

Technology Security Committee

May 19th, 2021

Agenda

Item 1: Approval of Minutes

Description: Review and approval of minutes from 4-21-2021 meeting.

Item 2: Governance Committee Reports (5 mins)

Description: Note relevant information from available reports as applicable.

- A. TAMU ITAC
- B. AgriLife Computer Advisory Team
- C. CoALS Council of Department Heads
- D. AgriLife Technology Leadership Council
- E. AIT Enterprise Technology Committee (ETC)
- F. AIT Technology Compliance Committee (TCC)

Item 3: Lessons Learned (10 mins)

Description: As applicable from recent activities.

- Vulnerability scans –
 - Expired certificates on web servers. Forwarded to Barry if 02 and Gene if 06., then sent to Tim and Alex as leads for Research Computing Center
 - Remote service using an SSL Certificate that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks
 - Remote service is accepting connections encrypted with SSL 2.0 and/or SSL 3. which is putting systems at risk.
 -

Item 4: New Business / Special Topics (15 mins)

Presenter: Kerry Pickens

Description: Differences between BFURD Audit and annual Risk Assessment

- BFURD Audit will include Research Computing Center and will be continuous
- RA is supposed to be seasonal, but the project scope keeps creeping. We started late in 2020 because of the reorganization and staff turnover. The 2020 deadline for Phase 2 was September 2020 so we just finished Phase 3 Reporting.
- RA only includes the college assets (02), but IT RM tried to add HIPAA assessments. Refer any HIPAA assessments on 06 assets to Keith Wicker.
- 2021 RA will include the applications by impact level category such as
 - Source code
 - No source
 - Vendor hosted

- RA is based on NIST v4 low standards. BFURD is based on NIST v5 and includes emerging technologies. Not notified by IT RM when RA will include NIST v5.
- Purpose of BFURD is to prepare staff for TAMU system audit by preparing audit records for verification and validation. Auditors have their own system and may be using NIST v5. Example of audit record is risk register that includes audit findings, security remediations and vulnerability scans.
- Vet Lab complies with ISO standards so if we consolidate IT departments, will we go to ISO or stay with NIST?

Description: Business Continuity, Disaster Recovery and DR Testing

Audit records that need to be updated and tests scheduled annually

- Plan exists just needs to be updated and include references to other TAMU plans
- DR Exercises need to be scheduled
- Vendor contacts and staff/faculty contacts need to be updated
- Need incident response process documented
- Business Impact Analysis for each department. Draft written by IT staff and then discussed with Dept Head. Include recovery times and objectives, and priority for recovery of assets.

Item 5:

Action Items

- A. Phase I RAIL inventory completed by June 4th
- B. Phase II assessors assigned by DRAC
- C. Business Continuity Plan and DR Plan updated – Sushant to complete by Sept 1
- D. Incident Response Process - Sushant to complete by Sept 1
- E. DR Tests Scheduled by Dec 31st