University Standard on Information Technology Change Management

Introduction

PURPOSE

This Standard sets minimum requirements for managing Information Technology (IT) changes which must be met by University units to comply with the requirements of our IT Security program.

SCOPE OF APPLICABILITY

University business units and constituent individuals responsible for material changes to Production IT systems, applications, and services.

Standard

Required

University business units responsible for changes to IT systems and applications must create and document processes or procedures which at a minimum:

- Classify types of IT changes into categories. At a minimum these must distinguish operational change, planned change (including emergency), and unplanned changes. Documentation should include examples for each category.
- Ensure changes are submitted and implemented by authorized users/requestors;
- Ensure changes are assessed based on risk, and approved by authorized approvers with appropriate separation of duties
- Address communication of material changes to all relevant individuals;

Recommended

The following should be implemented as appropriate and feasible. Units should consider the following for both applications and systems when developing IT Change Management processes and procedures:

- **Documenting the change request:** Change requests should be categorized and recorded, along with informal assessments of the
importance of that change and the difficulty of implementing it.

- **Formal assessment:**
  The justification for the change and risks and benefits of making/not making the change are evaluated. Document a system for accepting or rejecting change requests, with communications of decisions back to requestor.

- **Planning:**
  Those responsible for changes should document methodology for test plans or maintain records of detailed test/project plans for change design and implementation, as well as plans for rolling back changes and rollback triggers should changes be deemed unsuccessful.

- **Designing and testing:**
  Design the program for system/software change and tests. If the change tests are successful and approved they may be scheduled for implementation in a production environment.

- **Implementation and review:**
  Responsible staff implement the change and appropriate parties review the change as appropriate.

- **Final assessment:**
  The change request is closed when the implementation is completed satisfactorily and outcomes are achieved.

- **Change documentation:**
  All planned changes requiring change management approvals and made to systems (e.g. servers, databases, applications, batch jobs, and infrastructure) should be documented.

**EXCEPTIONS**

Due to the rapid implementation and transient nature of some research systems, self-maintained (not maintained by a formal IT group), single-server research systems used only within the area of responsibility of a single Principle Investigator (PI) may be excepted from the requirements of this Standard at the discretion of the University unit responsible for each system. This exception must be approved and documented by the IT or other staff member overseeing IT Change Management for the unit.

Test and Development systems are excepted from this Standard if they are separate from production systems such that changes to the test system would have a low risk of Production impact.

Until 12/31/2018 this Standard should be considered "best practice." After that date, the Standard will be in full force and effect.

**Definitions**

**Change:** The addition, modification, or removal of anything that could have an effect on IT services.

**University Constituent:** UNC-Chapel Hill faculty, staff, students, retirees and other affiliates, contractors, distance learners, visiting scholars and others who use or access UNC-Chapel Hill resources.

**Related Requirements**

**EXTERNAL REGULATIONS AND CONSEQUENCES**

Failure to comply with this standard may put University information assets at risk and may have disciplinary consequences for employees, up to and including termination of employment. Students who fail to adhere to this standard may be referred to the UNC-Chapel Hill Office of Student Conduct. Contractors, vendors, and others who fail to adhere to this standard may face termination of their business relationships with UNC-
Chapel Hill.

Violation of this standard may also carry the risk of civil or criminal penalties.

UNIVERSITY POLICIES, STANDARDS, AND PROCEDURES

University Policy for Information Technology Change Management

Contact Information

PRIMARY CONTACT

Unit: ITS Policy Office
Phone: 919-962-HELP
Email: its_policy@unc.edu

All revision dates:

Attachments:

 UNC-Chapel Hill Policy Submission Form - IT Change Management.pdf

Approval Signatures

<table>
<thead>
<tr>
<th>Step Description</th>
<th>Approver</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>University Policy Review Committee</td>
<td>Atinuke Diver: Administrative Director</td>
<td>pending</td>
</tr>
<tr>
<td>Incorporate feedback</td>
<td>Kim Stahl: Senior Policy and Process Lead</td>
<td>3/16/2018</td>
</tr>
<tr>
<td>Administrative Review</td>
<td>Matthew Teal: University Program Specialist</td>
<td>3/15/2018</td>
</tr>
<tr>
<td>Administrative Review</td>
<td>Lee Bollinger: Associate University Counsel</td>
<td>3/14/2018</td>
</tr>
<tr>
<td>Administrative Review</td>
<td>Philip Garriss: Information Systems Auditor</td>
<td>3/13/2018</td>
</tr>
<tr>
<td>Review by Key Stakeholders</td>
<td>Kim Stahl: Senior Policy and Process Lead</td>
<td>3/12/2018</td>
</tr>
</tbody>
</table>