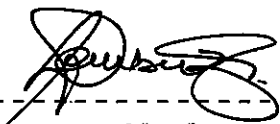


Policy library ID
ICT: 05



IT Change Management Policy

Sponsor division	Operations and ICT Services
Responsible Department	ICT Services
Related WSU policies	
Policy name	Policy Name
IT Service-desk Policy	
Change History	
Approval authority	Council
Approval Date	24 November 2017
Latest revision date	November 2020
Effective date	Immediately
Number of pages	13
 ----- Chairperson of Council	

Contents

1. Preamble.....	3
2. Purpose.....	3
3. Scope.....	3
4. Definitions.....	4 - 5
5. Change Control and Management.....	6
6. General Principles.....	7
7. Appendix.....	8 - 13

1. PREAMBLE

This Policy provides the steps necessary to implement and maintain IT Change Management (ITCM) processes for Walter Sisulu University (WSU), Information and Communication Technology (ICT) Services Department. The document indicates what *change* and *change management (CM)* are, defines the items needed for effective CM, establishes the roles of the people involved, describes the actual steps of the CM process, and specifies how these processes can be accomplished.

2. PURPOSE

The purpose of change management is to minimize the adverse impact of required changes on system integrity, preserve security, honour service level agreements, enable the coordination and planning of changes in order to provide a stable production environment, and to maximize the productivity of people involved in the planning, coordinating, implementation of quality changes and operational continuity.

Changes may be required for many reasons, including, but not limited to:

- a) User requests
- b) Vendor recommended or required changes
- c) Changes in regulations
- d) Hardware or software upgrades
- e) Hardware or software failures
- f) Changes or modifications to the infrastructure
- g) Environmental changes such as electrical, air conditioning and data centre upgrades
- h) Unforeseen events
- i) Periodic maintenance

3. SCOPE

This policy applies to all members of ICT Services staff and authorised vendors for the efficient and effective management of changes to IT systems, applications and services.

4. DEFINITIONS

Any definitions listed below apply to this document only with no implied or intended institution-wide use.

"Change" - The addition, modification or removal of anything that could have an effect on IT systems, applications and/or services.

"Change Request (CR)" – A broadly-defined term that describes the overall process of requesting validation of a change. The CR is composed of different pieces depending on the type of change and the project management documentation method.

"Change Advisory Board (CAB)" - The Change Advisory Board oversees change procedures, validates and approves changes. The CAB is responsible for reviewing the information provided in every change request in order to ensure that the changes are sufficiently researched, documented, planned, and executed.

"Technical Advisory Committee (TAC)" – The Technical Advisory Committee screens the requested change to establish technical viability, competency to effect the change and resource availability. The Technical Advisory Committee consist of the Manager of the unit in which the change is to be effected, Manager(s) of units that will be affected by the change, the Director ICT Services and technical staff of service providers competent in the area of proposed change and with which the university has an existing service level agreement.

"Change Coordinator (CC)" - The Change Coordinator is responsible for initiating the change and managing it through to its completion by researching the need for change, gathering input from the Technical Advisory Committee (TAC), presenting the changes, providing information and getting approval from the Change Advisory Board (CAB), and then executing, evaluating, and documenting the change. The CC also serves in a communications role, and therefore takes on the responsibilities of making sure that users are informed of a change and any potential outage it may cause before the change is made. The CC will in most cases be the manager of the unit in which the change is to be effected.

"Change Management (CM)" - the process of documenting a change, reviewing the potential impact of that change, controlling the timing of the change and, upon completion, verifying the completeness of the change.

"Change Manager (CMGR)" - the Change Manager is a member of the ICT Services staff who is responsible for changes in a particular area of responsibility. Based upon the information provided, the Change Manager should verify that all scheduled changes do not conflict with each other. The Change Manager has the authority to at any time defer any change request that is improperly classified, lacking information or which in any way represents a potential problem that will

affect systems availability or network integrity. The Change Manager's role will in most cases be accomplished by the Business Analyst.

"Change Planning Review Team (CPRT)" - A group that meets to review project planning, evaluate and determine a resolution method for technical conflicts, and identify potential CM pitfalls and risks before they become problems. The CPRT will review projects that the various groups are working on and determine if there are additional steps that need to be taken to ensure that the planned change is handled efficiently and effectively. Problems identified by the CPRT will be escalated to the CAB so that they can be resolved. The CPRT will be made up of the Managers of the five ICT Services units in which changes may be initiated, namely; Development and Standards, User Support, Servers and Storage, Telecommunication and Networks and Internet and Security.

"Emergency Change" - A change to systems that requires circumvention of the specific change management process in order to meet an immediate and critical need. Such a change should still involve as much approval and management as is practical, and in all cases should be recorded appropriately.

"Service Level Agreement (SLA)" - part of a service agreement where the expected level of service is formally defined. The term *SLA* is sometimes used to refer to the contracted delivery time or performance based on the type of problem or change that is encountered.

"Minor Change" - low risk change whose procedures are known and well documented.

"Major Change" - high risk change whose implementation must be planned in advance.

"New Development" - change that is specifically for the deployment of new features, functionality, services or applications.

5. CHANGE CONTROL AND MANAGEMENT

It is the responsibility of ICT Services to manage the life cycle of all information technology systems supporting the university's business objectives. As such, all requirements relating to change control and management are set out in this policy.

There are four types of changes that are permitted. These are:

- a) Minor
- b) Major
- c) Emergency
- d) New development

5.1 Effecting a Change

A change will not be effected without:

- a) A change request being raised via the change management portal.
- b) Approval by the CAB
- c) An approved, documented plan of the sequence or steps for implementing and releasing the change into the production environment
- d) Evidence demonstrating the fact that this change has been successfully implemented in test environment first
- e) Existence of a rollback and mitigation plan in case of failure
- f) A post-change test being documented to check that the change has been successfully applied

5.2 Incidents

Where a change has caused an incident, it will be possible to trace this back to the person responsible for making that change. The Change Manager will facilitate a review meeting of the TAC and a report will be generated and fed back to the CAB.

5.3 Exclusions

The change management policy processes are not meant for users to request IT system changes. Such requests should be channelled through ICT Services End User Support personnel.

6. GENERAL PRINCIPLES

6.1 Risk

By proactively planning and managing changes for the benefit of users, business continuity will be realised. If not properly controlled, changes could be made which will have a negative impact on the university and could prevent staff from fulfilling their roles. Changes could also be made by individuals who are not fully aware of the impact on other business units of the university. The approval process of all change requests includes risk assessment.

6.2 Roles and Responsibilities

The Change Manager ensures that changes follow the Change Management procedure and the CAB will oversee change procedures, validate and approve changes.

All ICT Services staff have a potential role and corresponding responsibility with regards to Change Management with the following specific responsibilities.

- a) Ensure prescribed change management processes and procedures are functional
- b) Submitting change requests through the appropriate systems
- c) Participating in pre-deployment and post deployment testing
- d) Timely sign off for the change
- e) Verifying that change requests are valid

The Office of the Executive Director, Operations and ICT Services is the custodian of this policy and as such has the overall responsibility for this policy and processes contained within it and ensures that this policy is regularly reviewed, relevant and followed by all ICT Services staff.

7 APPENDIX

7.1 Types of Changes

This section defines the different type of changes. Rather than use the ITIL classification of change, we adopt more meaningful titles to the various types of changes:

7.1.1 Minor Change - These are changes that may be done at any time as these have been categorised as low risk to the University and the procedures are known and well documented. Examples of this type of change are:

- a) Application-based security or business needs patches
- b) Regularly scheduled maintenance
- c) Operating system patches

7.1.2 Major Change - These are classified as needing approval and must be planned in advance and submitted for approval from the Change Advisory Board (CAB). The change request should also suggest a time for this change to take place via the change request form before being carried out. The CAB will have ultimate say if the change goes ahead at the suggested time or not. Detailed in the change request should be the documentation about what work is going to happen and the perceived benefit and impact to the users. These types of changes should always have a back out plan or mitigating action plan attached. Examples of this type of change are:

- a) Change that results in an interruption to a service, or has a significant risk of an interruption to service
- b) Change that results in a business or operational practice change
- c) Changes in any system that affect disaster recovery or business continuity
- d) Introduction or discontinuance of a service

7.1.3 Emergency Change - Unscheduled outages, for example server crashes that may require immediate attention whenever they happen. The change request form should still be filled in, but this could be done retrospectively. Examples of this type of change are:

- a) Department or Building is without service
- b) A severe degradation of service requiring immediate action
- c) A system/application/component failure causing a negative impact on business operations
- d) A response to a natural disaster
- e) A response to an emergency business need

7.1.4 New Development - This type of change is specifically for the deployment of new features, functionality, services or applications and is not to fix a problem.

7.2 Submitting a Change Request

7.2.1 Initiate a Request

- a) Complete the change request form - <https://icts.intra.wsu.ac.za/change/>
- b) Enter your username and password. This is to identify who filled in the change request form.
- c) Select the service you are making the change on. If your change affects multiple services then expand as many categories as necessary and select multiple services. You will either find it in the service area category, or start typing its name in the search box and select it.

7.2.2 Select the Type of Change

- a) Fill in the type of change, there are four choices available:
 - i. **Minor** – Select this if your change is a minor fix, well known and documented.
 - ii. **Major** – Select this if your change has business or operational practise shift and has a significant risk of interruption to service
 - iii. **Emergency** – Select this if your change is to fix an immediate problem.
 - iv. **New Development** – Select this if your change adds new functionality or features
- b) Fill in a brief description of the change, avoid technical jargon and try to keep it plain and easy to understand.
- c) Use the pull-down menu to estimate how long the change will take to be made.

7.2.3 Choose Risk Category

- a. Fill in the risk to the service category. There are two options:
 - i. **Minimal** - may be done at any time as the change has little or no risk of going wrong and the procedures are well known and documented.
 - ii. **Significant** - must be planned in advance and need approval. There could be a significant risk to the service.

7.2.4 Choose Date of Change and Submit

- a) Use the pull-down menus to choose the proposed date and time of the requested change.
- b) Submit the change
- c) Change request will be automatically logged within a Change Database. If the change risk category was classified as 'Minimal' then the change can be carried out as specified. If however, the change risk category was classified, as 'Significant' then this change request will automatically generate an email to the Change Advisory Board who will review it. The CAB meets monthly on dates published by the Change Manager. Ensure that submission is made one week prior to a CAB meeting for the request to be considered. Attendance of a CAB meeting in order to provide more information or answer questions about the change request may be required.
- d) If for some reason you need to cancel or reschedule a change or if it does not complete, then you will need to log back into the change form and update the status of the change. The statuses available are:
 - i. Uncompleted
 - ii. Successful
 - iii. Failed
 - iv. Partial
 - v. Cancelled

7.3 Change Procedure

All change requests should be documented and logged. This will be facilitated through the use of the online form. The documentation will be retained centrally within a change request database. For this reason verbal requests and authorisations are not acceptable.

If your change is urgent, then apply the Emergency Changes procedure.

7.4 Emergency Change

In some cases, events are critical enough that they must be rushed through, thereby creating an emergency change. Each situation is different and as much consideration as possible should be given to the consequences of attempting this type of change. It is still necessary to obtain sufficient approval for the change, but this may be in the form of discussing the matter with a relevant manager and logging whom it was discussed with and how it was approved.

7.5 Change Advisory Board (CAB)

The purpose of the Change Advisory Board is to review all change requests and determine whether or not they should be made. In addition, it may determine that certain change requests are amended for them to be accepted. The Change Advisory Board membership is based upon the five different sections of the ICT Services Department plus at least one member of the Operations and ICT Services senior management. For the CAB to be quorate, at least 5 members should be in attendance.

- a. Executive Director: Operations and ICT Services
- b. Director: ICT Services
- c. Deputy Director: Enterprise and Application Services
- d. Deputy Director: Infrastructure Support Services
- e. Manager: Servers and Storage
- f. Manager: Telecommunication and Networks
- g. Manager: Internet and Security
- h. Manager: ERP Systems and Applications
- i. Head: ICT Services (Mthatha, Buffalo City, Butterworth, Queenstown)
- j. Business Analyst

7.6 Emergency Change Advisory Board (ECAB)

Due to the nature of emergency changes, it is not very practical to either wait for a group of advisory board members to gather or to seek approval for a change to be made. This is especially difficult for after office hours incidents that require immediate or quick changes to be made in order to restore a service. In these circumstances, an appropriate manager and member of the senior management has the authority to approve a change. In some exceptional circumstances this may not be possible and the authority will then fall on the person making the change. However, the change request form should still be filled in, even if it is retrospectively.

7.7 Change Freeze Periods

At certain critical times of the year, it will be necessary to impose a non-essential change freeze period. During this time only changes that are deemed essential to either the running of a service or fixing of a problem should be permitted. If there is need to make a change during this time, instructions sent out with the change freeze dates announcements should be followed. If in doubt, contact the Change Manager. The dates of any change freeze will be communicated by the Change Manager well in advance.

7.8 Risk Mitigation, Business Continuity and Change Management

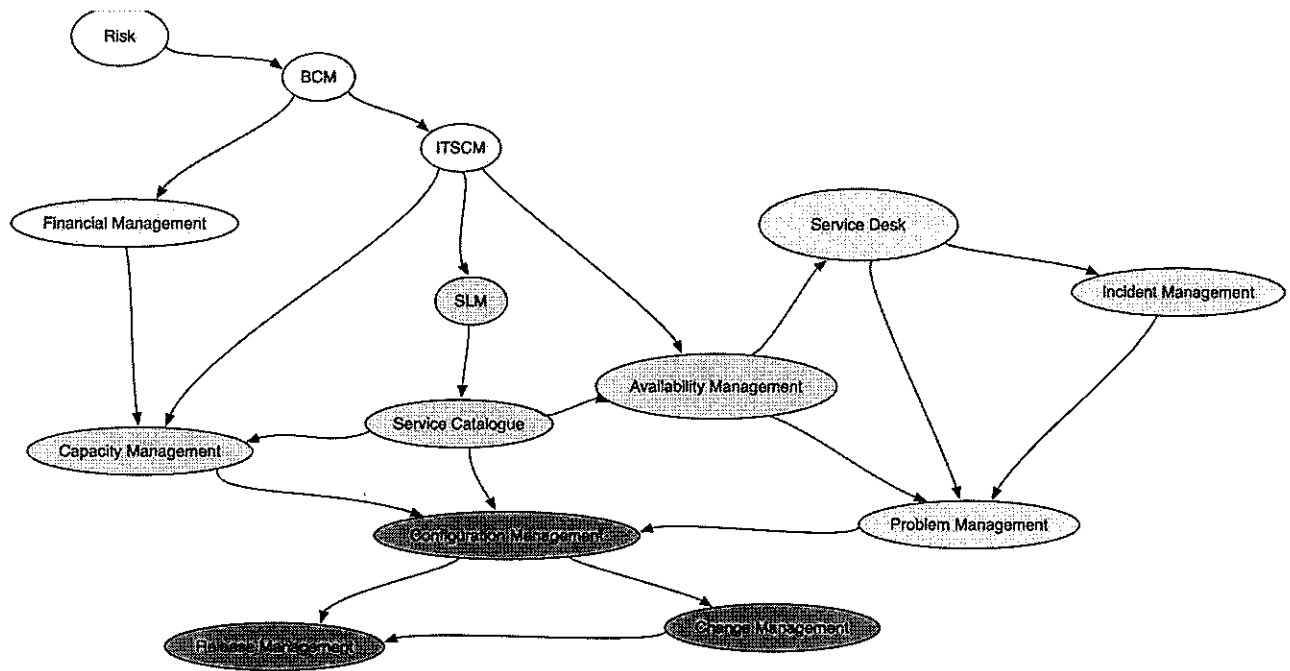
No organisation can have complete control over its business environment. It is therefore essential for companies to have a business continuity management (BCM) and crisis management capability, in case of crisis or disaster. IT Service Continuity Management (ITSCM) aims to manage risks that could seriously impact IT services. ITSCM ensures that the IT service provider can always provide minimum agreed service levels, by reducing risks to acceptable levels and planning for the recovery of IT services.

Service Level Management (SLM) aims to negotiate service level agreements with the customers and to design services in accordance with the agreed service level targets. SLM is also responsible for ensuring that all operational level agreements and underpinning contracts are appropriate, and to monitor and report on service levels. The list of services provided is available from the Service Catalogue.

Configuration Management (CM) is the detailed recording and updating of information that describes an enterprise's hardware and software. Such information typically includes the versions and updates that have been applied to installed software systems and the locations and network addresses of hardware devices. When changes are required, current configurations can be accessed from the configuration database to see what is currently installed. A more informed decision about the pending change can then be made.

Release Management helps coordinate and facilitate the activities necessary to help stakeholders receive and deploy the new solution. This also ensures that quality, security and compliance related aspects are addressed prior to deployment.

The relationship between BCM, ITSCM, SLM, service catalogue, configuration management, change management and release management is depicted by the figure below.



BCM – Business Continuity Management
 ITSCM – IT Service Continuity Management
 SLM – Service Level Management