Change Freeze Policy v1.0

1.0 Objectives

This policy defines how Information Services will protect IT systems from the risk of downtime during periods that are critical to operations.

Critical periods include examinations and clearing, during which changes to Information Systems will be addressed according to Change Freeze phases: Green, Amber and Red.

1.1 Scope

This policy covers all University IT systems managed by Information Services.

In addition to this policy, an IT Change Management process is always in place (regardless of current Change Freeze Phase) which approves / rejects changes to IT services through a Change Advisory Board (CAB). The CAB assesses the risk of all changes to IT systems, ensuring the changes have had their impact appropriately assessed, are sufficiently tested, and that a rollback plan is in place if applicable. The Change Management process is documented separately in its own policies and procedures.

1.2 Change Freeze Periods

Change Freeze Periods are currently determined using the table below but are subject to change based on the ongoing needs of the organisation.

Period	**Phase**
Semester 1 Assessment and Examinations	Amber
Semester 2 Assessment and Examinations	Amber
Supplementary Examinations	Amber
Senate Exam Boards	Amber
Results Release to Students	Amber
Graduation	Amber
Week before SQA Results	Amber
Thursday before Results Download until Sunday after A-Level Results Day	Red
Week after A-Level Results Day	Amber
Big Welcome Weekend & following week	Amber
Final week before Christmas vacation	Amber
All Other Times	Green

Please refer to the following web page for specific dates for Change Freeze Periods:

https://faqs.aber.ac.uk/9505

2.0 Green Phase

The Green phase is business as usual. Requests for changes SHOULD be submitted via usual channels e.g., the IT Service Desk, or web forms.

3.0 Amber Phase

The Amber Phase is used in the week(s) leading up to critical times in the University calendar. For example, the week before clearing. During this phase, Information Services technical staff MUST cease non-critical work on IT systems. The default stance will be to postpone changes until a return to the Green Phase.

ALL changes MUST be risk-assessed prior to being performed.

Changes with a risk of **HIGH OR ABOVE** MUST NOT be made unless there is a clearly defined business need, and the change is explicitly approved by both the Chief Digital Officer and the asset owner(s) of affected system(s).

Changes made during this phase MUST be performed using the approach detailed in Section 7.0 of this policy.

4.0 Red Phase

This phase is primarily used during the week containing the A-Level Results Day. The default stance will be to postpone changes until a return to the Green Phase.

ALL changes MUST be risk-assessed prior to being performed in accordance with Section 6.0

Changes with a resulting risk of **MEDIUM OR ABOVE** MUST NOT be made without the explicit authorization of the Chief Financial Officer or the Chief Digital Officer, and the asset owner(s) of affected system(s).

Changes made during this phase MUST be performed using the approach detailed in Section 7.0 of this policy.

5.0 Emergency Changes

Information Services may be required to make emergency, unplanned changes to IT systems during Change Freeze periods where failure to act may result in one of the following outcomes:

- Cyber attack
- Large scale data loss or service outage
- Risk to physical safety of people and buildings (e.g., issues with CCTV systems, door access, or building management systems)

BEFORE these changes are made, the approval of a senior member of Information Services technical staff with appropriate knowledge on affected system(s) MUST be sought.

Changes MUST be made in accordance with Sections 6.0 and 7.0 of this policy.

6.0 Risk Assessing Changes

During Amber and Red Change Freezes, ALL changes MUST be risk assessed using the risk matrix below.

Likelihood	Harm severity			
	Minor	Marginal	Critical	Catastrophic
Certain	High	High	Very high	Very high
Likely	Medium	High	High	Very high
Possible	Low	Medium	High	Very high
Unlikely	Low	Medium	Medium	High
Rare	Low	Low	Medium	Medium
Eliminated	Eliminated			

Mitigating controls MUST be identified and recorded for each individual risk. Where risk managers have exhausted all mitigations within their own resources, risks MUST be escalated to an appropriate risk owner with suggested additional mitigation options.

7.0 Executing change during Amber and Red Change Freezes

Once appropriate approval has been sought, any changes made whilst the University is in an Amber or Red Change Freeze MUST follow the following procedure:

- A risk assessment MUST be performed in accordance with Section 6.0 of this policy BEFORE any change is made.

- The two-person rule MUST be followed during all stages of the change. No one individual should act alone without consultation with others. At least one person involved MUST be a senior member of Information Services technical staff with specific knowledge on the affected system(s).

- A document MUST be authored by the member(s) of staff authorizing the change detailing the following information. Once created, this document must be provided to the Chief Digital Officer and the asset owner(s) of affected system(s). These documents will be recorded by Information Services for auditing purposes.

    - Justification for the change to be made.
    - Details of risk assessment performed **before change was made.**
    - Contact information of staff involved in both the decision-making process as well as executing the change itself.
    - Detail of what was changed, when, and which systems were affected.
    - Detail of any adverse impact caused because of the change.

8.0 Definitions

Change	Any alteration to a system, process, data, or configuration which has the possibility to have an adverse impact.
Senior Member of Information Services Technical Staff	An individual who is either a manager, team leader, or equivalent position of seniority within an IS technical team.
Asset Owner	Individual(s) responsible for specific IT systems.