Published on *University of Colorado* (https://www.cu.edu)

IT Purchasing Standards [1]

Standards for promoting security controls in Contracts, RFPs, and other service arrangements

Date of last review: 03/13/2017

DOWNLOAD IN PDF [2]

Purpose:

The purpose of this document is to provide guidelines for ensuring adequate security controls in the acquisition and renewal process of new products and services for the university.

Authority:

The IT Security Program APS 6005 [3] discusses the need to establish IT Security requirements in RFPs, Contracts, and other service arrangements.

Guidelines:

For any new purchases or renewals related to information technology (IT), including software as a service (SAAS), application service providers (ASP), consulting or other outsourced IT services, it is important to incorporate security considerations early in the process. Attempting to address security concerns late in the purchasing process often results in increased cost and delays. Campus Information Security Officers (ISO) and Office of Information Security (OIS) have a responsibility to provide guidance regarding required security controls.

1. Authorization to use University data - Has department received authorization from the appropriate Data Steward to provide or store data with the third party? Review the data governance process [4] for information on requesting authorization to use university data.
2. Contact Campus ISO or OIS if the purchase/renewal of any product or service that allows access to or that requires transmission, processing or storage of the following information types:

    - Protected Health Information – Individually identifiable health information; health information combined with name, or med record #, or address, or key dates, or family members, or any other information that would link a person to their health condition.
    - Student Records - Individually identifiable student information; name or student id or SSN or photo, in combination with grades, demographics, admissions, schedules, class rosters, financial, or any information needed and used by faculty

and staff about students, with the exception of a limited amount of directory information.
- Personal Identification Information – NIST defines PII as “PII is ?any information about an individual, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.”
- Payment Card information – Any of Primary Account Number (PAN), Cardholder name, expiration date, security code or PIN.
- Export controlled – Data covered by the International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EAR). Visit the Office of Export Controls [5] for more information.

Considerations regarding third party contracts:

- Opt-out options - Any agreement must clearly define what is required for the University or the third party to terminate the service. Additional important considerations include what is the maximum duration of the agreement, and how do we gain access to your intellectual property or University data if the agreement is terminated?
- Expectations regarding intellectual property and data - What are the expectations from the third party to protect intellectual property or University data? Are there additional fees if it is necessary to audit access to the third party systems to the service or restore data from a backup? Will the data be stored in the United States?
- Attestation to standards and Right to Audit: Does the vendor have a SSAE 16 SOC 2 or equivalent report of its controls? Or does the vendor attest to industry accepted security standards such Cloud Security Alliance’s Cloud Control Matrix? Right to audit vendor’s security controls should be included in any agreement that involves sending sensitive university information to third parties.
- Regulatory compliance provisions - Any agreement must specify that the vendor has an obligation to maintain compliance with applicable regulations or standards (FERPA, FISMA, or PCIDSS, etc.). The agreement must identify requirements or fees should it be necessary for the university to audit compliance or review independent third party audit documents. University has recommended language for insertion into contracts that deal with regulatory compliance. Departments should be aware of this language and contact ISO for guidance.

Use of third party providers (Subservice organizations) by vendors: In certain instances, the data sent by the university to the vendor may be stored on infrastructure that does not belong to the vendor itself but rather a third party provider (e.g. Amazon, Rackspace, Google). It is important to clarify with the vendor, the legal relationships it has with the subservice providers and the services that will be provided by the subservice organizations. This is critical if transmission, processing, and/or storage of sensitive university data are involved. Contact your Information Security Officer for further guidance in these cases.

Groups audience:
Office of Information Security

Links

[1] https://www.cu.edu/security/it-purchasing-standards [2] https://www.cu.edu/doc/purchasing-standardspdf [3] https://www.cu.edu/ope/aps/6005 [4] https://www.cu.edu/data-governance
[5] https://www.colorado.edu/researchinnovation/node/8496/office-export-controls