POL00337561

IT Policies

IT Change Management

Version – v1.0

POL00337561

Policy Sponsor:	Rob Houghton Group CIO
Policy Owner:	IT Security and Service Director
Policy Author:	IT Change and Release Manager
Approved by:	IT Security and Service Director
Approved:	16-10-2018
Next review:	16-10-2019

POL00337561

POL00337561

1. Overview

1.1. Introduction by the Policy Owner

Post Office's Board and Group Executive (GE) recognise that changes to IT services should be delivered in a controlled manner to reduce potential risk to the business caused by adverse affects. In an ever changing technology landscape, where IT contributes greatly to the success of the business, the risk associated with IT changes must be minimised.

The GE are committed to developing a strategic response to possible risks to enable Post Office to achieve its objectives, whilst preserving the Post Office brand, commercial image, reputation, competitive advantage, revenues, profitability, legal, regulatory and contractual compliance.

Employees have a responsibility to understand the requirements set out in this policy. If there is any misunderstanding, the employee must gain clarification from the IT Service Performance team.

1.2. Purpose

The purpose of this document is to detail the IT controls required to reduce negative exposure to the Post Office brand should any IT service change cause unwanted impact and to ensure that all changes to Post Office Ltd IT services are managed through an established process.

IT Change Management refers to the formal process for making changes to Post Office IT services, within the production environment. It controls the life cycle of all changes, enabling beneficial changes to be made across the internal and supplier-delivered, maintained and supported environments, with minimum disruption to the Post Office, its customers and end users.

1.3. Core Principles

- Coordinate and control all changes to IT services
- Minimise the risk and adverse impact of changes on business operations to levels accepted by the business
- Ensure that changes are recorded, evaluated, authorised, prioritised, planned, tested, implemented, documented and reviewed in a controlled and auditable manner
- Provide staff with a common understanding of change management
- Maintain and enhance shareholder/stakeholder value
- Protect revenue streams and business profitability
- Improve governance
- Compliance with Legal and Regulatory requirements

1.4. Application

This Policy is applicable to all areas within the Group and defines the minimum standards to control financial loss, customer impact, regulatory breaches and reputational damage in line with the Group's Risk Appetite.

POL00337561

In exceptional circumstances, where risk sits outside of the Groups's accepted Risk Appetite a Risk Exception can be granted. For further information in relation to the risk exception process please contact the Risk & Assurance team – georgina.blair@postoffice.co.uk.

1.5. The Risk

Reliability and business continuity are essential for the success of the organisation. Service and infrastructure changes can have a negative impact on the business when risks are not identified and changes not planned correctly.

Change management enables us to add value to the business by:

- Protecting the business and other services while making required changes
- Implementing changes that meet Post Office requirements while optimising costs
- Ensure adherence to governance, legal, contractual and regulatory requirements
- Reducing failed changes, service disruptions, defects and rework
- Improving service availability by improving the speed and success of corrective changes
- Reducing the time and effort needed to manage changes
- Aiding productivity of staff through minimising disruptions due to high levels of unplanned or 'emergency' change and hence maximising service availability
- Reducing the Mean Time to Restore Service (MTRS), via quicker and more successful implementations of corrective changes
- Liaising with the business change process to identify opportunities for business improvement

1.6. Industry Guidance

The change management process is a structured approach to managing changes. In line with ITIL v3.0 (2011) best practice guidelines, the change management process falls within the service transition area of the service lifecycle.

It is the formal process for making changes to Post Office IT services, within the production environment. It controls the life cycle of all changes, enabling beneficial changes to be made across the internal and supplier-delivered, maintained and supported environments, with minimum disruption to the Post Office, its customers and end users.

A change is defined as the addition, modification or removal of any configuration item that could have an effect on IT services.

POL00337561

2. Risk Appetite and Minimum Control Standards

2.1. Risk Appetite

Risk Appetite is the extent to which the Group will accept that a risk might happen in pursuit of day to day businesses transactions. It therefore defines the boundaries of activity and levels of exposure that the Group are willing and able to tolerate.

Please refer to IT Risk appetite.

Post Office acknowledges that in certain scenarios, even after extensive controls have been implemented, a risk may still sit outside the agreed Risk Appetite. In exceptional circumstances a Risk Exemption waiver may be granted.

2.2. Policy Framework

This policy forms part of the IT Policy Set. IT Policies are currently under review.

2.3. Roles and Responsibilities

Effective change management is essential for the success of the organisation and numerous individuals are involved. The roles and responsibilities differ with each change and will depend upon the stage the change is at within its lifecycle.

Change Requestor Receives the request for change from one of the triggers and is responsible for logging the change and representing the change in the CAB. May be from an external supplier and must maintain ownership of the change throughout the lifecycle. The must provide updates on Change outcomes and any relevant information to Change Management as requested.

Change Management Responsible for facilitating the change through its lifecycle. Allocating requests for change to the appropriate change authority and reviewing the results of the change. Change management reports measureable information to service management. Overall responsibility for the change management process belongs to the Change & Release Manager.

Change Advisory Board (CAB) The CAB consists of a group of change requestors, supply chain members, technical advisors, key stakeholders and business representatives from the Post Office. CAB members are called together to review and provide authorisation for normal changes. The CAB will review changes based on risk and impact, make suggestions for improvements, where applicable and authorise/reject changes.

Business Owner Responsible for representing the business interests of a service and providing approval during the CAB. They are often the originator of the change, requesting it on behalf of the business.

2.4. Who must comply?

This policy applies to all Post Office permanent staff and contractors, suppliers, vendors and anyone with access to, or responsibility for Post Office IT services. Anyone involved in activities that cause or require changes to IT Services that affect Post Office must follow this policy.

POL00337561

The scope of change management covers changes made to all Post Office IT services and configuration items within the production environment.

Service requests are an exception to this and fall under the scope of request fulfilment, e.g. Account administration, Password resets, Mailbox management.

The following aspects are also out of the scope of this policy and are managed as part of other processes:

- Contractual or service level changes covered by Service Level/Portfolio Management unless there is an impact on Configuration Items
- The design, development, build, test of Releases covered by the Release Management Process
- Documentation and process changes
- Changes made in development or testing environments
- Services where change process has been arranged independently as part of the Service Design document, e.g internally managed business applications

2.5. Control Standards

The control standards described below are derived from the IT Controls Framework (COBIT 5). The controls are in place to manage the risks within the defined Risk Appetite statements, as contained within the table below. To comply with this, mechanisms are in place within IT to demonstrate compliance.
The table below sets out the relationships between identified risk, and the required minimum control standards.

POL00337561

Risk Area	Description of Risk	Minimum Control Standards	When
Define and communicate Change Management processes aligning to PO Change Management Policy	Absence of well-defined and communicated change management policy and related processes may result in implementation of unauthorised or untested changes to a PO production environment causing adverse impact to PO business operations resulting in financial or reputational loss.	CHM-C1.1 Post Office has a Change Management Policy that clearly defines what constitutes a change, how changes are raised, classified, prioritised, and how these changes should be processed by suppliers. CHM-C1.2 PO ensures that the suppliers' policies and procedures are in line with the PO Change Management Policy. Updates to the PO Change Management Policy and/or procedures are agreed with and communicated to all its suppliers.	Annual
Change Categories, Prioritisation and KPIs are defined.	Absence of clearly defined categories of change, prioritisation and agreed KPIs may result in ambiguity in prioritising/categorising changes leading to delay for high priority changes and inefficient allocation of resources. Ambiguous categories will also restrict the management in reviewing the types of changes being implemented on different systems (functional / bug fixes / upgrades / security etc.) in an extended time period.	CHM-C2.1 PO Change Advisory Board (CAB) is responsible for ensuring changes are evaluated, assessed and reviewed by affected parties/stakeholders and either approved or rejected. Risk and impact assessments should be completed and rationale documented as a part of the Request for Change (RFC) process. All CAB decisions are recorded for audit trail purposes.	Annual

POL00337561

All change requests must be planned, documented, evaluated, assessed and approved.	Failure to plan, document, evaluate, assess and approve change requests may result in undocumented and / or unauthorised changes being implemented in the production environment which may result in incidents leading to unavailability of business critical systems.	CHM-C3.1 An Emergency Change Advisory Board (ECAB) meeting is convened to review and approve any emergency change. CHM-C3.2 Any retrospective change requests must be raised and approved by the PO CAB.	Annual
All changes are scheduled and tested before being applied to live POL production environments (including but not limited to systems, applications and network devices).	Failure to effectively schedule and test changes before applying to live PO production environments may result in incidents and unavailability of PO business critical systems.	CHM-C4.1 The status of all open change requests is tracked and monitored against plan. CHM-C4.2 Monthly reports on change activity include KPIs. Post Implementation Reviews (PIRs) are also presented to PO for review and conformance checks.	Annual
Status of change requests is tracked and monitored and KPIs reported to ensure change requests are implemented and closed on a timely basis, based on priority.	Failure to review and update user change documentation may result in out of date configuration documentation for applications and business processes.	CHM-C4.3 Any decisions and agreements following the monthly supplier performance meetings/fora are recorded formally. It is also ensured that feedback is received in a timely manner from the business.	Monthly

POL00337561

All solution and user documentation is updated as part of change request closure process.	Failure to review and update user change documentation may result in out of date configuration documentation for applications and business processes.	CHM-C5.1 Change tickets are only closed upon successful implementation of a change.	Annual

POL00337561

3. Where to go for help

3.1. Additional Policies

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

https://poluk.sharepoint.com/sites/postoffice/Pages/policies.aspx

3.2. How to raise a concern

Any Post Office employee who suspects that a serious event is taking place is required to:

- Report this to the IT Service Desk

3.3. Who to contact for more information

If you need further information about this policy or wish to report an issue in relation to this policy, please contact IT Security & Service Director.

3.4. How to request an exception

If there is anything within this policy that causes business impact, please contact Head of IT Risk & Compliance who will process the exception. Any exceptions are presented to the Information Security governance body for ratification.

POL00337561

4. Version Control

4.1. Policy Version

Date	Version	Updated by	Change Details
01-05-2018	0.1	Cherise Osei	Draft Version
06-09-2018	0.2	Cherise Osei	Draft Version
13-09-2018	0.3	Cherise Osei	Addition of roles and responsibilities
24-10-2018	1.0	Cherise Osei	Socialised in ITLB 11-10-2018 Approved by Mick Mitchell on behalf of ITLB 16-10-2018