Introduction

The change control process provides a single point of contact for submission of planned changes and a forum for all affected groups to discuss the proposed changes. This provides all involved team members a better outline of the impact on both internal functions as well as external services facing the user community.

Change control is open to all OIT staff and TAG members, and meets each Thursday at 3:00 PM sharp in UTS 623 and SMSU 18N (the rooms are connected via video conference). The change control group discusses outages from the previous week, status of changes from the previous week, and changes for the upcoming week.

Overview of the Change Control Process

The change control process begins with the submission of a ticket to the change-control RT queue. This ticket contains a number of required fields that are designed to give others a good sense of what the change is and what the effects will be.

Every Wednesday at 3:00 PM an email is sent out to change-control@lists.pdx.edu containing a summary of all tickets in the change-control RT queue with a start date after the upcoming change control meeting on Thursday at 3:00 PM, and before the change control meeting the following week.

The weekly change control meeting begins with a discussion of "what broke" over the last week. Next, the changes from the previous week are discussed. Was the change successful, partly successful, didn't happen, etc. Finally, the changes planned for the upcoming week are discussed. Consensus is built around if and when changes should be allowed to move forward.

What Changes Should be Submitted for Change Control Review?

This can be a somewhat subjective decision, but here are several questions to help decide if a particular change should be submitted to Change Control:

- Will this change cause a service outage?
- Will this change modify the expected behavior of a production system?
- Do you have any doubt that the change will not go as planned?

If you answered "yes" to any of those questions then the change should be submitted to Change Control.

Creating a New Change Control Ticket

If you are ready to create a new change control ticket click here:

https://support.oit.pdx.edu/Ticket/Create.html?Queue=20

Be sure to click on the "Show details" link in the upper right of the screen to set a start date (if you don’t do this then it will not show up in the change control email). You will need an RT account to create a change control ticket. If you don’t have an RT account you can request one here.

Submission Deadlines

Change control RT tickets must be submitted by 3:00 PM each Wednesday to be considered in the following day’s change control meeting.
Change Control

Depending on the Risk and Impact of each change request, advanced notice must be given. The table below specifies the advanced notice required for each change request, with day 0 being the first change control meeting where the change has been discussed. A description of risk and impact levels is provided in Appendix B at the end of this document.

<table>
<thead>
<tr>
<th></th>
<th>No Risk</th>
<th>Low Risk</th>
<th>Medium Risk</th>
<th>High Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low Impact</td>
<td>Immediately</td>
<td>Immediately</td>
<td>1 Day</td>
<td>1 Day</td>
</tr>
<tr>
<td>Medium Impact</td>
<td>Immediately</td>
<td>1 Day</td>
<td>7 Days</td>
<td>7 Days</td>
</tr>
<tr>
<td>High Impact</td>
<td>1 Day</td>
<td>1 Day</td>
<td>7 Days</td>
<td>14 Days</td>
</tr>
</tbody>
</table>

Approval of Changes

In general, proposed changes are approved by gaining consensus from those present at the weekly Change Control meeting. If consensus cannot be reached then a vote will take place with 75% approval required to move forward with the change. Each OIT team and each department represented by a TAG member gets one vote.

Denial of Changes

At the discretion of the Change Control host, a change may be denied if the Change Control RT ticket is not fully complete or if there is no one present with sufficient knowledge to discuss the proposed change. Changes that have been denied by the Change Control host can be appealed to the OIT Director for the affected department.

Emergency Changes

There will inevitably be cases where a change must be made outside of the Change Control process due to the importance and time sensitive nature of the change. Such changes must be approved by a Director level manager. A detailed description of the change (matching the formatting of changes sent out in the weekly change control email) as well as a justification for the emergency change should be sent to OIT-ChangeControl-Group@pdx.edu.

Change Control Participants

The following OIT teams are participants of the change control process:

- CIS: Client Systems Administration
- CIS: Infrastructure and Operations Team
- CIS: UNIX Team
- CIS: Windows Server Team
- CIS: Database and Application Platform Team
- NTS: Network Team
- USS: Helpdesk

Each team listed above is required to submit their changes through the Change Control process as well as send a representative to the Change Control meeting each week.
Change Control

Moratorium Dates
During certain times of the year a moratorium is enacted to minimize potential impact on our customers. This typically includes the beginning and end of most terms as well as several days in summer when the business office is closing the fiscal year. Below are the standard moratorium dates for the beginning and ending of terms:

Fall Quarter
- One week prior to the start of term beginning at 12:01am on Monday through the first Friday evening of the term (7:59pm).
- During finals week, Monday @ 12:01am through Wednesday @ noon the week following finals.

Winter Quarter
- The first week of the term, Monday @ 12:01am through Friday @ 7:59pm.
- During finals week, Monday @ 12:01am through Wednesday @ noon the week following finals.

Spring Quarter
- The first week of the term, Monday @ 12:01am through Friday @ 7:59pm.
- During finals week, Monday @ 12:01am through Wednesday @ noon the week following finals.

Summer Quarter
- The first week of the term, Monday @ 12:01am through Friday @ 7:59pm.

Weekly Maintenance Window
OIT's weekly maintenance window is from 8 PM on Friday evening to 6 AM on Saturday morning. During this time services provided by OIT may not be available. Most extended outages initiated by a change control ticket should be done during this window of time. In some cases, changes are performed outside of the normal maintenance window so that staff are available immediately (or the following business day) to troubleshoot related issues.
Change Control

Appendix A - Change Request Field Descriptions

The information below describes what should be entered into each of the fields on a change control ticket.

Starts:

Click on the Show Details tab and enter the day and time that the change will begin.

**IMPORTANT:** If this date is not entered correctly the change will not show up on the weekly email.

Type:

See the "Included IT Systems" tab on the [OIT System Outage Communication Plan](#) to determine whether a change should be listed as an Announcement or a Change Request. If the change is an emergency change then select Emergency Change and follow the Emergency Change process described above.

Public Description:

This field should describe the change in terms an end customer can understand. The exact names of servers involved, detailed protocol issues and the like should not be listed here where the general public is not likely to care. Instead, describe the service a customer may be using that will be changed or be unavailable during the change. Also include how long the change/outage is expected to take.

Scope:

This is where the technical details should be outlined. List the expected impact of the change or outage. In a sense, think of it as the class of user. MySQL is being upgraded? Then users attaching to the databases directly and web sites using the db for back-end storage are effected but not email users using Thunderbird.

Benefits:

List the reason for the change. This is often "security patching", "fix know bugs", and the like. It could also explain why the change is better than some older system used before.

Risk:

What are directly related consequences that may result if the change fails for some reason. Obvious risks include protracted outages and loss of data. More important is when these risks affect related systems a customer may not suspect. RADIUS upgrade? All dialup, wireless, vpn users may be at risk.

Testing:

What testing has been done to give you confidence that the change will succeed? This seems obvious but this can often be involved partially in the risk. Some systems are too expensive to own a development environment or too complicated to perform all testing in a development environment. If this is the case, it should be stated as a warning.

Roll Back Plan:

Explain what might be a non-trivial strategy needed to revert systems to their prior function (or dysfunction). Some changes are one way trips into the future and so this text also can serve as a warning that there is no turning back.
Change Control

Customer Impact:

Describe what the effect of the change will be on end users if everything goes as planned. It’s also helpful to describe what the effect might be if something goes wrong.

Duration:

How long will the change take? 1 hour, 3 hours, two days, etc.
Change Control

Appendix B - Risk and Impact Definitions

Risk

Risk defines the potential disruption of business operation associated with a given change request. A risk is measured by the probability of a threat or the vulnerability of the IT service to that threat. Typical risk definitions are:

- **None**: The RFC has no potential for disruption.
- **Low**: Business operations may be interrupted or delayed with little impact to commitments.
  - Requires no work outage
  - Affects only one noncritical application or system
  - Affects a limited number of clients
  - Involves changes that are made during nonproduction hours
- **Medium**: Business operations may be interrupted or delayed, which affects commitments.
  - Requires a limited outage
  - Affects a few applications or one mission-critical application
  - Requires a business application redesign or enhancement
  - Affects more than X clients (use impact for guidance)
- **High**: Business operations may be interrupted or delayed, resulting in financial impact to the business.
  - Requires a widespread outage
  - Affects multiple business-critical applications
  - Requires a new business application or a major redesign
  - Affects more than X clients (use impact for guidance)

Impact

Impact measures the pain caused by a defective IT service. In most cases, variables such as geography, users and so on help identify the scale. Typical impact classification definitions are:

- **Low**:
  - Affects one to a few end users
  - Affects a few configuration items (for example, one to 10 desktops and one server)
  - Notification is needed for one IT department
- **Medium**:
  - Affects multiple customers
  - Affects more configuration items (for example, 10 to 100 desktops and two to 10 servers in a department)
  - Notification is needed for a few IT and business departments
- **High**:
  - Affects multiple departments and sites
  - Affects multiple and/or a variety of configuration items (for example, desktops and servers, multiple services and/or a mission-critical service, such as three mission-critical applications, 50 servers and 250 desktops)
  - Notification is needed for multiple IT departments and business sites