Critical Data and the KFS
Critical Data Defined

- One of four data classifications at IU (critical; restricted; university internal; public)
- Type of data that imposes significant risks, especially when mishandled

Inappropriate handling of this data 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.
Critical Data Examples

- Health Information
- Social Security Number
- Driver’s License Number
- Passport and Visa Numbers
- Credit and Debit Card Numbers
- Student Loan Information
- Bank Account Numbers
- Student Transcripts

http://datamgmt.iu.edu/classifications.shtml
Unrestricted Fields in the KFS

Never put critical data in unrestricted fields in the KFS:

- Notes and Attachments
- Document Description
- Explanation
- DV Check Stub Text
- Organization Document Number or Organization Reference ID
- DV Supporting Documentation
Restricted Fields in the KFS

Only enter critical data in restricted fields if it is required, i.e.:

- Vendor Document – SSN
- Disbursement Voucher – Wire Information
Redacting Critical Data

Physical Documents
- Black out completely (*beware the Sharpie!*)
- Physically remove data from document

Electronic Documents
- Convert to PDF and utilize Adobe Acrobat’s redact function
Critical Data Policy Violations

Recent Violations:

• W-9 attached to Vendor document
  • Contained vendor SSN

• Receipts/invoices with credit card numbers attached to PCDO documents

• Vendor Information Packets attached to Requisition documents
  • Contained direct deposit information
Critical Data Policy Violations

What went wrong?

• Incomplete redaction

• Inappropriate submission of documentation
Critical Data Policy Violations

What’s next?

- Ongoing incident review
- Policy and procedure review
- Training and documentation review
- New and updated policy and procedure implementation
Reporting Violations

If you see it, you are obligated to report it:

- To your FO
- To FMS for removal

FMS and Procurement Services will take the following actions:

- Notify offenders of violations, copy account and RC FO, campus admin, vice chancellor, and university controller;
- Send monthly report to the Committee of Data Stewards
Policies and Resources

Data Management Policies
• http://datamgmt.iu.edu/policies.shtml

Classification of Institutional Data
• http://datamgmt.iu.edu/classifications.shtml

Acceptable Use Agreement
• https://protect.iu.edu/online-safety/acceptable-use.html

Policies Website
• policies.iu.edu

FMS Support Form
• https://fms.iu.edu/support

Adobe Acrobat Redaction Help

Critical Data Memorandum
• https://fms.iu.edu/index.php/download_file/807/