



Information Security Workgroup

July 15, 2021

Zoom Session

Present:	Rick Salomon, Student Affairs Kelly Sebastian, Office of the President Kristy Cutter, OCOB James Mwangi, CAED Trish Brock, R-EDGE Troy Weipert, ITS Jon Vazquez, ITS	Lynne Harrington, SEM Craig Nelson, UD Joan Pedersen, UCM Matthew Ryan, CPC Dale Kohler, ITS Doug Lomsdalen, ITS Gary McCrillis, ITS
Absent:	Derek Gragson, CSM Josh Machamer, CLA Bill Hendricks, CAFES	Robert Crockett, CENG Jennifer Haft, A&F Kyle Gustafson, ITS

I. 2021 Annual Risk Self-Assessment (ARSA) Out Brief

Per CSU Policy (8020) we are required to conduct an annual risk assessment; we accomplish this task via the Annual Risk Self-Assessment. This year, we are significantly reducing the requirements from each College and Division, focusing on just the completion of the questionnaire.

Three broad observations of note:

1. Asset Inventory: We are still seeing an issue with getting our suite of security tools broadly installed.
2. Access Control: Physical and logical access to resources are not performed consistently on campus.
3. Incomplete/missing questionnaires: Completion rate this year was at an all-time low.

Our assessment, based on Division/College reporting, is aligned with the findings of the CSU Chancellor's Office audit team. Based on centralization of IT personnel and resources, we are expecting the discrepancy of installation of security tools will be remediated within the next year, using a single software delivery platform (e.g., SCCM (Windows) and JAMF (Mac)). Efforts to streamline access control reviews will be a priority item for the Information Security Office.

II. Update: CSU CO InfoSec Audit

The CSU Chancellor's Office Audit team finalized our list of observations/findings on June 2, 2021. ITS coordinated the management responses to each observation with the primary office of responsibility.

Since this report is posted in a public space, we will not provide details on the findings. Please contact the security office with specific questions or interested in knowing the details of the findings.

III. Upcoming Security Projects

Disable Legacy Email Protocols: The Information Security Office, in partnership with the ITS Office 365 team, is actively reviewing options and conducting a risk assessment to identify any pitfalls associated with disabling protocols ahead of Microsoft’s sunsetting of them on their schedule.

Enable MFA for Emeritus: Protecting emeritus accounts is the next user group we want to protect via Duo MFA. We are expecting an implementation date of November 1; in the meantime, ITS teams are working on the communication strategy and updating “how-to” documentation for Emeritus.

IV. Post-Centralization – Information Security Coordinator (ISC) Role

The IT Management Council Security workgroup is continuing to grow as we add new divisions to the group, fill vacancies, and add the ITS Client Services Zone Managers.

The roles and responsibilities of the Information Security Coordinators are not changing, the Information Security Office will rely on the ISCs to help spread security related news items, keep division/college leadership informed of security issues, and work closely with the ITS Client Service Zone managers to address security issues in a timely manner.

We currently have vacancies in: Academic Affairs, Strategic Enrollment Management, and ITS Client Services Zone A and C.

V. Action Items

ISO - Gary: Provide Student Affairs a list of devices and their status based on inputs from tools assessment.

VI. Next Meeting

a. October 8th, 2021, 1:10 pm – 2:00 pm, via Zoom