Attachment 2
2020 Data Access Report

Feb 18, 2020

Dr. Mindy Markham, President
Kansas State University Faculty Senate

Dear President Markham:

The Electronic Mail Policy, PPM 3455, requires the Chief Information Officer 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 designee, to access specific mail and data for these purposes.*

The three conditions that require CIO and appropriate Vice President 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 2020, the CIO granted permission for the following 21 cases (note there were 15 cases in 2019, 30 cases in 2018, 18 cases in 2017, 36 cases in 2016, 36 cases in 2015, 19 cases in 2013, 28 cases in 2012, 21 cases in 2011):

Item d: 14 cases – three investigations into inappropriate access to data by an employee; three cases related to employee terminations; three cases involving honor code violations; two cases of student data shared inadvertently via email; two cases related to financial fraud; one case relating to investigations of time theft

Item e: 7 cases – six requests to preserve relevant email evidence related to existing or pending lawsuits per the federal rules for civil procedure (aka eDiscovery); one case was in response to federal subpoena

Please contact me if you have any questions.

Sincerely,

Gary L. Pratt
CIO