Information Security Workgroup
January 14, 2022
Meeting Cancelled – Topic updates sent via email

I. Microsoft Retirement of Legacy Email Protocols

There is no proposed timeline from Microsoft to retire the various protocols that do not support MFA. The ISO will work with the O365 email team to see who's currently impacted (e.g., currently using a retiring protocol(s)). ISO will draft general communication for CP Report, and we'll also draft targeted communication to affected users. No defined timeline at this time.

II. Log4J at Cal Poly

Log4j is an open-source, common logging software for Java-based applications.

Late last year, multiple remote code execution vulnerabilities were discovered, and subsequent patches released to address these vulnerabilities. ITS teams are working to remediate. The reach of Log4J is wide and touches many applications running on desktops/laptops, lab machines and servers across the Cal Poly Enterprise.

III. ICT True-Up

It is the policy of the CSU to make information technology resources and services accessible to all students, faculty, staff, and the general public regardless of disability.

To ensure Cal Poly's "due diligence" for accessibility and Information Security compliance, expired ICT reviews with Level 1 data will be assessed in Jan-Feb 2022.

Action Required by Monday, Feb 14, 2022
Step 1 - Review the specific ICT listing (upcoming email).
Step 2 - Indicate if the product/service is still in service.
Step 3 - If "Yes", submit an Online ICT Form for each product/service.

Expired ICT reviews for Level 2, 3 or Non-Sensitive data levels will be addressed in future assessments.

IV. Annual Access Review

For all systems/products/services that process, store, or transmit Level 1 data, CSU Policy requires appropriate access controls be in place. This means only those users with a business justification have access to those systems/products/services. When users change roles, they are granted new privileges and the same due diligence should apply to privileges their new role does not require. Users who have separated from Cal Poly should no longer have access.

For systems that integrate and utilize a centrally managed Authentication and Authorization system (e.g., SSO, Central AD, etc.) provided by Cal Poly, the review is handled via an Access Review of SSO and Central AD.

For systems not utilizing a centrally managed Authentication and Authorization system, an annual Access Review audit must be performed.

The ISC, or their Delegate(s), will be required to ensure the completion of the Annual Access Review Audit for each system/product/service that handles Level 1 data.

V. Action Items

None.

VI. Next Meeting

a. April 8, 2022, 1:10 pm – 2:00 pm, via Zoom