Information Security Standards & Guidelines Management Process
Version: 1.0

Revision History **V1.0 Approved by Chief Information Security Officer (2/14/18)**

Overview

The University Information Security Policy outlines management intent, roles & responsibilities, and high level objective for the University Information Security Program.

To support these objectives additional standards, guidelines, and procedures are needed to provide more detailed requirements on how the high level goals are to be met. This document outlines the process for drafting, reviewing, approving, and maintaining of related standards and guidelines.

Process Steps

I. Standards & Guidelines Drafting - (ITS , Chief Information Security Officer)

The Chief Information Security Officer and ITS-OIS team are responsible for the development of Information Security Standards.

- Develop and initial draft of a new Information Security standard or guideline (Google Doc for collaboration) using defined template.
- Indicate how this standard supports the high level objectives of the University Information Security Policy and associated ISO27002 Objectives (UNC Info. Security Baseline).
- Indicate the risks and/or compliance objectives that that this standard helps to address and anticipated outcome (value) of implementing the standard.
- Indicate any existing standards, policies, or guidelines that this new standard would supplant.

II. Collaboration & Governance

The following Campus bodies will be asked to provide feedback based on their respective governance roles and expertise. (ITIG and ITSLs will need to provide feedback prior to IT Board of Directors, Data Stewards, or ISAC review).

It is expected that the standard draft will be updated (version releases) as it undergoes review and these changes will be indicated in shared Google Doc. These changes to version will be indicated to

A. **ITS IT Implementation Group (ITIG)-**
  - Feedback, suggestions, and outline of how the goals embodied in the standard can be met on a technical & procedural basis.
  - Cost evaluation & general compliance timeline estimate for reaching the objectives of the standard in central IT.

B. **University IT Security Liaisons (ITSL) -**
  - Feedback, suggestions, and outline of how the goals embodied in the standard can be met on a technical & procedural basis.
  - Cost evaluation & general compliance timeline estimate for reaching the objectives of the standard in non-central IT units.

C. **CIO, IT Board of Directors, and Data Stewards Council**
  - Provide feedback & suggestions of draft.

E. **Information Security Advisory Council (ISAC) -**
  - Review whether the proposed standard addresses high level policy goals outlined in the University Information Security Policy.
  - Review campus feedback and compliance timelines and cost evaluations from ITIG and ITSL.
  - Provide up/down endorsement (not approval) on ratification of standard.

III. Standards Approval / Sign-Off

The following roles will review the proposed standard along with cost estimates, compliance timelines, and overall feedback collected to determine if the standard may be fit for approval.

A. CISO - Will indicate whether the proposed standard has his/her recommendation for approval.

B. CIO - Will indicate whether the proposed standard has his/her recommendation for approval.

C. If CIO and CISO are in agreement to approve then the Standard will be enacted.

D. If CIO and CISO are in agreement not to approve then the Standard will be rejected and or revisions requested that will constitute a new draft. This new draft will then be brought back to Step II (Collaboration & Governance).

E. If CIO and CISO are not in agreement to either approve or disapprove, then they will review potential amendments to the standard that will constitute a new draft that will return back to step II (Collaboration & Governance). If no amendments are found then standard will not be approved. This will be recorded in University ISO27002 crosswalk.

IV. Approved Standard Publication & Communication

Upon publication of a new standard, the following steps will be taken:

A.. The new standard will be published to:
https://security.appstate.edu/resources/policies_and_standards

B. The University Information Security Policy will be updated to reference the new standard.

C. A brief notification Email & Memo with link to new standard sent to:

- Provost & VCs
- Chief Audit Officer
- General Counsel
- Campus IT Directors
- Directors of "Secure Data Environments" (Secure Data Handling Standard).
- Institutional Data Stewards

D. The University ISO27002 crosswalk will be updated to reflect the new standard.

V. Review & Maintenance of Standards

A. Standards will be reviewed on annual basis by OIS-ITS or an per-need basis given circumstances.

B. ITS-OIS can make minor revisions to standard on a per need basis provided that they do not significantly change the objective or compliance costs associated with maintaining adherence to the standard.

C. Major changes constitute a overall change to an objective contained in the standard or introduction of a new significant requirement. These changes will be reviewed / vetted in the same manner defined in the steps listed above.