To: All KFS Users

From: Joan M. Hagen, Associate Vice President & University Controller

Jill M. Schunk, C.P.M., Associate Vice President, Office of Procurement Services

Date: December 8, 2015

RE: **KFS Critical Data Security Violations**

Memorandum

This memorandum addresses recent inappropriate critical data entry into the Kuali Financial System (KFS). Please read carefully and direct any questions or concerns to:

Charlie Sinex
Director, IU Accounts Payable and Records Management
Financial Management Services
csinex@iu.edu

Policy, Procedure, and Legal Implications Related to Critical Data

The Office of the Vice President for Information Technology defines critical institutional data as data the "[i]nappropriate handling of [which] could result in criminal or civil penalties, identity theft, personal financial loss, invasion of privacy, and/or unauthorized access to this type of information by an individual or many individuals." The Classifications of Institutional Data is published and provides a representative list of data elements classified as critical.

University Policy DM-01: Management of Institutional Data mandates that users of institutional data must not disclose data to others except as required by their job responsibilities. Furthermore, the Indiana University Acceptable Use Agreement obligates university employees to "[m]aintain information in a secure manner to prevent access, viewing, or printing by unauthorized individuals."

These policies and procedures are directly related to IU's legal and contractual obligations, including but not limited to, Indiana Code 4-1-10, which governs our disclosure of Social Security numbers and Payment Card Industry Data Security Standard (PCI-DSS). Failure to meet these obligations carries significant risk to the institution, as well as to those individuals who have been found to be in violation, including potential termination of employment and criminal prosecution.

In practical terms, if you add critical data (such as Social Security numbers, bank account numbers, driver's license numbers, passport numbers, visa numbers, and payment card numbers) to fields on KFS documents wherein such data is not explicitly required, you are violating our data security policies and practices. An example of a field that requires critical data is the Tax Number field when creating a Purchase Order (PO) vendor. **You must not enter critical data in KFS document descriptions, explanations, and notes. You must not attach files that contain critical data to KFS documents.** If you see a full credit card number on a document to be attached to a PCDO, you must redact the number and confirm its successful redaction before attaching the document to the PCDO. If you need to send a Form W-9 that contains a Social Security number, you should fax the form instead of attaching it in KFS. Never add an attachment with a social security number to a KFS document.

Recent Incidents

Within the last five weeks, violations of our critical data policy have been identified within KFS, prompting incident reports to the University Information Policy Office (UIPO). As a result of these violations, access to the affected areas of KFS documents (e.g., Notes and Attachments) has been restricted while UIPO, Financial Management Services, and the Office of Procurement Services are actively investigating these incidents and conducting risk assessments.

Examples of critical data policy violations have included:

- Attaching a Form W-9 containing a Social Security number to a KFS document; and
- Attaching an ACH authorization form containing bank account information to a KFS document;
- Attaching a receipt with an unsuccessfully redacted credit card number to a KFS document; and
- Typing critical data elements in open-text areas, such as the Description, Explanation, Organization Document Number, Line Description, and Notes fields, of a KFS document.

In addition to ensuring that we protect the sensitive information of our vendors, students, employees, and other customers, strict compliance with our critical data policies and procedures will prevent disruptions to our business procedures. As recently demonstrated, a single incident can result in access restrictions that adversely impact the document review and approval process across the entire university.

Status on Restrictions

System restrictions related to these violations have been in place for Vendor Detail on KFS Vendor records, Vendor Maintenance Documents (PVEN), and Procurement Card Documents (PCDO). Permissions for these items is documented below:

- Vendor Detail on KFS Vendor records had previously been restricted from view. The permissions to view vendor detail have been restored effective today, December 8, 2015.
- Notes and Attachments on Vendor Maintenance Documents (PVEN) have been restricted from view. The notes on vendor maintenance documents will be available to only those users on the route log of each specific document, including the document initiator, effective today, December 8, 2015.
- Notes and Attachments on Procurement Card Documents (PCDOs) had previously been restricted from view for all users. That restriction has been removed effective Monday, December 7, 2015 for fiscal staff members on the routing of each specific PCDO document.

Going Forward

Effective immediately, each future violation of the critical data policy within KFS will result in the following actions:

1. A notification of the incident will be emailed to the policy offender and account and RC fiscal officer, with a copy to the campus administrator, vice chancellor, and the university controller; and
2. Incidents will be tabulated by Procurement Services and Financial Management Services jointly for monthly reporting to the committee of Data Stewards.

Please also note that the Financial Management Services and Procurement Services offices are working together to re-evaluate current business practices and system controls, and to design a long-term training and communication plan to mitigate these data security risks.