and seriousness of the incident, it may be necessary to notify, Executive Management, Legal Department, and External Customers as appropriate with this decision made by the POca Account Management Team.

The ISM is responsible for ensuring that all instances of security incidents, security weaknesses and security risks caused by software malfunctions are reported and resolved in a timely manner. Trend analysis is undertaken on a regular basis for review and discussion at Management meetings.

Actual or suspected security incidents are reported and dealt with effectively thus ensuring a quick and orderly response. All evidence relating to an actual or suspected security breach is recorded in accordance with EDS Corporate Procedures and copies sent to the POca ISM. Due to the sensitivity around this sort of incident, the amount of detail recorded and the potential audience will vary but it is likely that EDS and potentially Customer groups would be involved.

For a forensic investigation process to be effective it is important that all potentially impacted systems are able to isolate events back to a predefined point in time. This, coupled with the requirement on all systems to provide extensive audit logs will ensure that forensic examination of the POca systems will be able to build a picture of what was happening at the time of the security event.

The ISM will liaise with the incident investigation teams and agree or advise on the corrective actions to be taken where appropriate, thus ensuring a thorough investigation is completed and all evidence is recorded

Links: Computer Incident Response Plan Notification
Escalation Procedures
Incident Management process

2.4 Physical and environmental security

POca data centres and any location hosting other POca infrastructure facilities are protected by at least two layers of physical security:

- An outer *Security Perimeter* that restricts access by the general public.
- An inner *Secure Area* that applies additional restrictions and which must be located within a Security Perimeter.

POca information processing facilities are housed in secure areas, protected by a defined Security Perimeter, with appropriate security barriers and entry controls. They are physically protected from unauthorised access, damage and interference.

POL00397087

All sites used in delivery of the POca solution have security at the core of the physical and logical design. Processes and procedures developed over time ensure that access to both data and infrastructure is on a need to know basis only.

As the scope of the POca solution changes over time the security measures afforded to the project are regularly assessed to ensure they meet or exceed the requirements of EDS Security, the client and our customers.

2.4.1 Security of Operational Environments

2.4.1.1 Contact Centre
The POca contact centre housing the Customer Relationship Management (CRM) is located in Victoria House, a multi-storey office building in Preston.

Access to Victoria House, is through a shared reception area on the ground floor. Access onto the floors occupied by POca, is via a dedicated EDS reception area located on the second floor, which is manned during operational hours. An alarm system and CCTV cameras are installed at each entrance door, access readers requiring proximity cards are installed at the entrance to each floor, the server room, and the training room.

Contact Centre visitors are not allowed access to the premises unless authorised and accompanied by a POca/EDS authorised employee and are made aware of the security and safety requirements of the building prior to entry. Visiting technical staff requiring access to the Server room or other operational floors in order to resolve incidents or to implement changes will have access granted using the established POCA Permit to Work process which is requested as part of the POca Change Management process.

The Permit to Work (PTW) process is based on the process used to control access to EDS Data centres. The EDS process is managed by a dedicated central team and they are responsible for granting access to engineering staff for POCA equipment at sites such as Doxford, Washington and Stockley Park. The POCA variant of this PTW process requires groups to name individuals prior to them attending site. On arrival their identification will be verified using photo-id prior to access to the equipment being granted. Should an engineer attend site without a PTW they will not be allowed access to POCA equipment.

Infrastructure at Preston, supported by EDS ITO, is housed in a secure, dedicated server room , which is compliant with EDS' physical security standards.

2.4.1.2 BPO Scanning
The leveraged scanning centre used for POca is located at Matrix House, Swansea. This centre processes data for multiple EDS clients and internal EDS functions. As with Preston, this building is protected by alarms and CCTV systems coupled with secondary security around the scanning area and Server rooms which are behind access card controlled doors. POca paper records are stored in a separate secure caged area.

2.4.1.3 Data centres
POca utilises EDS data centres in Doxford, Washington and Stockley Park which are managed in line with EDS Security Policies. ITO manage communications infrastructure in two customer datacentres in Belfast which carry the Live Banking traffic between Post Office counters and the EBT banking system. These data centres are owned and managed by Fujitsu services and EDS have assessed the security afforded to the equipment and services at these sites. Additionally, a dedicated server room is in place at the Preston Contact Centre and a DR location in Warrington contains a number of POca servers for use in the event of a Disaster.

2.4.1.4 Outsourced locations
Where services have been outsourced to a third party, the physical access controls in place have been assessed either during an on-site visit or from the information collected in the initial security questionnaires.

Sensitive and confidential data and documentation when not in use, is stored securely thus protecting the information from both unauthorised access and physical damage.

POL00397087

All employees have received the appropriate training and have been issued with guidelines on working in secure areas.

Link: POca Change Management Procedure
EDS Security Policy (Data centre access control)

2.4.2 Equipment security

Important equipment is located in access controlled areas where protection from security threats and environmental hazards is minimised and reduces the threat of unauthorised access. Suitable precautions have been taken to guard against the environmental threats of fire, flood and excessive ambient temperature and humidity. Only suitable and approved cleaning materials are to be used on equipment owned and operated by POca.

Deliberate or accidental damage to property owned, leased or leveraged by POca must be reported to the ISM and a Security Incident report will be raised.

Only authorised personnel are permitted to take equipment belonging to POca off the premises and are responsible for its security at all times.

In line with Corporate EDS policies, all personal computers used on POca have their hard disk encrypted using a FIPS-140 compliant product. In addition to this access to removable media (CD/DVD or USB storage) is controlled .

Data is not routinely stored on portable devices, with key data transferred to the central POca data repository. Information and data stored on portable devices will be backed up regularly so that in the case of a temporary or permanent loss of power or equipment, any data loss is minimised and the device owner is able to quickly continue working. Non-authorised persons must seek permission from the ISM before removing any items.

Authorised personnel only may dispose of equipment or records owned or used by POca according to the media destruction policies. The asset owner must initially authorise the destruction or re-use of information assets ensuring that the relevant security risks have been mitigated. i.e. all information has been securely removed and verified. Where it is not possible to securely erase data from media prior to disposal, such assets will be destroyed.

A clear desk and clear screen policy has been established which ensures that all documentation is placed in a secure environment when the office is unoccupied, to ensure that confidential material cannot be read, damaged or lost by unauthorised parties for example whilst cleaning equipment.

Log-on procedures must be strictly observed and users must first lock access to their workstation or log-off prior to leaving their screen unattended. The standard server and workstation build includes a mandatory timeout after a fixed time period following which the user will have to re-enter their logon credentials to continue. All laptops are also configured to comply with this policy.

Links: EDS clear desk policy

2.5 Computer and network management

2.5.1 Operational procedures and responsibilities

The management and operation of POca is dependent upon the secure and effective operation of the network and operational facilities.

Documented operating procedures have been established for those operational activities directly under the control of the POca Live Support teams

- CRM applications
- CMS applications
- Surveyor application
- Application layer monitoring and alerting

POL00397087

It is the responsibility of the key service providers above to ensure that the relevant documented operating procedures have been established and are adhered to. ITO maintain up to date operating procedures as part of their ISO 9000 Quality Management System requirements.

All changes to the production environment are subject to strict change control requirements and must be reviewed by the ISM and the client where appropriate, prior to release. Changes are fully tested following an industry best-practice delivery life-cycle approach. This sees changes initially deployed on the development network where appropriate. From here they are migrated to System Test and User Acceptance Test (UAT) before finally being implemented on the Live and Disaster Recovery (DR) systems. Implementation plans are developed and strictly followed, and audit logs of all system changes are maintained.

Key duties performed by staff as part of their business as usual (BAU) responsibilities are segregated to reduce the risk of system misuse. Dual control and/or segregation of duties is used to divide responsibility of the completion of a process into separate, accountable actions to safeguard integrity.

2.5.2 System planning and acceptance

In order to reduce the risk of system failures, advance planning and preparation activities are conducted by all groups involved in POca.

Several critical components of the POca service rely on leveraged infrastructure. All changes to this infrastructure are viewed from a collective standpoint ensuring capacity demands due to the introduction of any change do not exceed available system resources

Capacity demands are monitored and projections of future capacity requirements calculated in order to ensure that adequate storage, processing power and network bandwidth is available both in the short, medium and long term.

Prior to upgrades or the installation of new versions of information systems, acceptance criteria are defined, agreed, documented and tested to an acceptable level and signed off and reviewed by the ISM, technical support teams and the customer if appropriate. Allowance for users acceptance testing is included in project plans.

2.5.3 Protection against malicious software

System hardware, operating and application software, the networks and communication systems have been configured to safeguard against both physical attack and unauthorised network intrusion.

2.5.3.1 Server

All POca servers are managed by Hub and regardless of role/environment are supported as if they were Live. Security patches and updates are maintained in accordance with vendor and Corporate direction. Anti-virus software is installed and maintained at the latest version on all servers. Deployment and management of these products is managed by ITO.

2.5.3.2 Personal Computing

Anti-virus and personal firewall software are the standard tools used for laptops and desktops throughout EDS. Deployment and management of these products is managed by internal EDS support groups. Suspected and actual security incidents are reported using the Corporate security reporting procedures.

As detailed in Section 2.5.6, the use of removable media is not permitted on POca PCs unless authorised via the appropriate Waiver process.

The threat posed by the infiltration of a virus and subsequent impact on POca's systems and data is very high. Any permitted removable disks and CD-ROM's are scanned for viruses before being used. All downloaded data shall be scanned for viruses prior to opening. .

Failure to comply with these policies will be treated as a disciplinary matter.

POL00397087

2.5.4 Housekeeping

Backup of POca data files and the availability to recover is a key priority. The ISM is responsible for ensuring that the frequency of such backup operations and the procedures for recovery meet the needs of the business. Processes for information backup have been established which will be undertaken in accordance with the account requirements as detailed in the Delivery Framework agreement and the Service Level Agreement's with external service providers.

Documented procedures have been established within ITO for data backup and restoration, the recording of operational events, and the recording of system errors and the corrective actions implemented. Operator and Security logs detailing tasks and system access are reviewed on a regular basis by each of the service providers. Audit and accounting logs detailing database access and policy rules and error logs will be regularly reviewed. Major security events are reported to the POca ISM and jointly investigated where appropriate. In addition, all system hardware and software faults are reported promptly and recorded. Only qualified and authorised staff or approved third party technicians may repair information system hardware and software faults.

2.5.5 Network management

POca data is segregated from operational data on its own Cable and Wireless (C&W) managed Virtual Private Network (VPN). ITO are responsible for managing and maintaining the POca VPN managed service and preserving its integrity.

An IP Select network has been designed and configured to deliver high performance and reliability that meets the needs of the business ensuring that the confidentiality of all data travelling across the network is protected. 128- bit Triple DES encryption (3DES) is used across all WAN links. This is provided in the Cisco routers. Firewalls will be provided where non-EDS communications enters an EDS site. Security is further enhanced within the network design utilising network tunnels between designated sites ensuring connectivity is provided only to sites which need visibility of each other.

Automated performance testing and monitoring is included within the managed service, geared towards maintaining performance for SLA purposes. Additional monitoring can also be undertaken for the purpose of failure detection and resolution.

All traffic is TCP/IP, although the critical banking transaction traffic conforming to ISO8583 is separated from "raw" TCP/IP traffic by the use of High Priority and Low Priority Virtual Networks within the VPN.

The contact centre LAN is a dedicated 100Mbps switched Ethernet LAN, with Gigabit links between the switches. All servers are provided with dual Ethernet NIC, providing automatic failover in the event of a NIC or line failure.

EDS Operational data is communicated via the EDS internal WAN network and may be used for support links. No POca data traverses this network as part of normal POca functionality.

ISDN links are used as backup links to 3rd Party card suppliers to mitigate against the risk of VPN failure.

2.5.6 Media handling and security

In order to reduce the risk of data loss, EDS has removable media policies at both a Corporate and Government Account level.

The global policy mandates that account leadership must approve every occasion where sensitive data is transferred to removable media such as CD, DVD or USB storage device. Any request to share data or reports via removable media must be submitted to the ISM who will request approval from the POca management team. Only when this approval is granted can the data be copied to the media using the appropriate encrypted media software processes to ensure data is not copied in the clear.

POca is a Government project and due to this has further security controls placed on removable media usage. These include software restrictions on the use of CD/DVD or USB storage media, with these devices disabled on all POca machines. A waiver process initiated via an Operational Change is in place to allow exceptional use of this media but every request requires approval from POca management.

POL00397087

All service providers are required to establish procedures to protect all types of POca media including system documentation from damage, theft and unauthorised access. Procedures in place for CMS and the Contact Centre include instructions on the secure printing and handling of sensitive information, safe and secure disposal of media, and the handling and storage requirements of all POca documentation and data.

2.5.7 Media destruction

Due to the nature of POca data, a policy covering all aspects of media destruction has been developed. Dependant on media type and circumstances it may be necessary to take a more robust approach to identifying, tracking and verifying destruction has completed. As an example, a single failed Storage Area Network (SAN) disk cannot have any data extracted and would be returned to the manufacturer whereas a refresh of an entire SAN device would require that all disk volumes are wiped clean and made secure.

The steps below show the approach adopted by POca to both Business as Usual (BAU) and Project replacements.

2.5.7.1 Server / Storage Infrastructure

All Server and data storage devices are assets owned by EDS. Some of these are dedicated to POca, others are leveraged across multiple projects. Server storage configurations vary between devices and sites and it is not appropriate to detail hardware configuration details within this policy. The risk posed by a particular disk failure is assessed at the time and actions determined according to the scenario.

For large scale refresh or replacement exercises the server disks and other storage devices associated with POca are always securely wiped. This process is managed by ITO and sees an approved company taking the disk(s), as part of a managed change control, and running them through a degausser.

2.5.7.2 PC / Laptop

Personal computers are typically leased from third party suppliers and returned at the end of the Lease period. All disks are routinely encrypted as part of normal operation to mitigate the risk of unauthorised access to data. Prior to the system being returned to the vendor/lease company the disk will be wiped using approved disk cleaning software such as DBAN or BLANCCO in accordance with EDS and POca Security policies

Disks which fail during that period are returned to the vendor but where possible will be wiped beforehand.

2.5.7.3 Removable storage

Common to all EDS accounts, the use of removable storage is discouraged on POca. Where exceptional circumstances dictate that this is necessary and a formal waiver has been obtained, any redundant or obsolete storage media (Optical media, CD/DVD or USB Storage device) is noted in a register, labelled and retained in a locked cupboard. Periodically, these media items are sent from site to a secure disposal company and certification is returned from them for all items securely destroyed.

2.5.7.4 Paper records

POca has a contract in place with a secure paper destruction company. This is managed by BPO on behalf of POca at the Preston and Swansea sites. All paper records are retained in line with business requirements and service levels when they are removed from site in locked containers and sent for secure destruction.

2.5.8 Exchanges of information and software

Upon commencement of their employment with POca, all employees are given access to general word processing e-mail and administration facilities on the network. Policies and guidelines have been issued detailing the appropriate use of word processing facilities

Sensitive and confidential data and information will only be transferred across networks or copied to other media when the confidentiality and integrity of the data can be reasonably assured, for example using encryption techniques, and when approval has been granted where appropriate.

POL00397087

Confidential information must not be transmitted via electronic mail over the Internet without adequate protection. All file attachments must be checked for viruses upon receipt and before sending. Computer files received from unknown senders must be deleted without being opened. Appropriate packaging and trustworthy couriers will be used to ensure the safe movement of any documentation.

Contact centre staff do not typically have access to the Internet, but may access the EDS intranet.

Sensitive or confidential information is not being recorded on answering machines or voice-mail systems. Sensitive or confidential information may only be faxed where more secure methods of transmission are not feasible.

2.5.9 Periodic operational security reviews

In order to validate end to end that security is not being compromised by system or application functionality changes that are introduced over a period of time, it is important that reviews are performed. These reviews involve the ISM and staff from impacted areas with scopes defined nearer the time. They jointly walk through the solution components at a software or hardware level to ensure that all is optimally configured from a security standpoint. Additional lower level checks are included to verify security practices and system health. Areas for consideration include Password policy compliance, vulnerability scanning and application patch update status.

In addition to these “internal” reviews there are periodic reviews by third party organisations (such as EDS partner companies) to check the security and risks around key elements of the POca solution.

Any observations from these reviews are fed back into the POca Risk Management process as documented elsewhere in this document.

Links: EDS UK Electronic Communications Policy
EDS E-mail Etiquette
EDS Use of Corporate Assets Policy
POca Risk Management process

2.6 Access control

2.6.1 Business requirement for access control

Access to information and business processes is controlled on the basis of business and security requirements and is only granted where there is a clearly established business need for access to a particular asset or group of assets. Appropriate authorisation to access or use the assets must have been given by the Asset Owner or ISM.

2.6.2 Access control policy

The adherence to and enforcement of the Information Security Policy is dependent upon the deployment of the formal access control policy. Without this policy, the confidentiality, integrity and availability of all information assets could be severely compromised.

This Access Control policy sets out the standards adopted by POca to ensure that access to information assets is formally controlled in accordance with business requirements. The policy provides the level of confidence required to ensure that access to sensitive and confidential information assets is denied unless formally authorised. .

Based on a genuine business requirement, and in accordance with an individual’s role and responsibilities, the relevant authority, in conjunction with the ISM will review each request for access to the POca network and/or information. The same parties are also responsible for approving, renewing, revoking and amending access rights and privileges to information systems.

User profiles are established and a unique 6 digit ID known as EDS NetID and password combination of 8 characters are issued to all users. Access to all systems will be via individuals assigned EDS NetID. Where this is not possible, an appropriate alternative will be employed. Access to the EDS LAN and systems connected to it is only possible by using EDS assigned NET ID’s.

POL00397087

Individual NetID's will be used to govern the appropriate levels of access available to that individual at both file and application level. Wherever possible, single sign-on is used, so removing the need to enter multiple passwords. However, where this is not possible, multiple entries are made rather than using single scripts to auto-log on.

Under no circumstances will there be a general purpose or shared log-on access to any system. Multiple roles have been established to ensure that one person acting alone cannot circumvent safeguards.

Logon screens and banners that may give away information to unauthorised users are not permitted. Records of current access rights and privileges are maintained.

Access rights of Contact Centre users are recorded in an access control list administered by the Contact Centre Manager.

POca has a defined user audit process which is executed on a 90 day cycle. This process is managed jointly by the Production Support and ITO teams with oversight and agreement of the ISM.

Modifications to user, network, operating systems and application access profiles are formally controlled and managed through change control procedures. All physical and logical access routes to systems and network resources are formally controlled and monitored by the ISM and other members of the change control review board. Required changes to users access profiles are re-approved following any major system changes.

Remote Access to the POca VPN is not permitted other than via the EDS network as if the user was sat in an EDS office. Where first line support is managed remotely, user and node authentication is completed prior to accessing the relevant servers. All privileges are restricted to those essential resources and services required for the users particular role. JPMorgan have remote access to EBT applications, which is in accordance with internal JPM documented control procedures.

The nominated and approved workstations and laptops have been configured to ensure that the POca networks are protected, any tampering of the installed software for remote access, is prohibited.

Implementation of this policy will restrict unauthorised access to both client and internal confidential company information thus protecting the integrity of the data.

In addition to the above controls, all data travelling across the VPN will be encrypted using triple des encryption, preventing the disclosure of unauthorised information should a non-authorised user gain access.

Links: POca Change Control Process
POca 90 day user audit process

2.6.3 User access management

Formal procedures have been established that must be followed at all times to ensure the correct allocation of access rights to information systems and services. These procedures ensure that:

- User access and de-registration rights are formally authorised and controlled for all multi-user information systems and services.
- Allocation of account privileges are strictly controlled and monitored.
- All users receive security awareness training on the need to keep passwords confidential and the use of good security practices in the selection and use of passwords.
- Password changes do not allow the last password to be used, but will allow subsequent incarnations.
- Allocation of temporary passwords is strictly controlled.
- Reviews of user access rights and allocated passwords ensure that tight control is maintained over temporary, regular and special privileges.
- Temporary passwords are changed at first log-on.
- PC's and terminals are secured when not in use either through the use of a secure screensaver, or by formal log-off using the correct process.
- Periodic checks are made to ensure users are not leaving logon details in their work areas.

POL00397087

2.6.4 Network access control

The Network has been designed to ensure only authorized users have access to the required monitoring, application and operating systems.

POca data is segregated from operational data on its own VPN and further segregated from other areas of POca data by using VLANs.

Access to both POca and EDS LAN networked services, business applications and information services is through a formal authorisation process and shall be restricted unless explicitly authorised. Network routing controls based on positive source and destination checking mechanisms; that provide additional protection from unauthorised access are provided through the use of external and internal firewalls.

Where first line support is managed remotely, user and node authentication is completed prior to accessing the relevant servers. JPMorgan have unique remote access to EBT applications. Remote access control procedures provide adequate safeguards through the use of robust identification, authentication and encryption techniques.

2.6.5 Operating system access control

Access to the operating system commands is restricted to persons authorised to perform systems administration or management functions. These controls are implemented through formal procedures, which ensure access rights are formally approved, users can be identified and verified and, all log-on attempts are authenticated and recorded.

Automatic terminal identification and terminal log-on procedures are employed using standard EDS netID and password management system for authorized users. Access to and use of system utilities is tightly controlled. Terminal time out and connection time is configured in line with EDS Corporate guidelines

Link: EDS Security Policy

2.6.6 Application access control

Access to this information and application functions is tightly controlled ensuring that authorised users are granted the correct levels of access according to their user profile Role specific access to applications is restricted to authorized personnel using NetID and passwords.

2.6.7 Monitoring system access and use

Monitoring of server usage is undertaken at an operational level and event logs are automatically raised via the incident reporting system for those servers directly managed or controlled by EDS. It is the responsibility of the third party to ensure that system availability meets or exceeds predefined agreed levels for all other servers.

Where possible, System Monitoring tools are standardized across the various locations. System audit logs are produced and reviewed as part of routine management activities to establish compliance with the access control policy through the number of authorised and unauthorised activities recorded. Unexpected and unusual events are brought to the attention of the ISM, for discussions and the client are informed if considered appropriate.

Where there is sufficient hard evidence of a security breach, legal action will be taken in accordance with the Computer Misuse Act 1990 and disciplinary proceedings will commence. Audit logs recording exceptions and security related events are kept securely in accordance with media handling and security procedures.

2.6.8 Mobile computing

Support activities are generally conducted from EDS secured sites using formal authentication procedures. Additional access via a remotely accessed EDS VPN allowed correctly authenticated EDS staff to gain access to POca. Access via this medium requires additional authentication to access via an EDS secured site.

POL00397087

JPMorgan deliver systems management remotely. JPMorgan support groups access EBT systems at Doxford and Washington via their highly resilient global data network from offices and VPN locations across the UK.

2.7 Systems development and maintenance

2.7.1 Security requirements of systems

The high level security/privacy and access requirements for POca were identified and agreed prior to the development of the solution. These requirements can be found in the Technical Environment Definition, Client Contract and in supporting documentation from the client.

Prior to commencing any systems development work, both the business and security requirements of the service or process are identified. All proposed system enhancements must be business driven and supported by an agreed business case. Overall responsibility for and ownership of any system enhancements and developments must be formally agreed and authorised. This will involve the system owner, ISM, POca Production Support Manager and the Client (POL). This policy ensures that the developed product not only meets the requirements of the user but also provides the required levels of security as identified in the security requirements analysis and specification documentation.

The implementation of any new or upgraded software is carefully planned and managed ensuring that the increased information security risks associated with such projects are mitigated using a combination of procedural and technical control techniques.

2.7.2 Security in application systems

Controls have been designed to protect system information, prevent loss, modification or misuse of user data in application systems. All application software is being provided with an appropriate level of technical support ensuring that any software problems are handled efficiently and resolved within an agreed time.

Validation checks are incorporated into systems to detect corruption of data or any possible fraudulent activity with audit trails and activity logs reviewed when necessary to ensure that any discrepancies are identified and corrective action implemented. Parallel running using normal system testing procedures will incorporate a period of time prior to the new or amended system being accepted into the live environment. The results of parallel running should not reveal problems or difficulties that were not previously identified during user acceptance testing.

2.7.3 Cryptographic controls

Cryptographic systems and techniques are used to protect POca information. Based upon the nature of the business service and the need for information security without compromise, cryptographic techniques have been employed to provide the level of security and confidence levels required from both an internal and external user perspective.

Triple DES (3DES) encryption is provided as part of the POca IP Select VPN. Managed by C&W. IPSEC key changes are automatically updated. Manual key changes to the routers will be undertaken by C&W on annual basis or sooner if the keys are actually or suspected to have been compromised. Any actual or suspected instances of an electronic key being compromised, disclosed, lost or stolen will be reported to the ISM immediately.

The two critical components of the Banking systems are EBT, managed by JPMorgan, and NBX which is managed by Fujitsu Services on behalf of POL. PINs are transmitted between NBX and EBT via an ISO8583 link, one of the POca VPN links, that is 3DES encrypted.

PIN encryption between EBT and the PIN Mailer Fulfilment sites which are EDS Managed will be secured with the introduction of Attalla encryptors at both Fulfilment sites. This ensures that all keys capable of disclosing plain text pins are processed within a hardware security module, evaluated to FIPS140, level 3 or higher.

JPMorgan uses an industry standard method of PIN generation, the IBM 3614 PIN calculation method and all keys are managed in accordance with ANSIx9.24.

POL00397087

To support EMV Compliance for the Card Account a Key Management process has been developed to generate and maintain the EMV-related keys and to ensure that relevant keys are transferred securely from EBT to the Card Suppliers TTi and TCT. A fundamental requirement of an EMV-compliant chip is the generation of Application Cryptograms (ACs) that are verified by the EBT host system to ensure data integrity and protect against skimming of the chip data (i.e. copying of the data onto fraudulent cards). EBT will only ever authenticate ARQCs for the Post Office® Card Account. This necessitates the generation and use of specific 3DES cryptographic keys. Master keys used to generate card-specific keys never exist outside the secure environment of the EBT cryptographic sub-system and are routinely changed on a bi-annual basis to limit the impact of compromise of any master key. At no time will any person, including staff from any domain, be able to gain access to or deduce the clear text of any key being used to secure any aspect of the EMV process.

The detailed specification of the Key Management process can be found in Electronic Benefits Transfer System Key Management For EMV Version 0.1

Links Electronic Benefits Transfer System Key Management For EMV Version 0.1

2.7.4 Security of system files

The integrity of operational software code is protected using a combination of technical access controls, restricted privileges and robust procedures. All IT projects and support activities are conducted in a secure manner. Program listings are controlled and kept fully up to date at all times. Access to server system files is strictly controlled and limited to authorised users.

There is little client-side code specific to the POca solution and what does exist is part of a standard PC build which can be rapidly deployed in the event of corruption of these files. As such there is no need for specific user privileges to be set on this area.

Access and changes to operational software, are controlled by the operations teams using governance procedures detailed earlier in this document. All updates and changes are tested prior to release into the live environment

All system test data and results are stored securely on dedicated Test servers and the environments are suitably configured to ensure that Test data can never pollute the live environment and vice versa. Live data is not used during testing, instead the Test team make use of synthetic data created specifically for this purpose. Transfers of software and data between the development and test environments will be strictly controlled with previous versions of operational code maintained providing contingency.

Program source libraries are held in a secure environment in order to minimise the likelihood of fraud and illegal access and corruption to computer programs and access restricted to authorised personnel.

2.7.5 Security in development and support processes

Project environments are strictly controlled to ensure that the maintenance of application system software and information is undertaken in a secure manner. All proposed system changes are subject to review to ensure that they do not compromise the security of either the system or the operating environment. All development projects are conducted in a controlled secure environment. Project development, test and production systems are maintained in separate environments.

Formal change control procedures detailed earlier have been established ensuring that all changes are conducted in a controlled manner thus minimizing disruption to operational activities. These procedures are used for all changes to systems.

All changes to programs are formally authorised and tested and user acceptance obtained prior to transfer to the production environment. Extensive testing of application systems are reviewed and tested by qualified personnel prior to sign off before being released into the production environment.

POL00397087

All patches and upgrades are verified to come from a reputable source and are thoroughly tested before use. Technical reviews of operating system changes are conducted following any changes to ensure that application systems have not been affected or security compromised in any way.

Emergency amendments to software are discouraged except in exceptional circumstances. Any such amendments must follow incident management and change control procedures. In the event of major issues arising during the upgrade process The backout plan detailed as part of the change implementation plan will be invoked.

2.8 Business Continuity Management

2.8.1 Business continuity and crises management process

Business continuity plans (BCP) have been established to ensure that key business services are not seriously disrupted due to an unexpected occurrence or security incident. Based upon the results of the formal risk assessment, the business continuity plan requirements have been established that cover all essential and critical business activities.

Consisting of a set of documented processes and procedures, the BCP are tested with customer involvement annually. Regular testing ensures that the plans remain up to date, that they are effective in resolving operational activities in a timely and cost-effective manner and, ensure that management and staff know how to execute the plan calmly and effectively. As a result of any tests, the BCP will be updated accordingly. All staff must be aware of the BCP and their own respective roles.

Included within the framework of BCP, crisis management procedures will be established and are tested on a regular basis with POL involvement to ensure end-to-end reaction to operation incidents is acceptable.

Third party service providers are responsible for providing the required levels of Business Continuity as described in the contractual documentation and service level agreements.

2.9 Compliance

2.9.1 Compliance with legal requirements

It is the intention of EDS to avoid breaches of any applicable criminal and civil law, and statutory, regulatory or contractual obligations, and of any security requirements. The laws of the United Kingdom under which services are administered or provided shall govern the enforceability, construction, and interpretation of the Corporate Security Policy and supporting documentation. It is the responsibility of the POca management team to ensure that all employees are fully aware of their legal responsibilities with respect to their use of computer based information systems and data. Such responsibilities will be included within key staff documentation such as Terms and Conditions of Employment and Security Awareness Training.

Relevant Legislation includes:

The Data Protection Act 1998
The Computer Misuse Act 1990
The Copyright, Designs and Patents Act 1988
Money Laundering Regulations 1993

In addition to the above requirements, JPMorgan our banking partner complies with the following legislation in the UK:

Financial Services Markets Act 2000
Data Protection Act 1998
UK Payment Services Regulations (2009)
Banking Code/ Banking Conduct of Business (2009)
Terrorism (united Nations Measures) Order 2001
Afghanistan (United Nations Sanctions) Order 2001

In addition to the above, EDS and their partners, comply with the Post Office Limited Community Information Security Policy.

POL00397087

2.9.2 Intellectual property rights

Guidance will be given to all employees on the key aspects of the Copyright, Designs and Patents Act, Software Copyright and Licensing legislation in terms of its impact on the company's activities. Only fully authorized and licensed software will be used within the business, and documented copies of all license agreements are maintained. Information from the Internet or other electronic sources will not be used or retransmitted without appropriate authorization from the owner of copyright.

All EDS, POca employees and third party contractors will be required to sign a formal undertaking regarding the intellectual property rights of work undertaken during their terms of employment and/or contract respectively. Disciplinary proceedings will be taken against those employees who do not adhere to company policy and infringe end user license agreements.

2.9.3 Safeguarding of organisational records and Fraud Management

EDS recognises the need to protect records and information held within the business from loss, destruction and falsification. Both hard copy and electronic data is retained in an environment that affords it the protection required and in accordance with relevant statutory and legal obligations. Such records will include records of any fraud related incidents, which will be made available to the Post Office if required. Any special storage requirements and data retention procedures will be documented in the respective operational procedures.

Links: EDS Records Retention Policy

2.9.4 Data protection and privacy of personal information

EDS/POca has an obligation to meet the requirements of the Data Protection Act 1998. In this regard, POca is required to respect the privacy of the persons concerned and attach utmost importance and caution to the processing and subsequent storage of personal data.

All EDS staff are required to sign a formal undertaking concerning the need to protect the confidentiality of any information, both during and after contractual relations with EDS. All employee data and client data is treated as EDS Confidential or EDS Limited Distribution and made available to only properly authorised personnel. Employee data will only be released to persons specifically authorised to receive this information.

Links: EDS Code of Practice for Privacy and Data Protection

2.9.5 Prevention of misuse of information processing facilities

Guidelines for all employees to ensure that they are aware of the Computer Misuse Act, 1990 and the impact and responsibilities on their daily activities will be included in Security Awareness Training and enforced in the Terms and Conditions of employment.

Employees may not use EDS/ POca systems to access or download material from the Internet which is inappropriate, offensive, illegal, or which jeopardises security.

Links: EDS Use of Corporate Assets Policy
Protecting EDS Assets
Computer Misuse Act 1990

2.9.6 Regulation of cryptographic controls

Where appropriate, sensitive or confidential information or data is transmitted in encrypted form. Triple DES encryption is employed to protect data travelling across the WAN and VPN. This does not conflict with current legislation in force within the USA and UK on the use of encryption.

2.9.7 Collection of evidence

Evidence relating to Information Security breaches will be collected and forwarded to the ISM. Reports relating to the results of internal audits and security investigations will be retained.

POL00397087

2.9.8 Review of security policy and technical compliance

The ISM is responsible for ensuring and organising reviews of POca Information Security Policies on an annual basis. The objective of these reviews is to establish the degree of compliance to security policies and procedures against working practices, implementing corrective and preventive action where required.

In addition to the above reviews the ISM is responsible for organising independent technical audits and penetration testing of the network and information systems. Technical Audit and Penetration Testing, will be formally controlled and managed through a formal agreement with an independent Information Assurance Testing team or approved third party subcontractor. Such agreements will formally state the scope of the audit and the required access requirements to data.

Managers should regularly review the compliance of information processing within their area of responsibility with the appropriate security policies, standards, and any other security requirements.

If any non-compliance is found as a result of the review, managers must:

a) determine the causes of the non-compliance;
b) evaluate the need for actions to ensure that non-compliance do not recur;
c) determine and implement appropriate corrective action;
d) review the corrective action taken.

Results of reviews and corrective actions carried out by local managers are required to be recorded and these records must be maintained. Managers are required to report the results to the ISM who will in turn inform the group carrying out the independent reviews when the independent review takes place in the area of their responsibility.

The ISM is responsible for ensuring that any identified issues and the associated risks arising as a result of any audit and operational review activities are managed effectively and that all audit activities are managed so as to minimise disruption to operational activities.

Access to any used system audit tools will be protected from misuse and stored in a separate directory.