Change Control Policy

Brunel University London

An ISO/IEC 27001:2013: *Aligned Document - Implementing Cyber and Information Security Best Practice*

Internal Use Only

Mick Jenkins
Chief Information Security Officer

Document History

Version	Author	Comments	Date
V 0.1	Andrew Clarke	Initial Draft	17/01/2017
V 0.2	Andrew Clarke	Alignment with Change Control Procedure v02 DRAFT	05/04/2017
V 0.3	Andrew Clarke	Amendments from PWG	25/05/2017
V 1.0	Andrew Clarke	Revised after CISA scope changes - approved	07/07/2017
V 1.2	Andrew Clarke	Revised Customer Services responsibilities	27/07/2017
V 1.2	Andrew Clarke	Annual Review	16/08/2018
V 1.2	Andrew Clarke	Annual Review	28/08/2020

Document Approval

Owner: Michael Jenkins	Chief Information Security Officer
Signature: MGJ	Date: 07 Jul 2017
Approver: Pekka Kahkipuro	Chief Information Officer
Signature: PK	Date: 07 Jul 2017
Distribution:	

This document requires the approval from BUL as defined in the ISMS Compliance document.

Contents

1. About this document

1.1 Purpose of Document

This Policy establishes the area within Brunel University London covering Change Control Management.

Please refer to Brunel University London ISMS Document BUL-GLOS-000 - SyOPs Glossary of Terms for the glossary of terms, acronyms and their definitions for the suite of Brunel University London ISMS documentations.

This process is for IS and University IT Operational change with the CAB aligned to operational matters. For IS strategic change, changes should be submitted to CISA/PMO following the PRINCE2 Project Management IS Project methodology.

1.2 Responsibilities

Table 1 – responsibilities

Title / Role	Description
Change Manager [CAB]	Is responsible for monitoring and managing all changes. Is responsible for CAB, chairing and scheduling. Is responsible for ensuring all parties involved in changes are available
Head of Infrastructure and Operations or delegate of authority [CAB]	Is responsible for overall Change Management on all systems and infrastructure managed by IS and ensure adherence to policy.
IS Systems Manager (Operational Team Manager) or delegate of authority [CAB]	Is responsible for monitoring and managing changes on the IS operational systems. Is responsible for ensuring IS Systems Management Team Change Requests (CRs) are correctly submitted to Remedy and Change Advisory Board (CAB). Is responsible for testing relevant changes on IS systems.
Network Manager (Operational Team Manager) or delegate of authority [CAB]	Is responsible for monitoring and managing changes on the network and network appliances systems. Is responsible for ensuring IS Networks Management Team Change Requests (CRs) are correctly submitted to Remedy and Change Advisory Board (CAB). Is responsible for testing relevant changes.
Head of Development and Application Services (Operational Team Manager) or delegate of authority [CAB]	Is responsible for monitoring and managing changes on server application software. Is responsible for ensuring IS Development and Application Services Management Team Change Requests (CRs) are correctly submitted to Remedy and Change Advisory Board (CAB). Is responsible for testing changes on software and web applications.
Software tester	Is responsible for testing development software items updates and implementations following changes.

Software Owners	Are responsible for tracking all changes for their assets.
Cyber & Information Security Manager CAB]	Is responsible for cyber security risk assessment of changes.
Head of Customer Services [CAB] or delegate	Is responsible for ensuring that Service Desk are informed, have a presence in CAB and all relevant Service Announcements are made and status is updated.
Operational Manager / Team Leader [CAB]	Is responsible for authorisation of Low impact Changes for their respective team
CIO delegate / consultant [CAB]	Is responsible for ensuring the correct ITIL processes are adhered in full, make recommendations and approve changes on behalf of the CIO.
College IT Systems Managers stakeholders [CAB – ex-officio]	Are responsible for monitoring and managing changes on the respective College operational systems and server application software. Are responsible for testing relevant changes on College IT systems.

1.3 ISO 27001 - Conformance

This section indicates the University Conformance to ISO27001:2013.

University ISMS Control Number	SOA – Number A12 – Operations Security
ISO 27001:2013 Conformance Control	Information Classification Objective A.12.1.2 Change Management

1.4 Scope

The scope of this document covers all changes made to:

- All the University's information systems;
- Accessibility to and hosting of Information and data;
- Server Hardware including SAN storage devices, server chassis mounted fibre channel and Ethernet switching, on-board remote management devices and applications, HDD, CPU, Memory that requires an interruption to service delivery;
- Desktop PCs, Workstations and Laptops, (campus wide, changes to vendor/model);
- Firewalls, Encryption Devices, Routers and Secure Access Solutions;
- LAN Switching Equipment;
- Wi-Fi Equipment;
- Server Applications;
- Operating Systems;

- Printers;
- Front end interface changes (GUI);
- Backend changes, e.g. database, backup routine;
- Processes that affect the handling of Informational Assets on authoritative systems (e.g. SITS, HR, PAYROLL);

The following changes are considered routine and are therefore not subject to this Process and are out of scope:

- Anti-virus definition and signature updates;
- Single Client / end user computing application updates;
- WSUS Windows updates – notification required, not approval;
- Backup/restore jobs;
- Development and Test environments – no live environment;
- System Admin with no risk to the Production service; providing this is documented under general housekeeping schedules;
- User Administration (creation, deletion, phone extensions, email accounts, etc.);
- Replacement of PC's/Laptops that have already been accepted into live service;
- Enlivenment of Network Ports;
- The replacement of like for like is undertaken, and that no alteration has occurred in the original design, or feature (patch update) or a work around has been put in place) - Ref Appendix C IS Incident Management;

1.5 References

Brunel University Computer Centre - Remedy Based Change Control Procedure v2.1
BUL-POL-12.6 - Patch Management
BUL-POL-12.5 - Release Management
BUL-POL-12.1.2 - Change Control Policy
UCISA – ITIL Guide to Change Management
BUL-POL-16-1 Infosec Incident Management
BUL-PROC-16-02 Infosec Incident Management Procedure

2.0 Introduction

2.1 Policy Summary

An effective Change Management policy is important to:

- Ensure that standardised methods and procedures are used for efficient and prompt handling of changes;
- Minimise the impact of changes on service quality;
- Improve the day-to-day operations of the organisation;
- Provide an auditable account to satisfy our regulatory and legal obligations;

Changes arise as a result of Problems, but many Changes come from proactively seeking business benefits, like reducing costs or improving services.

A change can be defined as “any modifications to equipment or the configuration of that equipment which may impact upon the confidentiality, integrity and availability of University assets”.

All changes must be submitted using a standard Remedy or the CR form; see BUL-PROC-12.1.2 - Change Control

- Complete the forms (Remedy or if unable to use Remedy, electronic form);
- Operational Manager to log, verify details and approve;
- Pass to the Change Manager to monitoring and manage change;
- Change Manager to pass to the Change Advisory Board (CAB) to consider approval;
- Execute the change only after approval;

Please ensure that any deviations to the Change or execution to the implementation of the change are referred back to the Change Manager, to review any potential impact.

The CAB is made up of the Change Manager, IS Systems Manager, Head of Infrastructure and Operations, Network Manager, Head of Development and Application Services, Cyber & Information Security Manager, Head of Customer Services, CIO delegate / consultant and representatives from relevant stakeholder Operational Business Units and Colleges as required – ex-officio. [Ref. Table 1 – responsibilities].
If an individual cannot attend, a delegate of authority must be authorised to act on their behalf.

Copies of all change requests are retained to provide an audit trail.

Changes initiated by Third Parties must follow the same change management procedure that would apply if those changes were being made by University staff.

2.2 Standard Change Policy

You must raise a Change record for all Production-affecting Changes. There are two processes – STANDARD and EMERGENCY. Do this as soon as you have full, agreed technical details and at give least 72 hours' notice

- Complete the Change Request form;
- Complete all fields where possible; The "sponsor (approved by)" person should be your Operational Manager or Team Leader, WHICH MUST BE DONE BEFORE RAISING THE CHANGE;
- A testing plan, complete with clear acceptance criteria must be documented on the CR prior to commencing the change;
- The individual responsible for testing the change must be identified and fully briefed;
- If necessary, the testing plan can include a dry run of the change in a test environment;
- Operational Manager will review the Change and give approval;
- Submit to Change Manager;
- The Change Manager will seek approval from the Change Advisory Board (CAB). Approval is dependent upon a review from those responsible for carrying out a risk assessment to identify potential risks, their impacts and to identify and cost the required controls in line with the University's risk management framework
- Once approval has been given, The Change Manager will log the change; No change implementation work is done until the change is agreed
- You will be updated by the Change Manager on the progress of your request;
- *ONLY when it's been assigned back to you marked "Implement" may you proceed with the change*
- You must tell the Change Manger when a change has been actioned or if a change did not proceed as planned, as well as the results of any changes;
- Operating procedures and documentation are updated; (an essential part of Change);
- Note that all Changes scheduled before 09:00 on the next working day will be considered "Emergency";

2.3 Emergency Change Process

- Emergency changes must reference a Service Desk IS Incident or Security Incident reference number;
- Remedy must still be completed before a change is carried out and passed to the Change Manager who will liaise with the two ECAB members from the responsibility matrix in 1.2 who cannot be the requester or implementer to assess risk and gain approval,

In the event no agreement can be made, the matter needs to brought to the attention of the Head of Security or the CIO for final approval.

If the emergency change is outside of normal hours, best endeavours must be taken to gain approval from the on call call-out list and a retrospective change processed next business day, and the implementer will be required to attend the daily operations meeting to brief the members.

- Always give closure details (results) if it is a retrospective Change;
- An emergency change is not to be abused, and is for the most serious cases, where you can show/demonstrate to the independent members, that this is required because of an imminent service failure, *and not to be confused with "I just need to do it now",* lack of planning could be shown here;
- The risk matrix will also guide you (2.4.1);
- These changes are subject to review;

Example of an Emergency Change:
The University is receiving a DDOS attack, we need to patch a server or servers/devices, if we don't, we lose services and we are receiving sustained attacks now.
The members should question, can this be undertaken as a high change rather than an emergency, as Emergency Changes will most likely cause an unforeseen outage owing to the unplanned nature of an emergency change but if the change is required immediately, it is essential that if approved, Stakeholders who will be affected and Service Desk are informed.