CAL POLY

IT Services

tech.calpoly.edu

Information Security Workgroup
January 13, 2023
Session Notes

Present:

Joe Borzellino, SEM
Trish Brock, R-EDGE
Rick Salomon, Student Affairs
Cheryl May, AA
James Mwangi, CAED
Arthur Heubner, ITS Client Services (A)
Vince Hunter, ITS Client Services (B)
Andrew Kersten, ITS Client Service (C)
Troy Weipert, ITS Client Services (D)
Sarah Jones, ITS
Margie Coolidge, UP (HR/AP)
Joan Pedersen, UCM
Craig Nelson, UD
Lori Serna (A&F)
Kristy Cutter, OCOB
Doug Lomsdalen, ITS
Kyle Gustafson, ITS
Gary McCrillis, ITS
Jon Vazquez, ITS
Craig Schultz, ITS

Absent:

Bridget Benson, CENG
Matthew Ryan, CPC
Kelly Sebastian, Office of the President
Emily Taylor, CSM
Jennifer Boncich, CAFES
Josh Machamer, CLA

I. ICT True-up Project

- ICT purpose: required per policy; documents due diligence; addresses CSU audit finding.
- Thanks to all who submitted their ICT updates.
- Status:
  - Level 1
    - 97% completion rate (n=67)
  - Level 2
    - Phase I "Vintage" - 83% completion rate (n=167) (no info sec review on file)
    - Phase II "Expired"- 15% completion rate (n=144) (accessibility and info sec review on file, but outdated)
    - Notable: ICT product/services no longer in service are averaging ~15% (varies by area).

II. ICT Renewal Notices

- Thanks to everyone who provided feedback on messaging preferences:
  - ICT renewal reminder message schedule = 60/30/15 days prior to "trigger date".
- ICT renewal reminder messages are being sent now and include:
  - Vendor, Title and version of product/service.
  - Recap of product/service (brief sentence).

    - Original ICT requestor.
    - ICT renewal "trigger date".
- As the ICT True-up is ending, we're shifting to a predictable maintenance mode. Most campus units will have 4-10 renewals per month.
- As requested, ITS will explore ways to provide access to prior ICT submission data (PDF).

III. Information Technology Disaster Recovery Audit Update

- We had a very successful IT/DR audit, with three observations
    - Require data center staff require fire extinguisher training and the inspection of the data center fire suppression system.
    - Test failover capability of specific system if both data centers are lost
    - Update a list of ITS supported critical software/services for the Department of Emergency Management to coordinate an initiative to update Division/College Business Continuity Plans.

IV. Security Projects

- Continued Security Audit Remediation – Hardening
    - Informational.
    - The hardening project created in response to the Chancellor's Office Information Security Audit is ongoing.
    - Linux and MacOS operating systems are proceeding with minor updates, while a major effort is underway to create new hardening baseline configurations for all windows systems, including domain controllers.
    - These efforts will potentially impact systems such as workstations and labs, and work is proceeding with careful testing to ensure new configuration items do not break current functionality.

- New Vulnerability Management Software Search/Procurement
    - Informational
    - Qualys, our vulnerability management tool vendor, significantly changed their pricing (doubled Cal Poly's annual bill).
    - Cal Poly has been using Qualys for over a decade; given the cost and time we've been with the same vendor, we are looking at other vulnerability management tools.
    - The team will make a recommendation during Q1 or early Q2 to either continue with Qualys or switch to another solution.
    - If we do decide to change vendors, we anticipate the change will occur during the summer.

- Firewall Rule Audit Remediation
    - Informational
    - In Q4 of 2022, the Information Security Office performed an Audit of the Border Firewall rules

- From the audit, we identified a list of rules presenting a potentially critical risk to the Campus
- Starting in February, ITS will start reviewing the identified rules for:
  - Business justification
  - Remove/Modify critical risky rules
- After the Rules are modified, the ISO will analyze the network isolation of the destination systems, including Risks classified as Critical and Mediums (there are no Highs)

V. Action Items

[] Kyle Gustafson: Contact LastPass to determine breach impact to enterprise users.

[] Craig Schultz: Review options for making previous ICT submissions available.

[] Doug Lomsdalen: Determine need for LastPass notice to current enterprise users.

VI. Next Meeting

April 14, 2023 @ 1:10pm