NORTH CAROLINA AGRICULTURAL AND TECHNICAL STATE UNIVERSITY

INFORMATION TECHNOLOGY CHANGE MANAGEMENT

UNIVERSITY STANDARD

I. Purpose

This standard defines Information Technology Change Management requirements at North Carolina Agricultural and Technical State University (N.C. A&T). Change Management ensures that modifications to Information Resources, or the introduction of new applications in a Production Environment, are planned, evaluated, authorized, communicated, implemented, and reviewed in a successful manner with minimal disruption to campus operations. Change Management provides structure to manage risks associated with changes and ensures the efficient use of organizational resources.

This standard is an extension of the university's Information Security Policy (ISP) and provides additional technical specifications. All requirements and sanctions of the ISP apply to this standard.

II. Scope

This document includes requirements for Change Management of all Information Resources owned or operated by N.C. A&T regardless of the location, purpose, college, or division that is responsible for said resource. This includes modifications of existing systems or the introduction of new technologies. This also includes Information Resources that are housed in facilities owned or operated by third parties. In this event, only those Information Resources owned or operated by N.C. A&T are within the scope of this standard. However, other standards specify the requirements for facilities managed by third parties.

This standard does not apply to changes in the scope, objectives, or deliverables of projects. Note, however, that changes to an Information Resource resulting from a project change must comply with the requirements of this document.

This standard does not apply to cloud computing systems in which the vendor implements changes without approval of its clients. Such changes represent a risk the university accepts in the contractual relationship with the vendor.

Information Technology Services (ITS) may approve exceptions to any portion of this standard as required to meet operational or technical requirements. All remaining portions shall apply.

III. Definitions

Change Advisory Board (CAB) – A group of Stewards and Custodians charged with evaluating, approving, and reviewing Major, Minor, and Emergency Changes to Information Resources under the joint purview of the Stewards.

Change Management – A defined process that ensures all changes to Information Resources are planned, evaluated, authorized, communicated, implemented, and reviewed in a controlled manner by the appropriate Steward(s) and Custodian(s). Change Management helps to control risk and minimize disruption to university operations.

Emergency Change – A change that must be implemented immediately due to security or availability concerns.

Information Resource – As defined in the ISP, an Information Resource is information owned or processed by the university, or related to the business of the university, regardless of form or process or transmit that information. Information Resources expressly include data, metadata, software, processes, procedures and physical assets. Updates to the definition in the ISP shall have precedence over the definition in this standard.

Information Resource Custodian (Custodian) – As defined in the ISP, Information Resource Custodians are university employees authorized to grant access to university data based on delegation from an Information Resource Trustee or Steward, or who have been assigned operational responsibilities for maintaining applicable controls such as data security, physical security, backup, and recovery. Updates to this definition in the ISP shall have precedence over the definition in this standard.

Information Resource Steward (Steward) – As defined in the ISP, Information Resource Stewards are unit or department leaders with planning and management responsibility for defined Information Resource data sets, software or physical assets. Data stewardship responsibilities include data classification, access control, accuracy, integrity, retention, and disposal. Updates to this definition in the ISP shall have precedence over the definition in this standard.

Information Resource Trustee (Trustee) – As defined in the ISP, Information Resource Trustees are senior university officers (e.g., Vice Chancellors, Vice Provosts, Deans, etc.) who have oversight, policy, and compliance level responsibility for defined Information Resource data sets, software, and hardware resources. Updates to this definition in the ISP shall have precedence over the definition in this standard.

Major Change – Changes that have a significant impact on Information Resources and therefore pose a significant degree of risk to operations, the use of organizational resources, or the introduction of new vulnerabilities.

Minor Change – Changes that have low impact on Information Resources and therefore have low risk to operations, the use of organizational resources, or the introduction of new vulnerabilities. The impact of a Minor Change is similar to that of a Standard Change, but the former does not occur with the frequency of the latter and must be evaluated and approved by Steward(s).

Non-production Environment – An environment in which Information Resources are created, modified, or tested to meet the needs of the university. Non-production Environments may be used to test new technologies, new versions or modifications of software, new configurations, or new applications before these resources are deployed in Production Environments. Non-production Environments do not support actual university operations.

Production Environment – An environment in which Information Resources are used for university operations. Production Environments are used to support academic, administrative, or research functions and are distinct from Non-production Environments.

Standard Changes – Changes that have low impact on Information Resources and therefore have low risk to operations, the use of organizational resources, or the introduction of new vulnerabilities. Standard Changes occur on a recurring cycle. Examples include operating system or application security patches but exclude application upgrades that introduce new or modified functionality.

IV. Responsibilities

A. Trustees – Trustees shall provide executive oversight of Change Management processes and ensure that resources are provided for their successful execution. Trustees shall authorize Emergency Changes in the absence of a Steward.

B. Stewards – Stewards shall plan, test, evaluate, authorize, and review Major, Minor, and Emergency Changes to Information Resources. Stewards shall communicate all changes to impacted stakeholders and shall maintain records and artifacts of all changes.

C. Custodians – Custodians shall work with Stewards to plan, test, evaluate, authorize, and review Major, Minor, and Emergency Changes. Custodians shall plan, evaluate, test and review Standard Changes. They shall install changes and advise Stewards of issues resulting from changes. Custodians shall work with Stewards to maintain records and artifacts of all changes.

D. ITS – ITS shall work with Stewards and Custodians to plan, test, evaluate, authorize, and review changes. Note that ITS staff members may also serve as Trustees, Stewards, or Custodians.

E. Vice Chancellor for Information Technology and Chief Information Officer (CIO) – The CIO shall provide oversight of IT Change Management processes and authorize Emergency Changes in the absence of a Steward.

V. Requirements

All changes to Information Resources shall follow a formal Change Management process that complies with the requirements of this standard.

A. Change Management processes shall specify responsibilities for planning, evaluation, testing, authorization, communication, installation, and review of changes. Change Management processes shall specify types of communication and groups of recipients as appropriate and shall be designed to minimize the disruption of campus operations.

B. Major and Minor Changes will be planned, tested, and evaluated by the appropriate Steward(s), Custodian(s), and others as needed to address risks related to the change. Testing and evaluation shall ensure that changes have a minimal impact on operations, do not introduce additional vulnerabilities, and make efficient use of organizational resources. Stewards and Custodians shall conduct acceptance testing prior to deployment in Production Environments and shall verify the operation of Information Resources following deployment.

C. Major and Minor Changes shall be authorized by the appropriate Steward(s) before said changes are deployed to Production Environments.

   Due to the urgent nature of Emergency Changes, the appropriate Steward(s) shall authorize deployment in Production Environments with limited evaluation. The appropriate Trustee(s), the CIO, or the CIO's delegates shall authorize Emergency Changes in the absence of the appropriate Steward(s). Emergency Changes shall be evaluated and authorized by the appropriate Steward(s) following the deployment to Production Environments as soon as feasible.

   The appropriate Steward(s) shall authorize Custodian(s) to evaluate and install Standard Changes in Production Environments on an ongoing basis without additional evaluation or authorization from the Steward(s). Custodians shall, however, notify Stewards of pending changes, and Stewards shall provide communication to the appropriate stakeholders. Standard Changes that result in recurring issues shall be reviewed by the appropriate Steward(s) and Custodian(s) to eliminate said issues.

D. Emergency Changes shall be applied only to address an immediate threat to or restore functionality of an Information Resource in a Production Environment. Emergency Changes shall be applied only when there are no other effective means of addressing the situation.

E. In cases where multiple Stewards share responsibility for an Information Resource, each Steward shall approve the change. Alternatively, the Stewards may collectively approve a Change Management process that specifies the Steward(s) who subsequently approve changes. The group of Stewards who approve changes constitute a Change Advisory Board.

F. Changes shall be scheduled to minimize the disruption of campus operations to the extent possible. Standard Changes shall be installed during a regularly scheduled maintenance window.

G. Changes shall be installed, tested, and evaluated in a Non-production Environment before said changes are applied in Production Environments where possible.

H. Whenever possible, changes shall include roll back plans to reverse the change and revert the Information Resource to its previous state, should it produce unacceptable results following implementation.

I. Change Management processes shall include communication plans to notify all stakeholders of the change and relevant information. Steward(s) shall be responsible for communications with stakeholders.

J. Stewards and Custodians shall comply with the Information Resource Risk Classification Standard when changes require the Information Resource risk classification be updated.

K. Stewards and Custodians shall review changes after their deployment to ensure that they are functioning as intended and have not led to disruption of campus operations or inefficient use of organizational resources.

L. Change Management procedures shall be applied to data changes that bypass normal application controls, such as direct modification of data in a database.

M. Non-production Environments exist for testing and evaluation of changes or new technologies. Stewards and Custodians shall use these environments to prepare for deployment of changes in Production Environments and shall apply relevant portions of this standard as appropriate.

N. Stewards and Custodians shall maintain records and artifacts of changes made to Information Resources in each environment. These records shall include changes that were proposed but never installed in Production Environments.

VI. Authority, Exemptions, and Advisement

A. Authority and Enforceability – This standard is established under the authority of the university's Information Security Policy and the Vice Chancellor of Information Technology (Information Security Policy IV.C.5).

B. Exemptions – Exemptions to this standard must undergo a formal risk assessment and be approved in writing by Information Technology Services.

C. Review and Oversight – Collaborative advisement concerning these standards is provided by N.C. A&T technology professionals. The Information Security Advisory Committee (ISAC) is responsible for review, revision, and endorsement of information security standards.

VII. References

A. ISO 27002:2013 Code of Practice for Information Security Controls

B. UNC Policy 1400.1 Information Technology Governance

C. N.C. A&T Information Security Policy

D. N.C. A&T Information Resource Risk Classification Standard

Approved by the Chancellor

Date standard is effective: Upon approval

First approved: March 30, 2020