Jefferson Committee of Research (JCoR)
April 18, 2016
BLSB 105
12:00PM-1:30PM

Chair: Sue Menko, PhD
Recording Secretary: Jessica Gutierrez

Introduction
Meeting was brought to order at 12:05pm by Dr. Menko. The committee approved the minutes from our previous meeting in March and they will be posted onto the JCOR site.

Presentation by Andrea Mancaruso and Sung Moon – a constructive open dialogue with leaders of IS&T to discuss the needs and concerns of research intensive faculty regarding Information Technology at Jefferson

Encryption
The discussion began by talking about the encryption. The current encryption may cause particular computer software to work incorrectly. The IS&T team is aware that there is an encryption problem and they are moving forward with a new software called Checkpoint to protect Jefferson data. Currently they are on the testing stage and so far it seems to be working.

VPN/RAP Differences
Some faculty are experiencing difficulties. VPN gives you access to the whole network and there is a security risk because it is not restricted to corporate devices. RAP limits to what you can have access to and is based on configuration. Faculty raised concerns about accessing RAP through Mac computers. Java must be downloaded and maintained on Mac computers following Mac updates in order to access RAP. Apple products automatically delete every remnant of Java from its system every time there is an update. Instructions on how to access RAP will be going to be posted on the Jefferson Research website.

Spam Email/Accessing Jefferson Email
A concern about being able to control the email filter and reduce the amount of spam that is received was brought up. Too many spam mail gets through the filter to the inbox and the amount makes it difficult for faculty member monitor their e-mail, sometimes missing very important emails. Faculty we informed of the many ways spam e-mail senders change domains and evade Jefferson filters; however, IS&T will look into tightening the parameters of the spam filters that could result in some desired e-mails placed in the junk mail folder

As of September 1, 2015, faculty and staff will no longer be able to access their Jefferson e-mail through their own personal cellphones without IS&T uploading the Airwatch app to manage the email. This was a business decision made to protect the Jefferson enterprise. If accessing Jefferson e-mail from personal cell phones it is possible to get a stipend to cover the use of your phone for work related activity following a manager’s approval. This app will monitor and
manage your email. Using this app requires a 6 digit password, and allows IS&T to wipe the phone if stolen. If you are using your personal phone and decide to leave Jefferson, IS&T will be able to remove all Jefferson information. Jefferson e-mail will always be accessible through the web version of jeffmail.jefferson.edu as it does not leave a footprint on your phone.

The meeting was adjourned at 1:05pm