Research Computing Advisory Committee joint meeting with Information Security Advisory Committee

Minutes Apr 16, 2019 (taken by Erik Deumens)

Present: Cammy Abernathy, Rob Adams, S. Balachandar, Avi Baumstein, Joe Cannella, Ana Conesa, Ryan Davisson, Maureen De Armond, Erik Deumens, Amy Hass, Greg Kiker, Damon Lamb, Colin Mailloux, Jeff Martens, Lauren McIntyre, George Michailidis, Rafa Munoz-Carpena, Donald Novak, Steve Pritz, Ann Progulske-Fox, Melissa Rethlefsen, Elizabeth Ruszczyk, Erik Schmidt, Bruce Vogel, Chris Vulpe

Agenda

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

i. Risk Management policy and standard (completed last meeting)
ii. Acceptable Use Policy (completed last meeting)
iii. Biometrics Policy (completed last meeting)
iv. Incident Response Policy
v. Monitoring of IT Resources Policy
vi. Physical Security Policy

Discussion

The general principle is that policies should be short, but the AUP policy is long. What is the principle? General-Counsel team explains that in general policies are short and will be read by select people. The AUP is an exception in that it has to be ready by everyone and must be clear to everyone.

- Incidence Response

Policy item 2 is very broad. After discussion it is decided that these details are covered in the incident response procedures and plan, which is a restricted document, exempt from public record requests. However, while not a live link, its existence should be acknowledged in the policy under References. References should be numbered and this reference need to be placed in Item 2.
Policy item 1 should list the positions that comprise the CSIRT so that the policy clearly shows the scope of involvement in the CSIRT.
Policy item 3 should refer to the policy on monitoring IT resources as a numbered reference.
Policy item 4 should include the CIO as the decision maker with input from GC and notification to UR.
Policy item 5 The ISAC needs to be added to the definition section to expand on what it is and the value it brings.
Responsibilities items 3 & 4 should have a reference to the full incident response procedures document.

- Monitoring of IT resources

Policy item 2d Include in the heading of item 2 and end with “such as, but not limited to, the following” as a lead-in to items a through c.
Policy item 2c and 2b The RCAC felt that this is redundant. Discussion clarified that 2b pertains to persons who may have violated a policy or law, whereas 2c covers persons who are involved in the investigation, but may not themselves by under investigation. For example supervisors and witnesses.
Policy item 3c Remove as redundant
Policy item 3f Remove as redundant
Policy item 3d There was concern from RCAC that there was no IT emergency that could warrant this; however, discussion clarified that the action may be needed in cases unrelated to IT where there is the potential of personal harm where no time is available to obtain approval. Leave unchanged.

- Physical security

Policy item 1d requires that access be reviewed. For UF data centers and most server rooms and critical telecommunications rooms this is possible as these facilities have electronic card access control, which produces such logs reliably. However, the vast majority of telecommunications rooms and closets in UF buildings are protected by regular locks with no capability to monitor access authorized or unauthorized. To bring these telecommunications rooms in compliance with the policy as written is very expensive and may not be the best use of UF funds. The ISO will investigate what the NIST control requires and what is achievable.

Action items

All the changes discussed during the last two meetings will be implemented by Avi. Then the next meeting this joint committee will review and send the policies on for further distribution and review.