POL00362828

Cyber Security Guideline

Secure Development Life Cycle (SDLC) Guideline

Version – V2.0

POL00362828

POL00362828

1 Overview

1.1 Introduction by the Guideline Owner

Post Office is committed to protecting its employees, customers, Third Party Supply Chain and information assets from damaging or illegal actions by individuals, either knowingly or unknowingly. Post Office enables this through the development and deployment of policies, standards and guidelines which are aligned to international best practices. Effective cyber and information security is a team effort involving everyone in Post Office.

1.2 Purpose

All development activities performed on behalf of the Post office must be conducted in accordance with a documented system development methodology.

To ensure that software acquired from external suppliers, or Post Office employees provides the required functionality and does not compromise the security of critical or sensitive information and systems.

1.3 Core Principles

To ensure that:

- Systems (including those under development) meet Post Office's business and information security requirements.
- System build activities (including program coding and software package customisation) are carried out in accordance with industry good practice, performed by individuals provided with adequate skills/ tools, and inspected to identify unauthorised modifications or changes.
- Systems under development (including application software packages, system software, hardware, communications and services) are tested in a dedicated testing area that simulates the live environment, before the system is promoted to the live environment.
- Systems under development are subject to security testing, using a range of attack types (including vulnerability assessments, penetration testing and access control testing).
- Rigorous criteria (including security requirements) are met before new systems are promoted into the live environment.
- New systems are installed in the live environment in accordance with a documented installation process, which is subject to proper change control.
- Information security requirements are treated as an integral part of business requirements, fully considered and approved.
- Robust, reliable software is acquired (e.g., purchased or leased) following consideration of security requirements and identification of any security deficiencies.
- Systems are built correctly, able to withstand malicious attacks, and help ensure that no security weaknesses are introduced during the build process.
- Systems function as intended, meet predefined security requirements and do not compromise information security.
- Security weaknesses in systems are identified and tools are used to determine how systems will behave under attack conditions.

POL00362828

- Only security tested and approved versions of systems are promoted into the live environment.
- There is minimal disruption to Post Office when new systems are installed in the live environment.

1.4 Application

All development performed by or on behalf of the Post Office by third parties, or where Post Office is procuring software from a supplier 'off the shelf'.

POL00362828

2 Policy Framework

2.1 Policy Framework

This guideline document is part of the Cyber Security Policy set. These form the baseline to provide Cyber Security and Information Assurance (CSIA) protection for the Post Office.

2.2 Who must comply?

Compliance with the Cyber Security Policy set is mandatory for all Post Office employees and applies wherever in the world Post Offices business is undertaken. All third parties who do business with Post Office, including consultants, suppliers and business and franchise partners, will be required to agree contractually to Post Offices Policies and standards or have their own equivalent policies and standards in place.

POL00362828

3 System Development Methodology

There should be a documented system development methodology (often referred to as the systems development life cycle (SDLC)), which is based upon sound systems development and project management practices

(e.g., Structured Systems Analysis and Design Method (SSADM), Jackson Structured Program (JSP) and SCRUM as part of agile development).

There should be documented standards/procedures for developing business applications (including those under development), which cover:

- training of software developers in secure coding techniques and industry best practise (**which should occur at least annually**)
- specifying requirements
- designing, building and testing applications
- promoting applications into the live environment

The system development methodology should ensure that applications are developed to:

- comply with legal and regulatory (including privacy) requirements
- meet contractual requirements (e.g., those relating to external parties such as customers, clients and suppliers)
- adhere to the Post Office's information security policies, standards and procedures
- meet particular business requirements for security

The system development methodology should require that:

- good information security practices are not sacrificed in the interest of speed of delivery
- initiatives are driven by business requirements (i.e., they are not technology-led)
- dependence on immature technology is minimised
- the security implications of implementing vendor solutions are assessed
- program code is reviewed by an independent party (e.g., an individual that does not work in the same development group, and is highly skilled in the relevant languages and techniques)
- testing is performed in an environment (e.g., a staging environment) which is separate from development and live environments
- the duties of individuals responsible for development, testing and implementation are segregated.

The system development methodology should be kept up-to-date to include new and emerging:

- development techniques (e.g., Rapid Application Development (RAD), agile software development, extreme programming and Joint Application Development (JAD))
- methods of delivering applications (e.g., via cloud services or using mobile technology)
- application architectures (e.g., Web 2.0, Service Oriented Architecture and Web Services)
- security standards and techniques (e.g., Web Services Security, XML firewalls, data loss prevention, intrusion prevention and digital rights management)

POL00362828

The system development methodology should require that, upon starting each new project, initial activities include the:

- notification of the start of the project to the information security function (or equivalent)
- assessment of the need for confidentiality, integrity and availability of information
- clarification of the Post Office's information classification scheme and how it will be applied. (for further reference please review the Post Office's Information Classification Standard)
- creation of a risk register related to the project
- creation of a project management office (PMO) file (or equivalent), which contains all project control-related documentation
- recording of important details about the application in a business application register (or equivalent)

Software developers should be trained in how to apply all aspects of the system development methodology in a secure and effective manner, this training is to be repeated annually.

The system development methodology should be:

- applied in practice
- used by external parties that are employed to develop parts or all of a system for the Post Office (e.g., when using contractors, outsourced software developers or cloud service providers).

Adherence to the system development methodology should be monitored and demonstrated at key stages in the system development life cycle (e.g., during requirements, design, build, testing and deployment)

POL00362828

4 Specifications of Requirements

Business (including information security) requirements for systems under development should be documented in a specification of business requirements (or equivalent) and supported by an agreed process for handling changes to requirements.

Business requirements should cover the need for system:

- performance (e.g., processing speeds and response times)
- capacity (e.g., number of users or volume and size of transactions)
- continuity (e.g., maximum length of time to recover key components following a system failure/outage)
- scalability (e.g., to support future developments or changes)
- connectivity (e.g., interfaces to existing systems, networks or external resources)
- compatibility (e.g., with particular technical environments or components).

Business requirements should:

- define the different types of information that will be handled by the application, such as customer records, personal information and standing data (e.g., pricing details or exchange rates)
- specify the classification of information (e.g., confidential, internal or public).

Business requirements should cover the need for confidentiality, integrity and availability of information throughout its life cycle, including:

- creation (e.g., input validation)
- processing (e.g., integrity checking and performance)
- storage (e.g., location and access control)
- transmission (e.g., source and destination checking)
- destruction (e.g., secure erasure and physical destruction).

Business requirements should take into account:

- contractual, legal and regulatory obligations
- privacy requirements (e.g., the need to protect the confidentiality of customer records or personally identifiable information (PII) such as medical details)
- the Post office's information security policies, standards and procedures
- the provision of arrangements to support systems in the live environment (e.g., the need for a helpdesk or technical support)
- fall-back/contingency plans
- the reduction or elimination of single points of failure.

Business requirements should take into account the need for access:

- by particular types of user (e.g., internal users, IT specialists, technical support staff, suppliers or customers)
- from particular locations (e.g., home offices, external party premises or public places)
- to particular types of information (e.g., credit card details, personally identifiable information or trade secrets).

System requirements should be signed off by the head of systems development (or equivalent).

POL00362828

5 System Design

The system design phase should:

- be based on specified business requirements
- address security requirements, while balancing cost with business needs
- be supported by other relevant information (e.g., the results of risk assessments, security audits or technical security reviews).

The system design phase should involve analysis of the information life cycle in systems under development, including:

- data inputs and connections to systems
- transmission of data between system components
- storage of information, access to databases and other types of storage
- outbound connections to other systems and applications
- inbound connections that provide application data from other systems
- security of information outputs
- secure erasure of information.

The system design phase should involve the integration of a security architecture that can support the technical security requirements, such as performance, capacity, continuity, scalability, connectivity and compatibility.

The system design phase should involve consideration of potential threats (often referred to as 'threat modelling') and review of industry standards to help determine:

- significant threats (including those that are adversarial, accidental or environmental), such as nation states, organised criminal groups, inexperienced developers or poorly informed contractors
- threat events that could compromise the information handled by the application (e.g., software exploitation, malware attack, user error)
- the priority of threat events in terms of the risk they pose.

System design should include analysis of:

- the full range of security controls required to protect information and systems against identified threat events (e.g., policies, methods, procedures, devices or programmed mechanisms)
- specific security controls required by particular business processes supported by systems under development (e.g., encryption of sensitive information, integrity checking and digitally signing information)
- where and how security controls are to be applied (e.g., by integrating with a security architecture and the technical infrastructure)
- how individual security controls (manual and automated) work together to produce an integrated set of controls.

The system design phase should involve consideration of the security implications of how systems will interface with other systems (e.g., running as a standalone application, using two-tier or three-tier architecture, operating in a Web Services or Service Oriented Architecture (SOA) environment, or interacting with cloud services).

The system design phase should involve:

POL00362828

- the use of security architecture principles, including 'secure by design', 'defence in depth', 'secure by default', 'default deny', 'fail secure', 'distrust input from external applications', 'secure in deployment' and 'usability and manageability'
- a review of designs to ensure security controls are specified, and meet security requirements
- documentation of security controls that do not fully meet requirements.

The evaluation of alternative designs for systems under development should take into account the:

- need to integrate with a security architecture
- technical security infrastructure (e.g., Public Key Infrastructure (PKI), Identity and Access Management (IAM), Data Loss Protection (DLP) and Digital Rights Management (DRM))
- capability of the Post Office to develop and support the chosen technology
- cost of meeting security requirements
- skills needed to develop required security controls (e.g., policies, methods, procedures, devices or programmed mechanisms intended to protect the confidentiality, integrity and availability of information)
- costs of deploying security controls.

Before coding or acquisition work begins, system designs should be:

- documented
- verified to ensure that they address security requirements
- reviewed by an information security specialist (e.g., to check that security architecture principles have been applied)
- signed off by the head of systems development (or equivalent) and the business owner of the system under development.

POL00362828

6 Software Acquisition

There should be documented standards/procedures for acquiring software (or systems), which specify:

- guidelines for selecting software (e.g., lists of approved suppliers, security considerations and contractual terms)
- methods of identifying and addressing security weaknesses in software
- a process for reviewing and approving software prior to acquisition
- maintaining a record of software in a register (e.g., in a Configuration Management Database (CMDB) or a corporate asset register, which contains details about both hardware and software
- the need to meet software licensing requirements.

Standards/procedures should apply to all software acquired throughout the Post Office, including:

- operating system and virtualisation software
- enterprise software (e.g., enterprise resource planning (ERP) and customer relationship management (CRM) applications)
- commercial-off-the-shelf software (COTS)
- security software (e.g., Data Loss Prevention (DLP), Digital Rights Management (DRM), Enterprise Mobility Management (EMM) and Intrusion Detection Software (IDS)).

Software should be:

- acquired (e.g., purchased or leased) from approved suppliers (i.e., those with a proven record of providing robust and reliable software)
- tested prior to use (e.g., by performing penetration tests and vulnerability tests) to help identify and resolve security weaknesses
- covered by adequate support and maintenance agreements.

When acquiring software:

- security requirements should be identified
- suppliers should provide assurance that they can meet security requirements (e.g. by producing results of penetration tests, secure code review and vulnerability assessments, demonstrating adherence to standards, and providing an effective method for delivering software patches/fixes)
- a high priority should be placed on reliability in the selection process
- contractual terms should be agreed with suppliers.

The risk of potential security weaknesses in software should be reduced by:

- obtaining and reviewing external assessments from trusted sources (e.g., external auditor's opinions and specified security criteria, such as the Information Technology Security Evaluation Criteria (ITSEC), Common Criteria (CC) and Federal Information Processing Standards (FIPS))
- identifying security deficiencies (e.g., by detailed inspection, malware testing, vulnerability scanning, reference to published sources, or by participating in user/discussion groups)
- addressing any security weakness found

POL00362828

- requiring that the delivery process take security requirements into account so that software cannot be compromised during delivery
- considering alternative methods of providing the required level of security (e.g., an alternative method of authentication or additional application and system monitoring).

Software licensing requirements should be met by obtaining adequate licenses for planned use and by providing proof of ownership of software (e.g., via 'blanket' licence agreements – one licence covering a large number of software deployments).

The acquisition of software should be:

- reviewed by individuals who have the necessary knowledge and skills to determine the extent to which software meets security requirements
- approved by an appropriate business manager
- recorded in one or more registers (e.g., a Configuration Management Database (CMDB) or a corporate asset register that contains details about both hardware and software).

Registers should include important details about software acquired, including:

- a unique description of software in use (e.g., using serial numbers, network address(es) or product numbers)
- versions of hardware and software in use (including patch levels)
- the location where software is installed (e.g., on mobile devices and servers)
- licensing details (e.g., license keys and proof of ownership).

Registers containing details about software should be checked regularly to identify any discrepancy with software licenses. Any unlicensed or unapproved software identified should be investigated and resolved (e.g., by purchasing new licenses, removing unlicensed software or renegotiating contracts).

The accuracy of details about software recorded in the register should be supported by the use of automated discovery/ mapping tools, which are used to:

- identify discrepancies in the register
- discover the introduction of unauthorised software
- detect the illegal use of software (e.g., no license).

POL00362828

7 System Build

There should be documented standards/procedures for building systems (e.g., program coding, web page creation, customisation of software packages and defining data structures), which specify:

- approved methods of building systems (e.g., defining competence levels for staff writing or reviewing code, customising software packages, and documenting changes)
- mechanisms for ensuring systems comply with good practice for system build (e.g., the use of structured programming techniques, methods of secure program coding and documenting code)
- methods of managing the use of code samples (e.g., defining acceptable sources for developers to obtain sample code and requiring a security review of any sample code before it can be used in the system)
- 'secure' methods of making changes to the base code of software packages
- review and sign-off processes (including those for software package customisation).

The build of systems under development should be inspected to identify unauthorised modifications or changes which may compromise security controls.

When building systems:

- staff should comply with good practice for program coding (e.g., using structured programming techniques and documenting code)
- the use of insecure design techniques should be prohibited (e.g., the use of hard coded passwords, unapproved code samples and unauthenticated web services)
- development tools, such as Integrated Development Environments, should be configured to help enforce the creation of secure code
- application source code should be protected from unauthorised access and tampering (e.g., by using configuration management tools, which typically provide features such as access control and version control)
- automated tools should be used to ensure adherence to coding standards.

Where modifications have to be made to the base code of external party software packages a documented customisation process should be applied, which takes into account the risk of:

- suppliers refusing to support or maintain modified software
- built-in security controls being compromised
- incompatibility with updated versions of the base software package.

The customisation process should specify that modifications to the base code of external party software packages can only be made:

- following approval by a systems development manager
- with written permission from the supplier of the software package
- to a clearly identified copy of the original code
- following agreement with the supplier of the software package to change the support arrangements.

System build activities (e.g., program coding and software package customisations) should be reviewed by a systems development manager to ensure that systems function

POL00362828

as intended, and to confirm that security weaknesses (e.g., those related to hardcoded passwords, SQL/LDAP injection attacks, cross-site scripting (XSS), session token attacks and URL forgery) have not been introduced.

System build activities should be signed off by the head of systems development or equivalent.

The Open Web Application Security Project (OWASP) is a cooperative community focused on improving the security of application software. OWASP provides industry accepted practice guidelines for promoting security within web application development. All web application development should include a phase to review against OWASP guidelines to ensure industry accepted security practices are being followed.

The OWASP site can be found here, and it should be checked periodically for updates: https://www.owasp.org

As a guideline, the testing of any web application should include (but not be limited to) checks to ensure that the following vulnerabilities are prevented:

- Injection flaws, particularly SQL injection. Also consider LDAP and Xpath injection flaws as well as other injection flaws.
- Buffer Overflow
- Malicious file execution
- Cross-site scripting (XSS)
- Insecure direct object references
- Cross-site request forgery (CSRF)
- Information leakage and improper error handling
- Broken authentication and session management
- Insecure cryptographic storage
- Insecure communications
- Failure to restrict URL access

POL00362828

8 System Testing

There should be a rigorous process for testing systems under development (system testing), which is supported by documented standards/procedures.

Standards/procedures for testing systems under development should cover the:

- types of hardware, software and services to be tested
- use of test plans, including user involvement
- types of testing (e.g., end-to-end and performance testing, use under normal and exceptional business conditions, error situations and the effectiveness of security controls)
- data used for performing tests
- documentation, review and sign-off of the testing results.

Key components of all new systems should be tested before being installed in the live environment, including application software packages, system software, hardware, communications services and environmental facilities (e.g., air conditioning and backup power supplies).

New systems should be tested in accordance with predefined, documented test plans, which should be cross-referenced to the system design/specification to ensure complete coverage. Key user representatives should be involved in planning tests, providing test data and reviewing test results.

System testing should:

- be performed independently of system development staff
- involve business users
- simulate the live environment
- be supported by documented and approved test plans.

Tests should involve testing the complete system environment (e.g., end-to-end testing or compatibility testing) to identify any conflicts or dependencies with other systems, which includes:

- using the underlying technical security infrastructure (e.g., identity and access management, public key infrastructure, patch management and security event logging)
- interfacing with other applications (e.g., Service Oriented Architecture (SOA) components, Web Services, program calls, hyperlink references and browser software)
- running on different operating systems (including those running on tablets and smartphones) or based on browser software
- interacting with databases and directory services, such as Lightweight Directory Access Protocol (LDAP)
- processing on particular hardware platforms, including servers, desktop computers, mobile devices and specialist equipment
- communicating using different technologies (e.g., IP networks, the Internet, USB, Bluetooth, RFID, mobile applications (apps) and HTML5).

POL00362828

Tests should involve the system running in expected conditions, which include:

- full integration testing, to ensure there will be no adverse effects on individual modules (e.g., Web Services) and existing, related systems
- functional testing (i.e., testing the application functions against the business requirements)
- performance testing when handling planned volumes of working (i.e., load testing with realistic numbers of users/volumes of transactions)
- stress testing/volume testing (i.e., subjecting the system to large volumes of data to assess the performance under abnormal loads) to identify the maximum system capacity.

Tests should cover use under:

- normal (i.e., usual or expected) conditions and special business conditions (e.g., financial year end or national holidays)
- exceptional conditions (e.g., natural disasters, industrial action and denial of service attacks).

Tests should involve infrequent or unexpected conditions, which include:

- installation/uninstallation testing (i.e., of system components and software using different hardware platforms, operating systems and software configurations)
- application failure testing (e.g., to determine what happens if all or part of the system fails and how errors are handled)
- recovery testing (i.e., how well new systems recover from events such as software malfunction and hardware failures)
- testing of manual fall-back arrangements (i.e., revert to previous versions/procedures) or other contingency procedures.

Sensitive business information (e.g., customer data, medical records, product prices or manufacturing details) used for testing purposes should be protected by:

- prohibiting the use of personally identifiable information (i.e., information that can be used to identify an individual person) in the testing process
- using data masking to conceal real information (often referred to as data sanitisation)
- requiring separate authorisation each time business information is copied from the live into the testing environment
- restricting access to business information in the testing environment
- logging the use of business information
- securely destroying copies of business information once testing is complete.

Automated tools should be used to improve the testing process (e.g., to check the validity of system interfaces, simulate loading from multiple clients and test resistance to denial of service attacks).

Test results should be documented, checked against expected results, approved by users and signed off by an appropriate business manager.

POL00362828

9 Security Testing

There should be documented standards/procedures for testing the security of systems under development, which include:

- performing independent checks of the application code
- sign-off of the results of code review by a competent management representative
- determining the effectiveness of security controls
- performing specific attack tests to identify weaknesses in browser-based applications
- using test data for security testing
- resolving flaws and security weaknesses identified during code review and testing.

Prior to security testing, independent checks of the application code should be performed (e.g., code analysis and unit testing) to ensure that:

- code adheres to security policies and standards
- security and design requirements have been met
- vulnerabilities (e.g., 'back doors' or 'time bombs') have been identified and addressed
- programming features have not been used insecurely
- unnecessary sensitive information (e.g., authentication details, comments by developers in HTML or JavaScript and details about the Post Office or our customers) has been removed from the application code.

Checks of the application code should be performed using:

Systems under development should be tested to determine the effectiveness of security controls, including:

- vulnerability assessments (to identify weaknesses in software and security controls)
- penetration testing (e.g., using black-box, white-box or grey-box testing to simulate attacks that demonstrate how vulnerabilities can be exploited)
- authentication and access control testing (e.g., brute force attacks and dictionary attacks on passwords)
- specific attack tests customised for the application (e.g., SQL/LDAP injection, cross-site scripting (XSS), unencrypted cookie transfer, session token attacks and URL forgery)
- browser-based application testing, which includes rigorous review of external content, such as Web 2.0 content provided by external websites (e.g., targeted advertising, digital maps and videos).

Security tests should include the use of:

- transaction data (e.g., sales order, financial payments or foreign exchange deals)
- standing data (e.g., customer master file, pricing tables or stock numbers)
- specifically prepared test data (e.g., large numbers, URLs, command-line inputs and random data) designed to identify system faults or system weaknesses (e.g., buffer overflow and memory corruption).

SD2.6.6

POL00362828

There should be a process for ensuring that flaws or security weaknesses identified during the testing process are resolved in a consistent manner, which includes:

- recording details of security weaknesses identified (e.g., in a test log or on a test results sheet)
- assessing the associated risks
- implementing actions to address these risks
- repeating tests of the application following corrective actions.

POL00362828

10 System Promotion Criteria

Rigorous and documented acceptance criteria should be met before new systems are promoted into the live environment.

Before new systems are promoted into the live environment, reviews should be performed, by implementation staff and business owners, to ensure that:

- security assessments have been carried out
- limitations of security controls have been documented
- approval has been obtained from an appropriate business representative
- service level agreements (SLAs) have been established to support systems in the live environment.

Checks should be carried out to ensure that:

- the application code (or equivalent) has been digitally signed to protect its integrity
- performance and capacity requirements can be met
- all necessary patches and updates have been tested and successfully applied
- all development problems have been resolved successfully
- there will be no adverse effects on existing live systems
- the security of new systems can be supported on a continuing basis (e.g., through a predefined point of contact such as a helpdesk)
- arrangements for fall-back have been established, in the event of new systems failing to function as intended
- sensitive test data (including relevant customer information) has been securely destroyed.

Before new systems are promoted into the live environment:

- error recovery and restart procedures should be established
- contingency plans and arrangements (e.g., as part of business continuity or disaster recovery) should be developed or updated
- operating procedures should be documented and tested
- users should be educated and trained to use systems correctly and securely
- IT staff (e.g., helpdesk staff/system administrators) should be trained in how to run systems correctly and apply required security controls effectively.
- pre-production and/or custom application accounts, user IDs and/or passwords are removed

Arrangements should be in place to ensure that only tested and approved versions of hardware and software are promoted into the live environment.

POL00362828

11 Installation Process

The installation of new systems should be scheduled in advance and approved by an appropriate business manager and the change management board (or equivalent), to avoid disrupting the live environment.

Systems should only be installed in live environments that are:

- supported by robust and reliable technical infrastructure that follows standard security management practices (e.g., system hardening, patch management, malware protection, and access control).
- protected by a minimum set of standard security management practices (e.g., access control, malware protection, patch management, analysis of security-related events and incident management)
- subject to a strict change management process.

The installation of new systems in live environments should be:

- governed by a documented installation process (or deployment plan)
- restricted to a limited number of authorised individuals
- carried out from authorised locations.

The installation process should cover required technical activities, which include:

- integrating with the Post Office's technical security infrastructure (e.g., Public Key Infrastructure (PKI), Identity and Access Management (IAM) and Data Loss Prevention (DLP)
- validating the load or conversion of data
- restricting the installation of new or significantly changed software to executable code.

The installation process should include carrying out sufficient testing to:

- validate system functionality (e.g., users are able to login, all menus are working as expected)
- confirm that the system is operating as expected in the live environment
- verify that security controls are functioning as designed
- ensure that fall-back arrangements will work if needed.

The installation process should cover required user-related activities, which include:

- providing new or revised documentation
- informing the individuals involved of their roles and responsibilities
- making users aware of their responsibilities for using new systems securely
- providing ongoing technical support (e.g., via electronic help screens, a telephone helpdesk or hot-line support)
- implementing new or revised standards/procedures
- handing over responsibility to individuals running the live environment.

SD2.8.7

The installation process should cover required housekeeping activities, which include:

POL00362828

- discontinuing old software, procedures and documentation
- arranging for fall-back in the event of system failure
- recording installation activity, highlighting details about unexpected conditions, ad hoc changes to the system and security issues
- archiving previous versions of software, together with corresponding information (including configuration settings, operations procedures, and supporting software).

POL00362828

12 Post-implementation Review

Post-implementation reviews should be conducted for all new systems.

- Post-implementation reviews should cover:
- fulfilment of business (including information security) requirements
- the efficiency, effectiveness and cost of security controls
- scope for improvement of security controls
- information security incidents that occurred during system development.

Post-implementation reviews should provide assurance that:

- information risks associated with new systems have been identified, assessed and treated (e.g., accepted, avoided, transferred or mitigated)
- selected security controls (to mitigate identified information risks) have been reviewed, built into new systems and operate as expected
- outstanding security issues have been or are being addressed.

Post-implementation reviews should:

- involve the collection and review of performance information (typically using metrics) relating to the development life cycle as a means for measuring and improving the systems development life cycle (SDLC)
- identify successful approaches to information security (e.g., new software development techniques, security protocols or technologies)
- provide recommendations for improving the systems development life cycle (SDLC).

The findings of post-implementation reviews should be:

- signed off by the person in charge of systems under development, an appropriate business representative and an information security specialist
- communicated to individuals involved in the development of new systems, business owners of the new system and executive management
- used to update information security policies, standards and procedures.

POL00362828

13 System Decommission

Systems that are no longer required (sometimes referred to as redundant or obsolete systems), and that may require decommissioning, should be identified.

The risks posed by redundant or obsolete systems that have not been decommissioned should be evaluated, which include those associated with:

- standard security management practices that are no longer applied
- technical vulnerabilities arising (e.g., due to lack of maintenance, updates or patching)
- inadequate protection of sensitive information, resulting in exposure to unauthorised disclosure
- non-compliance with the legal, regulatory or contractual obligations.

Actions to address identified risks should be agreed, which can result in systems being decommissioned.

Where a decision has been taken to decommission a system it should be subject to a documented, approved decommissioning process, which includes:

- identifying the type, classification and location of all information, software, services, devices and equipment associated with the system
- conducting a risk assessment
- migrating, archiving or destroying information (as required)
- uninstalling or removing particular software and services
- securely disposing of devices and equipment.

Different types of information associated with systems being decommissioned (e.g., personal information, customer records and standing data, such as pricing details and exchange rates) should be evaluated to identify their:

- classification (see Classification Standard)
- location (e.g., stored on servers, mobile devices, storage systems, backup devices or archive systems)
- use by other systems or business processes.

An assessment should be conducted of the system being decommissioned (sometimes referred to as a system assessment), which takes account of the potential business impact associated with:

- the type, classification, location and use of associated information
- business processes still supported by the system
- any dependant and supporting systems, services, devices or equipment.

Dependent on the result of the system assessment, relevant information should be:

- migrated to a new or replacement system, as required
- archived in accordance with corporate data retention requirements
- securely destroyed when no longer required.

Dependent on the result of the system assessment, relevant software and services should be:

- subject to termination or amendment of existing contractual arrangements (including software licensing)

POL00362828

- uninstalled, removed or terminated (including in development, testing and live environments).

Dependent on the result of the system assessment, relevant devices and equipment should be:

- sanitised prior to being re-used, sold or returned to leasing company (e.g., by the secure erasure of stored information)
- securely destroyed if no longer required (e.g., via incineration or physically crushing).

A review should be carried out to ensure all aspects of the decommissioning process have been satisfactorily completed.

POL00362828

14 Where to go for help

14.1 Additional Policies

This guideline is one of a set of policies. The full set of policies can be found at:

https://poluk.sharepoint.com/sites/cybersecurity2/SitePages/Cyber-and-Information-Security-Policy-Set.aspx

14.2 How to raise a concern

Any Post Office employee who suspects something is wrong has a duty to:

- Discuss the matter fully with their Line Manager; or,
- Report their suspicions by contacting the Service Desk.

14.3 Who to contact for more information

If you need further information about this standard or wish to report an issue in relation to this standard, please contact Cyber Security Team via GRO

POL00362828

15 Version Control & Approval

15.1 Version Control

Date	Version	Updated by	Change Details
29/01/2020	1.0	IT Security	Changed from Standard to Guideline
12/06/2020	1.0	Cyber Security	Approved by ISC
29/07/2021	1.1	Cyber Compliance	Final draft for approval
02/08/2021	2.0	Cyber Compliance	Approved by ISC

15.2 Standard Approval

Guideline Owner: Chief Information Security Officer
Guideline Author: Hazel Freeman
Approved by Owner: 02/08/2021
Next review: 15/05/2022