

March 28, 2018

Dr. Brian Lindshield, President
Kansas State University Faculty Senate
Fairchild Hall
CAMPUS

Dear President Lindshield:

The Electronic Mail Policy, PPM 3455, requires the Chief Information Officer (CIO) to report annually to the Faculty Senate regarding cases where permission to access data was granted per this policy. The relevant portion of section .020 from the policy is:

The University encourages the use of electronic mail and respects the privacy of users. Nonetheless, electronic mail and data stored on the University's network of computers may be accessed by the University for the following purposes:

For items a-g, the extent of the access will be limited to what is reasonably necessary to acquire the information and/or resolve the issue.

- a. troubleshooting hardware and software problems,*
- b. preventing unauthorized access and system misuse,*
- c. retrieving University business related information, **
- d. investigating reports of alleged violation of University policy or local, state or federal law, **
- e. complying with legal requests (e.g.; court orders) for information, **
- f. rerouting or disposing of undeliverable mail,*
- g. addressing safety or security issues.*

** The system administrator will need written approval, including e-mail, indicating the extent of access that has been authorized from the Chief Information Officer or the CIO's designee, to access specific mail and data for these purposes.*

The three conditions that require CIO approval are described in items c, d, and e above. Cases where a terminated employee's access is removed before the normal expiration of such privileges fall under category b, preventing unauthorized access, and do not require approval. However, the approval of the CIO is normally requested under those circumstances.

During calendar year 2017, the CIO granted permission for the following 18 cases (note there were 36 cases in 2016, 36 cases in 2015, 19 cases in 2013, 28 cases in 2012, 21 cases in 2011, 22 cases in 2010, 17 cases in 2009, 18 cases in 2008):

Item d: 6 cases – three cases related to missing or stolen computer equipment; one investigations into alleged harassment requested by KSPUD; one investigation into alleged fraud requested by KSUPD; one investigation into inappropriate email access requested by a former student

Item e: 12 cases – seven requests to preserve relevant email evidence related to existing or pending lawsuits per the federal rules for civil procedure (aka eDiscovery). We were notified of 16 eDiscovery requests in 2017, but only 7 required central IT Services to preserve users' email; three cases were in response to open records requests; two cases were in response to federal subpoena

Please contact me if you have any questions.

Sincerely,



Gary Pratt
Chief Information Officer

