University of Colorado
Boulder | Colorado Springs | Denver | Anschutz Medical Campus

---

APS JUSTIFICATION

Policy Title: IT Security Program Policy

APS Number: 6005   **APS Functional Area: Information Technology**

Date Submitted:	August 1, 2023
Proposed Action:	Revision
Brief Description:	The IT Security Program serves as the core for the University's *IT security* activities and provides general guidance to the computing community on ensuring the privacy of personal information and the availability of *University information* and *IT resources*.
Desired Effective Date:	October 1, 2023
Responsible University Officer:	Associate Vice President and CIO
Responsible Office:	Office of Information Security
Policy Contact:	Office of Information Security
Last Reviewed/Updated:	January 1, 2014
Applies to:	Universitywide or as specifically defined by each policy section.

Reason for Policy: Establishes the required roles, responsibilities, and functions for the effective management of the University's IT Security Program and provides general guidance to the computing community on ensuring the privacy of personal information and the availability of university information and IT resources.

I. **REASON FOR PROPOSED ACTION**

As part of a review and refresh of APS 6005, the Office of Information Security has removed extraneous parts of the previous version, updated the titles of the various governance groups and roles related to information security, and tied the updated document to a new security standard based on the NIST-800-171 framework.

As part of the refresh, information that was not specific to information security has been determined to better reside in other governance documents. While those updates cannot be implemented at the same time, we are noting this and leaving those sections within APS 6005 until which time they can be included in the update for the other pertinent documents.

II. **STAKEHOLDERS ENGAGED IN THE POLICY REVIEW**

As a precursor to the review that will take place as part of the OPE process, the updated document was created in concert with the campus IT security teams. After the updates were complete, the document was communicated to the campus IT leadership teams, as well as to the Cyber Risk and Compliance Committee for review and comment.

III. **LEGAL REVIEW**

    A. Do you think legal review would be required for these proposed changes?
        1. If no, please explain.
        2. If yes, what is your plan to get the legal review? **We are communicating the updated APS 6005 document to legal for review and comment.**

B. Date legal review completed:
C. Person completing legal review:

IV. **FISCAL REVIEW**

Are there any financial (human resources, technology, operations, training, etc.) or other resource impacts of implementing this policy (e.g., cost savings, start-up costs, additional time for faculty or staff, new systems, or software)? **No. At this time, there is no financial impact due to the changes within this update**. If yes, please explain: