UNIVERSITY OF OKLAHOMA
Health Sciences Center
Information Technology
Security Policy

IT Change Management Policy

Current Version	Compliance Date	Approved Date
1.0	05/31/2018	05/08/2018

1. Purpose

The purpose of this policy is to ensure that all applicable changes to the OUHSC IT environment are documented and managed through an established process.

The goals of the OUHSC IT Change Management Policy include, but are not limited to the following:

- Establishing and enforcing a standard process for planning, approving, implementing, communicating, and reporting changes to the OUHSC IT environment.
- Preventing and/or minimizing risks to the OUHSC IT environment as a result of a Change Request being implemented.

2. Scope

This policy applies to all OUHSC Information Technology personnel and contracted vendors involved in activities that cause or require changes to technology solutions managed by OUHSC Information Technology. All Information Technology changes are within scope of this policy.

Technology covered under this policy are defined by the OUHSC IT Leadership Team on an ongoing basis and include, but are not limited to: platform services, network and security devices, storage infrastructure, physical server hardware/software, virtual server hardware/software, datacenter facilities, network closets, and other service platforms.

3. Policy

The following policy is established for OUHSC IT Change Management:

Applicability

- All OUHSC Information Technology personnel and contracted vendors must use the current system of record and the documented ***Change Management Process*** to prioritize, control, and request approval for all technology solution changes.
- Unless previously documented as a Service Request, Incident ticket in the system of record, or a pre-approved No-Risk Change ticket in the system of record, a Change Request is required for **ANY** change to the technology realm(s) that are subject to the policy.
- All Firewall and Router Changes must be performed under the ***Change Management Process*** without exception.
- Where appropriate, proposed changes should be first applied to Development or Test environments to accurately define the risk of impact prior to submitting a Change Request.

Request Documentation

The request for change must include, at a minimum, the following:

- Description of the following in the ***Description*** field of the **Change Request** form, for risk analysis purposes:

    - Known or possible or expected impacts, failures, losses of service
    - People, Groups, Information Systems, or Services affected by the requested Change
- Modifications may be needed to clarify or correct a submitted Change Request. However, modifications to *Target Date, Target Time, or Change Plan* on a previously approved Change Request, without express notation by a Change Advisory Board member, invalidate the existing approvals and the change approval process must be restarted.
- Change Requests cannot be submitted more than 14 University business days before the Planned Start Date.
- Multi-part Changes that would impact multiple OUHSC IT environment components must be submitted as individual Change Requests per component (i.e., "Creating a new VLAN," "Adding VLAN to F5 Load Balancer," and "Creating Firewall Address Book Entry for VLAN," are all separate Change Requests).
    - **EXCEPTION:** Operating System or Database patches or infrastructure changes being implemented across the entire platform (i.e., "Monthly Maintenance," or "Ghost Vulnerability Patches to Oracle Hosts")
- Change Requests cannot span more than 5 University business days between Planned Start Date and End Date.
- All Standard, Normal, and Emergency Changes must be associated with the appropriate and accurately identified *configuration item* that will be changed. If a configuration item (CI) is not documented in the system of record at the time of the Change Request, the Change should be associated with the CI of the affected Service.
- All Standard, Normal, and Emergency Changes must have a documented back-out plan in case of change failure as part of the Change Request.

Request Approval

- A Change Request must be submitted to the System of Record for approval in the required format available in the system of record, with a defined Change Plan and Back-out Plan, as well as a Target Date and Target Time. Failure to include these items will result in the Change Request being denied.
- Standard Changes are pre-approved; however, they must still be documented with an appropriately-crafted Change Request and MUST reference the appropriate (approved) Change Plan. Associating an irrelevant or incorrect Change Plan to a Standard Change invalidates the change request and is subject to Change Accountability review.
- Pending Normal Change Requests are reviewed weekly; Normal Change Requests must be submitted before 12:00 pm on Wednesday of a given week in order to be considered at the same week's Change Advisory Board meeting.
- All Standard, Normal, and Emergency Change Requests (see below) that are not in response to a service outage must be marked as Approved in the system of record before they are implemented; Emergency Change Requests in response to a service outage are approved at the discretion of an OUHSC Information Technology manager.

Emergency Changes

- Emergency Change Requests that are not in response to a service outage must have written or verbal approval from the eCAB prior to implementation.
- Emergency Change Requests that are in response to a service outage can be performed first and documented after service is restored, at the discretion of an OUHSC Information Technology manager.

This policy does not supersede any conflicting or more stringent regulatory requirements such as thos in the PCI, HIPAA, or FERPA regulations.

4. Enforcement

The OUHSC IT Change Advisory Board will conduct a *Change Accountability Review* on a quarterly basis, or more often as needed. Change Accountability Review identifies and evaluates change requests, the changes themselves (documented and undocumented), and the individual users requesting/performing changes if there are variances from either change policy or procedure. Errors in either will be documented, and the CAB will address them with individuals involved, their HR manager, OUHSC IT leadership, and/or OUHSC HR, depending on the severity, frequency, or other factors determined during the Change Accountability Review.

5. Regulatory References

- Section 501(b) of the Gramm-Leach-Bliley Act (“G–L–B Act”)
- Payment Card Industry Data Security Standard (PCI DSS)
- FERPA
- HIPAA § 164.308(a)(8)

6. Authorization

This policy is authorized and approved by the OUHSC Dean’s Council and Senior Vice President and Provost and enforced by the IT Chief Information Officer. Internal Audit and other authorized departments of the University may periodically assess compliance with this policy and may report violations to the University Administration and Board of Regents.

7. Renewal/Review

The Change Management Policy will be reviewed on the following basis:

- Annually, by the change Management Process Owner, or more often if circumstances warrant.
- Upon an update to the ***Change Management Process*** and/or system of record
- Upon request of the OUHSC IT Leadership Team

8. Revision, Approval and Review

8.1 Revision History

Version	Date	Updates Made By	Updates Made
1.0	05/20/2016	IT Security	Baseline Version
1.0	12/15/2016	Legal Counsel	Refined scope Moved scope Updated HIPAA regulatory reference
1.0	03/14/2018	IT Security	Minor revisions based on SME review
1.0	03/25/2018	Subject Matter Experts	Minor revisions

8.2 Approval History

Version	Date	Approved By
1.0	05/08/2018	Information Security Review Board

8.3 Review History

Date	Reviewed By
12/15/2016	Legal Counsel
12/15/2016	OUHSC IT
03/13/2016	Christopher Vance
05/08/2018	Information Security Review Board