COLORADO STATE UNIVERSITY: INFORMATION TECHNOLOGY STANDARDS AND PROCEDURES

IT Purchase Security Review

Last revised 14 August 2023, Steven Lovaas, CISO

Standards

To comply with Colorado and US laws, as well as specific requirements in CSU's IT Security Policy, the following should be considered standard practices:

Standard 1: Major IT Purchases Require a Security Review

All proposed IT purchases exceeding the threshold of Documented Quote must include a security review by the Division of IT's Cybersecurity & Privacy department.

Procedures

In support of Standard 1:

- The required threshold is currently $50,000, as described in CSU's Purchasing Manual. Proposed purchases above this amount must include a security review.
- Evolving service management technologies in the Division of IT necessitate a phased implementation of this standard.
  - As of this revision (14 August 2023), an email to the Chief Information Security Officer (steven.lovaas@colostate.edu) will suffice to trigger the required review.
  - When the Division of IT's new security web page is finalized, a link will be published to facilitate this request.
  - Upon launch of the FreshService IT Service Management platform, this security review for major IT purchases will be included as a service offering and supported by automated workflows.
- Purchase requests should anticipate enough time to complete an evaluation of the requested purchase, which will include an evaluation of the vendor's risk profile as well as an evaluation of the security and privacy implications of the specifically requested product or service. Depending on the nature of the product – and particularly whether the product houses or accesses sensitive information – the review may require the vendor to provide additional information, which could slow the process.
- Requests for security review will be treated as high priority requests and will be turned around as soon as possible to facilitate acquisition timelines.
- Results of the review will be communicated via email to both the requester and the Procurement department.
- Appeals of security review decisions may be submitted and will be reviewed by the Chief Information Security Officer in consultation with the Chief Information Officer and the Director of Risk Management.