RE: S&T Security: Some Need To Know Items

Wednesday, January 16, 2013
11:28 AM

Subject	**RE: S&T Security: Some Need To Know Items**
From	Lutzen, Karl F.
To	Wunsch, Donald C.
Sent	Wednesday, January 09, 2013 6:16 PM

Addendum

BPM-911 Electronic Records Administration

http://www.umsystem.edu/ums/rules/bpm/bpm900/manual_911

This policy goes hand-in-hand with the BPM 1201 policy. We need to be sure to use IT approved sources to store our electronic records (see policy for definition). This aids in recover of such records in case a person is not available and is needed by the department, Campus or in response to a legal request such as Sunshine requests or ediscovery. There are Managed Folders available on all Exchange mailboxes to aid and encourage proper record keeping.

Please note, external archives of email should not be used as the sole repository, as these may not be properly secured/backed up. Our new Exchange environment has adequate storage and a default quota of 15 Gigabytes per mailbox. This quota can be expanded but if there is a cost, or who covers it, is not known at this time.

From: Lutzen, Karl F.
Sent: Wednesday, January 09, 2013 10:44 AM
To: Wunsch, Donald C.
Subject: S&T Security: Some Need To Know Items

S&T Security: Some Need To Know Items

Postini

The S&T Campus uses Postini as its spam control engine. ALL spam control engines will capture legitimate mail periodically and it is a good idea to make it a weekly practice to check your Postini Quarantine. Simply log into

https://postini.mst.edu

From the quarantine, you can forward the mail and whitelist senders. Information on how to do this is at:

http://it.mst.edu/services/email/faculty-staff/postini-quarantined/

IMPORTANT: Mail in the Postini Quarantine will age out so this does need to be checked regularly, especially if you are expecting important mail.

Adjustments

If you wish to tweak the settings, while in Postini click My Settings. Here you can adjust your Approved and Block Senders lists as well as make adjustments to your Junk Filters. There are not too many options and it is fairly easy to understand. Click the “More Information” links for help.

Mandatory Reporting

http://infosec.missouri.edu/hr/mandatory-reporting.html

It is required that all information security incident and suspected incidents be immediately reported to the information security office on each campus. In S&T’s case, that is to either email security@mst.edu for suspected items, or call 573-341-6398 for any urgent issues. This phone number is the Information Security Officer’s number and it is monitored by security staff over weekends. Please note this does not include physical security issues like stolen devices. Those must be reported to campus police first, then to security. Please see the web page for examples of security incidents.

BPM-1201 Management, Access and Use of IT Resources

http://www.umsystem.edu/ums/rules/bpm/bpm1200/manual_1201

This is a fairly new policy that spells out using IT resources. The policy needs to be read in its entirety, but I will attempt to explain a key clause:

> **Required Use of IT Resources**
>
> University departments and employees are required to use IT and telecom resources provided or approved by the central IT department at the applicable business unit when conducting University business. Exceptions to this requirement must be approved by the CIO of the applicable business unit.

There are many reasons it is very important for departments, faculty and staff to abide by this, but here are two main reasons:

- Resources need to be checked to meet minimum security requirements prior to using. Failure to do so could result in the exposure of University information or the complete loss of the data.
- IT personnel must respond to any department or eDiscovery requests for data and we need to be able to access it in a timely fashion. This is extremely important in the case of death. If we do not know where the data is stored, it cannot be retrieved for University purposes. We have run into problems before when trying to locate data on deceased faculty. Keeping data on resources that IT has approved or is at least been made aware of reduces this risk significantly.

While it is not spelled out in the policy, researcher faculty have automatic exceptions when their research grants require they use external facilities in the process of performing their research. All other exceptions need to be approved by the CIO.

Karl F. Lutzen, CISSP
Information Security Officer
Missouri S&T
kfl@mst.edu