

Change Management Policy

Table of Contents

1. Purpose	3
2. Scope.....	3
3. Policy Statement	4
4. Roles and Responsibilities	4
4.1 Permanent Roles.....	5
4.2 Roles Specific to each Change Request.....	6
4.3 RACI Matrix.....	7
5. Categories of Changes	7
6. Priority Level Definitions.....	8
6.1 Urgency.....	8
6.2 Impact	8
7. Submission	8
7.1 Who Can be a Change Requester?.....	8
7.2 Required Information.....	9
7.3 Single versus Multiple Change Requests	9
8. Approval.....	10
8.1 Normal Changes	10
8.2 Standard Changes	10
8.3 Emergency Changes.....	10
9. Implementation	10
9.1 Normal Changes	11
9.2 Standard Changes	11
9.3 Emergency Changes.....	11
10. Rollback.....	11
11. Post Implementation Review.....	12
12. Cloud Services.....	12
13. Process Improvement	12
14. Policy Review Date	13

1. Purpose

Change management is a critical component to healthy and sustainable IT systems and infrastructure.

The purpose of this policy is to ensure that:

- There is a robust process for requesting, evaluating, testing, and implementing changes to prevent an adverse impact to the existing IT network and systems;
- All changes are subject to approval;
- All changes are assessed based on their urgency, impact, benefit and risk while providing the appropriate stakeholders the authority to approve or decline the request accordingly;
- All changes are logged and captured in a centralised system where the information can be shared, retrieved and reported on;
- There is timely communication of change implementation plans and schedules, availability of appropriate resources and consideration of other changes being deployed.

2. Scope

This policy applies to all non-automated changes to The Open College of the Arts (OCA)'s IT systems and/or infrastructure, including but not limited to:

- The implementation of a new system or service;
- The modification or expansion of the functionality of an existing system or service;
- The removal of an existing system or service;
- The relocation of a system or service resource;
- The addition, modification or removal of a component of system architecture;
- The addition, modification or removal of any system infrastructure component and/or routing configuration of network data traffic.

In most cases, the changes in scope for this policy are changes to be implemented in production environments. The implementation will always involve development and testing in non-production environments, following established practices, before the release into production is authorised – but there is no need for separate change requests to be issued for the implementation on those environments.

It is possible, however, that some changes pertain to non-production environments only, e.g. in the case of structural changes to their infrastructure or in the case of a system or service to be implemented as a 'proof of concept'.

This policy applies to all the OCA staff (including employees, temporary staff, contractors, consultants and partners), and any third parties who help the OCA provide its services.

3. Policy Statement

the OCA's policy in regard to change management is as follows:

- All changes to infrastructure and/or systems require a formal Change Request (CR) and will be subject to a formal change management process, supported by appropriate tools and documentation.
- There shall be a designated Change Advisory Group (CAG) with ultimate responsibility for the evaluation and approval/rejection of changes, based on defined criteria in terms of impact and risk.
- Low risk and low impact changes can be approved by the Change Manager and do not need to be submitted to the CAB.
- Low risk changes that follow an accepted and established procedure or work instruction can be pre-approved by the Change Manager (these are classified as *standard* changes).
- *Emergency* changes (which may be required to quickly restore service or prevent service disruption) follow a less strict process of approval and implementation but are still subject to approval by designated emergency change approvers.
- All approved changes shall be scheduled based on priority, impact and risk assessment, interdependency with other changes and resourcing.
- Information security requirements and impacts shall be documented and assessed for all changes.
- All approved changes shall be subject to technical testing prior to release to ensure they fulfil all the functional and non-functional requirements, including information security requirements.
- The implementation of changes shall be efficient, and risk optimised and follow established delivery gates.
- There shall be the ability to smoothly regress to a previous state in the event of change failure or unanticipated results.
- Disruption of IT services and consequently business disruption shall be minimised.
- There shall be high visibility, accountability and open channels of communication in order to promote smooth transitions when changes take place.
- Lessons shall be learned both from successful and unsuccessful implementation of changes, through a Post Implementation Review (PIR) involving the relevant stakeholders.

4. Roles and Responsibilities

Change management involves both permanent roles and roles specific to each Change Request (CR); both types of roles are described in the subsections below. A RACI matrix for the key roles is also provided.

It should be noted that the role of Change Requester and the Change Implementer can be fulfilled by a single individual, where appropriate, throughout the change management process.

4.1 Permanent Roles

- Change Manager (IT Manager):
 - Ensuring the maintenance, regular review and updating of this policy, and that revisions are communicated as appropriate;
 - Reviewing and where applicable reassigning the category, impact and risk of each CR;
 - Approving or rejecting CRs of low impact and low risk, and establishing the schedule for their implementation if approved;
 - Assessing and pre-approving standard changes;
 - Chairing and coordinating the Change Advisory Board (CAB), preparing and distributing agendas and other relevant information to its members in advance of each CAB meeting;
 - Communicating to change requesters the decisions of approval or rejection of their CRs;
 - Assessing whether a Post Implementation Review (PIR) is required for a change, and preparing and coordinating it where applicable;
 - Reviewing the effectiveness and efficiency of the change management process, identifying and addressing opportunities for improvement.
 - Reviewing the CR for completeness and accuracy, in liaison with the Change Requester;
 - Reviewing the implementation plan for the CR, including a risk assessment, testing plan and rollback plan;
 - Identifying and assigning a change implementer for the CR, once approved;
 - If the CR is rejected, supporting the Change Requester in collecting and preparing additional information required to resubmit it, where applicable;

- Change Advisory Group (CAG) - comprised of the Information Security Group (ISG):

- Evaluating and either approving or rejecting CRs (other than those of low impact and low risk); this shall include the assessment of information security requirements and associated impacts as applicable¹;
- Establishing the schedule for implementation of approved changes, taking into consideration aspects of priority, interdependency, resourcing, etc.;
- Authorising the release of approved changes into production, based on the review of documented outcomes of testing and operational readiness activities;
- Participating in and providing input to PIRs.
- All managers are directly responsible for ensuring this policy is adhered to by their staff.
- All staff shall adhere to this policy.

4.2 Roles Specific to each Change Request

- Change Requester:
 - Providing detailed description of the change and all associated information when submitting the CR, including providing the implementation plan;
 - Doing the initial assignment of the type of change;
 - Knowing what changes, they are authorised to request, and obtaining authorisation to request them when required;
 - If the CR is rejected, obtaining and providing any additional information required to resubmit it, where applicable;
 - Participating in and providing input to a PIR if required.
- Change Implementer:
 - Having overall responsibility for the implementation of the change (once approved), including:
 - Adhering to the implementation plan and schedule;
 - Ensuring that resources are available as required;
 - Coordinating with the relevant teams;
 - Following established procedures of development and testing in appropriate environments;
 - Reviewing the documented outcomes of testing and operational readiness activities for the change;
 - Requesting authorisation from the Change Manager for implementation of the change in production, providing the documented outcomes of testing and operational readiness activities;

¹ Information Security shall have a permanent member in the CAB.

- Implementing the rollback plan for the change if unsuccessful; if the rollback plan itself is not successful, identifying a workaround if feasible, or, if not, raising an IT incident for resolution;
- Participating in and providing input to a PIR if required.

4.3 RACI Matrix

The following RACI matrix summarises the responsibilities of the different key roles involved in the change management process, described in the subsections above.

Activity	Change Requester	CAG/ISG	Change Implementer	Change Manager
Request the change	A, R	I		I, C
Initial evaluation of change	R			A
Provide further info if required	A, R	I		C
Approval – low risk / low impact changes ²	I	I	I	A, R
Approval – other changes	I	R	I	A
Implement the change	I	I	A, R	C
Coordinate testing and operational readiness activities	I	I	A, R	I, C
Request release into production	I	I	A, R	C
Authorise release into production	I	A, R	I	C
Implement rollback	I	I	A, R	C
Conduct PIR if required	C	C	C	A, R

Key: R = responsible, A = accountable, C = consulted, I = informed.

5. Categories of Changes

The category of a change determines the level of rigor required for evaluating, approving and implementing it. All changes will be classified in one of the following categories: **standard**, **emergency** or **normal**. These categories are defined as follows:

- **Standard** changes correspond to specific types of low-risk changes that follow an accepted and established procedure or work instruction and are pre-approved by the Change Manager.

² Including pre-approval of standard changes.

- **Emergency** changes that are required to quickly restore service or prevent service disruption in exceptional circumstances. For this reason, they follow a less strict process of approval and implementation.
- **Normal** changes that are neither standard nor emergency changes. They follow the full process of change approval and implementation.

6. Priority Level Definitions

All CRs will be prioritised based on the **urgency** and **impact** of the change, as well as their relation to other scheduled or pending CRs. Specific circumstances may also affect priority such as disasters, regulatory compliance, etc. Priority is used when two changes are in conflict. The change with the higher priority will always take precedence.

6.1 Urgency

All CRs shall be evaluated by urgency and assigned a level of **critical (1)**, **high (2)**, **medium (3)** or **low (4)**.

Critical is reserved only for genuinely business critical changes where a system is down, or a major operation is impacted.

6.2 Impact

All CRs shall be evaluated by impact and assigned a level of **high (1)**, **medium (2)** or **low (3)** based on aspects including but not limited to the following:

- Number of users impacted;
- Percentage of the network estate affected;
- Criticality of the systems affected;
- Financial impact;
- Impact on customers;
- Risk associated with the change.

7. Submission

7.1 Who Can be a Change Requester?

CRs can be submitted by:

- Authorised members of the IT Department;
- Business owners of systems and services;
- Other OCA employees, within established rules and limits of which types of CRs can be issued/authorised by which roles.

7.2 Required Information

The following information shall be included in or provided with a CR for it to be considered for approval:

- Summary description;
- Business requirements (functional and non-functional), including, where applicable:
 - Information security requirements;
 - Requirements for updating documentation;
- Urgency;
- Impact;
- Risk;
- Implementation Plan, including:
 - Benefits and reason for change;
 - Target deployment date/time;
 - Technical specification;
 - Testing requirements;
 - Communications plan (if relevant);
 - Rollback plan.

The information listed above shall be collected and documented by the Change Requester and reviewed by the Change Manager.

In the case of emergency changes, given their nature, not all the information above is required; but sufficient information shall be provided to justify the emergency of the change.

7.3 Single versus Multiple Change Requests

All changes to the IT network or systems shall be treated independently. Changes shall be exclusive of one another and submitted as individual CRs. An independent assessment of each change is required to understand the actual impact and risk it may have on the environment. Changes that are totally independent or that have varying impacts shall not be combined within one CR.

Separate CRs shall be submitted for each request when any of the below criteria are true:

- Changes are being made by a separate application area or separate technical team;
- Changes are dependent on and/or have varying impacts on multiple environments or systems.

Note: A single CR is required for implementation into relevant Test/Staging and Production environments. The building and testing of changes are included within the one single CR. No separate CR is necessary for those activities. This can also include the moving of code through multiple Test/Staging environments.

8. Approval

8.1 Normal Changes

Normal changes are approved (or rejected) by:

- The Change Manager, in the case of changes of low impact and low risk;
- The CAB/ISG, in all other cases.

The initial assessment of the impact and risk of a change is undertaken by the Change Requester but is subject to revision by the Change Manager.

8.2 Standard Changes

Standard changes correspond to specific types of low-risk changes that follow an accepted and established procedure or work instruction, with documented tasks for completion.

Standard changes are subject to pre-approval by the Change Manager.

A list of all types of (pre-approved) standard changes shall be created, maintained and used for validation of CRs submitted for standard changes, without the need for specific case-by-case approval.

8.3 Emergency Changes

An emergency change occurs when a system or service is not available and must be restored immediately, or a change must be implemented immediately in order to prevent an outage. In the case of an emergency change, approval of the change by a Director level or above shall be granted, by e-mail, prior to implementation. The Change Manager shall be copied on the approval e-mail. The CR for an emergency change shall then be submitted with an urgent priority within one business day of the restoration of service or change implementation. The CR is expected to be completed within one business day of the submitted date.

Note: An emergency change describes a situation that would have required a CR if the change was requested without a service outage having occurred or being at risk of imminent occurrence. The completion of a formal CR is not a prerequisite for solution deployment.

9. Implementation

Version control, configuration baselines and other configuration management techniques shall be applied to all changes involving software (and, where relevant, also to changes that are not software-related).

9.1 Normal Changes

Once a normal change has been approved and the schedule for its implementation has been established, the process of implementation follows established processes and delivery gates.

- The number of applicable delivery gates and sign-off points depends on the scale of the change. Large projects have a higher number of delivery gates and sign-off points. As a minimum, the following delivery gates are applicable to all projects after they have been approved and prior to go live:
 - Design;
 - Build;
 - Test;
 - Operational readiness.
- In all cases, authorisation for release into production is the responsibility of the CAB. This will entail the review of relevant documentation and outcomes of the previous delivery gates.
- The Change Requester shall be informed of the decision to authorise (or not) the release into production.
- Once authorisation is granted, normal changes shall be implemented in production following established procedures. All affected users shall be forewarned of the change timetable and of any possible disruption to normal services. Notifications shall be issued as soon as possible to provide affected users with enough time to make alternative arrangements, if necessary.

9.2 Standard Changes

As standard changes follow established procedures or work instructions and are pre-approved, they do not require any delivery gates / sign-off points for implementation.

9.3 Emergency Changes

By their nature, emergency changes need to be implemented with an urgency that is incompatible with following the established delivery gates and sign-off points. Therefore, they are normally implemented in production with a (very) limited degree of execution and documentation of design, testing and operational readiness activities. Where applicable, documentation shall be retrospectively created or updated following the implementation.

10. Rollback

When a change is unsuccessful, the rollback plan as documented in the CR shall be implemented, under the coordination of the Change Implementer, to regress the affected systems smoothly back to their previous state. In the case of changes to software, and also where otherwise applicable, this shall include reverting to a previous established baseline.

In a circumstance where the rollback plan itself is not successful, the Change Implementer shall:

- Identify and apply a workaround, if feasible;
- If the above is not feasible, raise an IT incident for resolution.

11. Post Implementation Review

After a non-standard change has been implemented, the Change Manager shall assess whether a Post Implementation Review (PIR) is required, depending on the impact of the change and any aspects of its implementation which are deemed relevant for a review.

A PIR can also be (and usually will be) required for an unsuccessful change.

When required, the PIR is prepared and coordinated by the Change Manager, and attended by relevant stakeholders including:

- Change Requester;
- Change Implementer;
- CAB/ISG members.

The PIR is a key mechanism for identifying and discussing lessons learned from change implementation – both successful and unsuccessful – and to introduce improvements in the change management process.

12. Cloud Services

Where the OCA uses cloud services, the contractual agreements between the Cloud Service Providers (CSPs) and the Cloud Service Customers (CSCs) shall:

- Define the responsibilities of both parties for change management, in line with the Shared Security Responsibility Model³;
- Include provisions limiting changes directly impacting CSCs owned environments/tenants to explicitly authorised requests within service level agreements between CSPs and CSCs.

13. Process Improvement

The effectiveness and efficiency of the change management process shall be regularly reviewed by the Change Manager and discussed with the CAB, identifying and addressing opportunities for improvement, based on:

- PIRs and associated lessons learned;
- Metrics and reporting generated by and collected from the tools used to manage the process.

³ See [Cloud Security Policy](#).

14. Policy Review Date

This policy shall be reviewed and appropriately updated on an annual basis. It shall also be reviewed and appropriately updated when there are any changes to relevant regulations on information security and/or data protection.

15. Document Control

Document Control	
Title:	Change Management Policy
Reference:	
Version:	1.0
Date:	
Status:	Draft
Owner:	IT Manager
Classification:	Internal

15.1 Document Revision History

Version	Date	Author	Summary of changes
0.1	26/09/2024	NCC Group	Initial draft
0.2	06/02/2025	NCC Group	Refinements to roles and responsibilities
1.0	05/11/2025	Dean Humphreys	Adjustment of Group Names