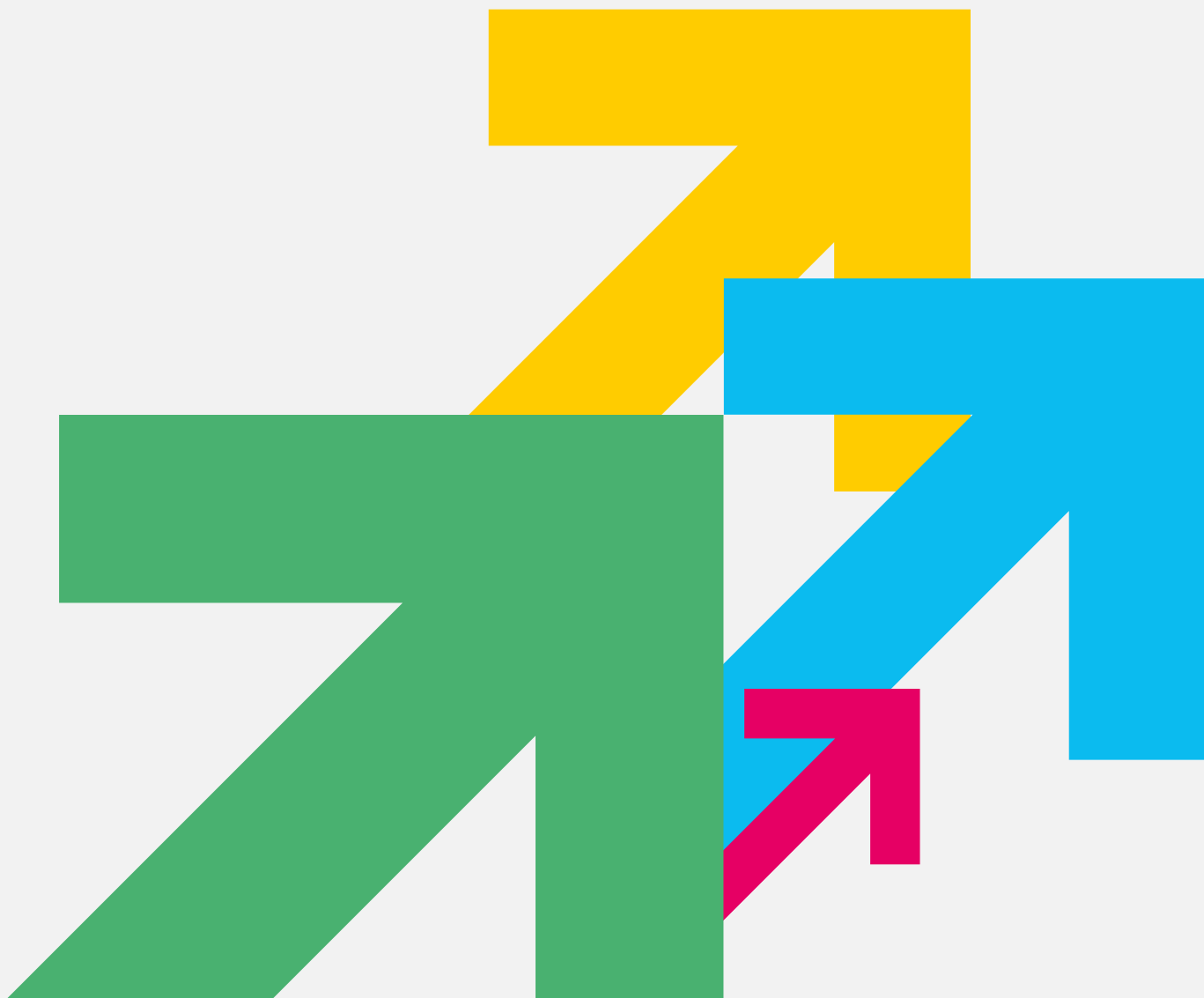


IT Change Management Policy

July 2023

RAD Volo



IT CHANGE MANAGEMENT POLICY

Purpose

IT underpins many of the processes and systems used by the College Group. Change is necessary to maintain and improve the IT facilities offered, to ensure the College Group can carry out its commitments to staff, students and Partners.

IT Services provide a complex and integrated set of services for the College Group. To ensure that maintenance work and improvements are completed with minimal disruption to our users, we manage changes to these systems in a controlled, planned and informed way; considering risks and any potential negative impact to staff and students.

Scope

IT Change Management is a process that makes it easier for STCG to roll out changes to the organisation IT Systems, whether they be hosted On-Site or in the Cloud by a 3rd Party. Change Management helps an organisation to request, prioritise, authorise, approve, schedule and implement IT system changes. This is done so that STCG can control risk and keep disruption to IT Services to a minimum.

The scope of this policy also covers STCG Users/Administrators who have responsibility for the Maintenance and Support of IT Systems that are hosted externally to the College Group, and not looked after by IT Services.

Change Approval process

We follow a standard process to assess, approve and implement changes to services. This ensures:

- Changes are well thought through
- Adequately planned
- Ready for implementation
- Do not conflict with other planned work
- IT Services staff are available to carry out and support the change

Depending on the scale of a change, it will either be classified as Minor or Major change.

The Deputy Director of IT Services can approve Minor changes on a daily basis, as these are low risk and unlikely to have an effect on users even if they fail. Major changes are approved by the Director of IT Services, and are tracked through an email log system, that allows the setting of flags, for monitoring/reporting purposes. In the absence of the Director of IT Services, the Deputy Director of IT Services with the agreement of the Head of IT Operations together can sign off a Major change.

Critical Periods

During critical periods in the academic year, such as Enrolment the impact of an IT change going wrong could cause reputational or financial damage to our College Group.

To protect against this, we reduce the number of changes we make to only Critical (Exception Period), or may even stop implementing changes completely (Change Freeze).

Our IT services continue to be available; however changes to them will not be made unless they are needed in an emergency to keep IT facilities and services running.

We may also implement change freezes when the number of IT staff available are reduced to an unacceptable level e.g. Illness.

Policy Title: IT Change Management Policy		Staff Member Responsible: Director of IT Services
Version: 11	Date EqIA Undertaken: July 2019	Review Date: August 2024

Planned Exception Periods

Changes will be limited during the following dates:

- Mondays till 12pm
- Fridays
- Open Days
- Public Holidays

This is to ensure that these key events run smoothly and are protected from unforeseen issues.

Policy Title: IT Change Management Policy		Staff Member Responsible: Director of IT Services
Version: 11	Date EqIA Undertaken: July 2019	Review Date: August 2024

Planned Change Freezes:

Changes will not be made during the following dates:

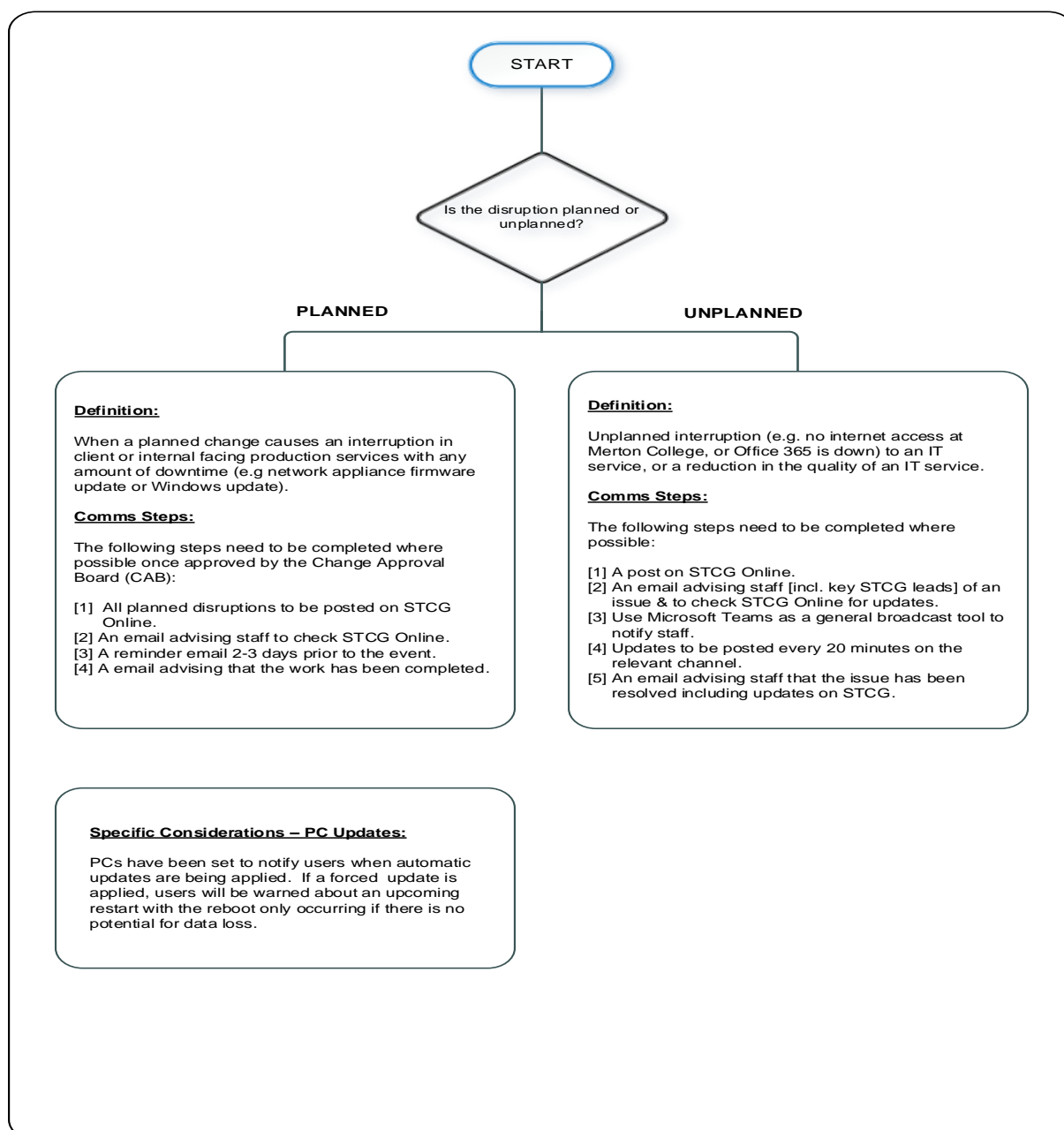
- Main College Enrolment period
- Summer Exam period
- Economic Closures Period e.g. Christmas

Firewall Changes:

All Firewall changes are treated as a 'Major Change' and follow the process described above. In addition, due to the specific function of the College Group Firewalls, flags are set against approved changes in the Email log so that when the rule has reached its expiry date, it is easily identified for prompt removal.

A monthly review of Firewall settings including the applied rules is also carried out by the Deputy Director of IT Services as a secondary check against the Firewall email log.

Change Communication Plan:



Policy Title: IT Change Management Policy		Staff Member Responsible: Director of IT Services
Version: 11	Date EqlA Undertaken: July 2019	Review Date: August 2024