Research Computing Advisory Committee joint meeting with Information Security Advisory Committee

Minutes Feb 19, 2019 (taken by Erik Deumens)

Present: Cammy Abernathy, Rob Adams, S. Balachandar, Avi Baumstein, Joe Cannella, Ana Conesa, Ryan Davisson, Erik Deumens, Damon Lamb, Colin Mailloux, Jeff Martens, Lauren McIntyre, George Michailidis, Steve Pritz, Ann Progulske-Fox, Bruce Vogel

Agenda

Joint discussion with Research Computing Advisory Committee regarding recommendations for security policy changes

i. Risk Management policy
ii. Acceptable Use Policy
iii. Biometrics Policy
iv. Incident Response Policy
v. Monitoring of IT Resources Policy
vi. Physical Security Policy

Discussion

Risk management

- RCAC worked on a thorough revision of the risk management policy over the summer of 2018. ISAC considers these changes too extensive and wants to keep the policy simpler.
- RCAC argues that the vagueness of the policy has led to very intrusive actions by mostly IT staff who tried to minimize risk without regard for the impact on mostly research activities.
- The group decided after long discussion to keep the policy simple and include a reference to a detailed process document with language such as “the process to implement this policy is described here.”
- The chair of ISAC advocated to create a process to appeal decisions made by UF staff, so that UF business, teaching, and research does not get blocked inappropriately.
    - It is not clear who the appeal should go to: ISAC? ISO? A best practices committee? To be discussed.
    - That brings in the question: Who signs off on IT risk? This is a UF business issue that does not yet have an answer. Privacy Office is working on that.
- Written best practices are needed to guide the IT community at UF
    - Example (from McIntyre): Collect 5 things people can do

workstation set up

- approved OS - list here of link to approved OS, Linux (Ubuntu, debian), Mac OS (list), Windows (7 unitl date XX after than 10)
- antivirus - link to approved list

- malware detection and removal
- phishing protection - link

workstations with restricted data the following are ALSO required

- list - software consistent with IRM list - link

THEN at the link we need the right details e.g. to onboard TREND

- Avi will draft a modification of the policy to include something like “the process to implement the policy is described HERE”
- We will review at the next joint meeting.

Acceptable Use Policy

- The RCAC considers that the AUP is much too detailed.
- Legal counsel makes it clear that the AUP needs to explicitly spell out some activities to ensure that the policy can be enforced.

Biometrics policy

- RCAC feels that protection must be stronger: all biometrics recording devices should be isolated from the network or on a special limited network with no access to the internet.