Research Computing Advisory Committee joint meeting with Information Security Advisory Committee

Minutes Sep 17, 2019 (taken by Erik Deumens)

Present: Cammy Abernathy, Rob Adams, Avi Baumstein, Jeff Capehart, Hai-Ping Cheng, Susmita Datta, Ryan Davisson, Maureen De Armond, Erik Deumens, Amy Hass, Richard Hennig, Colin Mailloux, Dan Novak, Steve Pritz, Elizabeth Ruszczyk, Erik Schmidt, Plato Smith, Bruce Vogel, Chris Vulpe

Agenda of ISAC meeting in Tigert 123

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

The joint meetings of Feb 19 and Apr 16 led to a set of proposed changes to the policies. These changes have been made and will be reviewed.

- Risk Management

The policy text remains short and the requested reference to the process description on the ISO website has been added.

- Acceptable Use

The content stays the same, but the policy has been rewritten to use a positive tone instead of a punitive one. General Counsel will review the edited text to make sure that the rewriting for tone does not change the meaning.

- Biometrics

The policy now states that the university will consider biometric data as restricted data. The legislature has declared biometrics data as special in 2017. ISO and General Counsel will properly develop the process to handle biometric data.

- Incidence Response

The definition of CSIRT has been added to the definitions page, the roles have been clarified.
The CIO has been added to the decision path for announcements together with General Counsel and University Strategic Communications.
The Information Sharing and Analysis Center (ISAC) term has been defined and the clarification has been added that only information about external threats will be shared.
A reference is given to the full incident response plan, indicating that this is a restricted document.

- Monitoring of IT resources

All changes have been made as discussed.

- Physical security

The policy has been amended to state that telecommunications facilities that are not monitored electronically to allow monthly audits must be assessed for the risk that is posed by not implementing the control.

- Policy review process changes

The process to review and approve policies will be changed to ensure more timely review and approval. A policy coordinator will be appointed to watch and manage the process.