IT Implementation of Change

Policy

Document Control

Responsibility for Policy:	Chief Information Officer
Approved by and date:	Pro Vice Chancellor (Research) 20th May 2022
Frequency of Review:	Annually
Next Review date:	May 2024
Related Policies:	None
Minor Revisions:	New title for Director of IT Services

1. Introduction

1. 1 Background

Computer and information systems underpin all the University's activities and are pivotal to its research, teaching and administrative functions. The provision of IT services is complex and consist of many different components. As a result of this complexity, it is essential that changes to the infrastructure are carefully managed in order that:-

- services are resilient and reliable
- services are available 24 x 7
- services do not deny access to other users
- the infrastructure is secure from malicious attack from third parties
- University IT resources are used as efficiently and effectively as possible
- all components are legally licensed and deployed
- all components and associated data are adequately backed up and can be recovered in the event of major failure
- all components can be adequately maintained and supported
- all appropriate documentation is up to date

1.2 Purpose

The purpose of this policy is to ensure that any components added, deleted or modified in the production domain comply with the above criteria regardless of who initiates it.

The policy will also apply to test systems if they are either linked to the live environments or they require access external to the University infrastructure.

Changes require planning, monitoring and follow-up evaluation to mitigate adverse impacts to the user communities and to increase the positive impact of the IT services.

The purpose of this policy is not to frustrate change or to question the rationale of proposed changes. It is to ensure that changes have their intended impact while avoiding unintended consequences.

1.3 Who is affected by the policy

Generally, the policy will apply to IT Services staff but will also apply to anyone else who wishes to make changes or add facilities to the live environment.

1.4 Governance of the Policy

This policy will be reviewed on an annual basis to identify any required revisions.

2. Policy / Principles

Prior to the implementation of any proposed changes, the Implementation Checklist (template attached) must be completed. The Checklist will be provided as an On-Line form which can be printed at the end of the process for audit purposes.

This will normally be completed by the relevant staff from within IT Services but may require inputs / documents from other parties.

Once complete, the proposal will be passed to the Chief Information Officer for approval that all the required criteria have been met in an acceptable manner.

3. Exemptions

An emergency change may be required which repairs a current breakage in the live environment or will prevent an imminent failure of a live service.

In such a case, the change can be authorised by the Chief Information Officer without the prior completion of the Implementation Checklist. The Chief Information Officer will subsequently review the change to ensure that the criteria above have been met.

Certain changes occur on a regular basis e.g. updating previously installed software. Once that type of change has been agreed, further instances of implementing the same change can be regarded as “pre-approved”. A list of such “pre-approved” changes will be maintained by IT Services.

4. Unauthorised Changes

Changes which do not comply with this policy will be regarded as unauthorised.

IT Services resources will not be made available for or committed to an unauthorised change.

IT Services reserves the right to reverse any unauthorised changes that cause, are suspected as causing or have the potential to cause disruption to other users / services or represent a risk to the University.