

KU PRIVACY AUDIT

Covered Data

1. For each of the types of data listed below (such data being "COVERED DATA"), please indicate
 - (a) whether your department has access to each type of COVERED DATA, and if so
 - (b) what is your department's business use for the COVERED DATA.

TYPE OF COVERED DATA	ACCESS (Yes/No/NA)	BUSINESS PURPOSE FOR COVERED DATA
a. Social security numbers (SSN)		
b. Research data containing SSN		
c. Credit card numbers		
d. Debit card numbers		
e. Other bank account numbers		
f. Passwords, pins, certificates & similar data permits access to financial accounts		
g. Driver's license numbers		
h. State (& other government) I.D. card numbers/information		
i. Passport & citizenship information (including passports of other countries)		
j. Income & credit information		
k. Tax returns		
l. Statements of assets &/or liabilities		
m. Financial aid application materials		
n. Other or additional financial aid application materials		
o. Other loan information (including repayment status)		
p. Scholarship application materials		
q. Donor/potential donor information		
r. Payroll information		
s. Other personally identifiable financial information not otherwise publicly available		
t. Health-related information (including KU CAPS data, student-athlete injury & rehabilitation data, & any other person's health care or health care payment information)		
u. Advising/counseling data		
v. Information on health related billing		
w. Research Data containing health information		
x. Research Data containing mental health or counseling information		
y. Student grades		
z. Other student information on athletic compliance forms		
aa. Official &/or unofficial transcripts		
bb. Student ID Numbers		
cc. Other student record information (not "directory information") see http://www.vpps.ku.edu/records.shtml		
dd. Employee ID Numbers		
ee. Personnel files (local, supervisory or		

KU PRIVACY AUDIT

TYPE OF COVERED DATA	ACCESS (Yes/No/NA)	BUSINESS PURPOSE FOR COVERED DATA
main files)		
ff. Other personal human resource information		
gg. Aggregations of names &/or contact information of KU applicants, students, faculty &/or staff		
hh. Sensitive externally owned data (such as data owned by an outside entity which requires confidential handling)		
ii. Public safety incident reports		
jj. Lists of hazardous materials stored @ KU		
kk. Insurance policy numbers		
ll. Legal files		
mm. Other information reasonable people would conclude is private in nature		

Location & Storage

Paper

2. Please answer the following questions regarding the location & storage of *hard copies* of COVERED DATA in your department that your department currently uses or considers "*active*" records.

Location & Storage	Yes/No/NA	Explain
a. Where does your department store this COVERED DATA (cabinet, shelves, etc.)?		
b. Are those locations lockable?		
c. If those locations are lockable, who has the key or code?		
d. If those locations are lockable, who & how is it managed/monitored regarding distribution of the key/code?		
e. If those locations are lockable, is it kept locked when unattended/data is not in use?		
f. Is the COVERED DATA maintained in an identifiably separate way from other files (separate location, different colored files, etc.)?		
g. How is the COVERED DATA physically protected against destruction, loss/damage due to potential environmental hazards, such as fire or water damage?		
h. For what period of time are the hard copies of COVERED DATA in use?		

3. Please answer the following questions regarding the location & storage of *hard copies* of COVERED DATA in your department that are no longer in use or are considered "*inactive*" records.

Location & Storage	Yes/No/NA	Explain
a. Once the hard copies of the COVERED DATA are no longer in use, are they		

KU PRIVACY AUDIT

Location & Storage	Yes/No/NA	Explain
converted to another form (scanned, microfiche, etc.)?		
b. If converted to another form, who converts the COVERED DATA - your department, another department, or a third party?		
c. If another department converts the COVERED DATA, how do manage security over access to COVERED DATA?		
d. If a third party converts the COVERED DATA, do all of the contracts with these parties cover the security of, & restrict further access to, the COVERED DATA?		
e. Where does your department store this inactive COVERED DATA (cabinet, shelves, etc.)?		
f. If this COVERED DATA is stored with a non-KU entity, is there a contract in place with that entity?		
g. If this inactive COVERED DATA is stored at KU, is the location lockable?		
h. If the location is lockable, is it kept locked when unattended?		
i. If the location is lockable, who has the key or code?		
j. If the location is lockable, how does your department manage & monitor distribution of the key or code distribution?		
k. Who needs access to this COVERED DATA to conduct their university work?		
l. Who, besides those who need access to this COVERED DATA, may have access to the area where the COVERED DATA is stored (including during &/or after business hours)?		
m. Is the COVERED DATA maintained in an identifiably separate way from other files (separate location, different colored files, etc.)?		
n. How is the COVERED DATA physically protected against destruction, loss or damage due to potential environmental hazards, such as fire or water damage?		
o. Does your department have a written plan for recovery of information in the event of an environmental hazard?		
p. For what period of time are the hard copies of the inactive COVERED DATA stored?		
q. What is your department's procedure for disposing of the inactive COVERED DATA once this period of time has passed?		

KU PRIVACY AUDIT

Electronic Format

Location & Storage	Yes/No/NA	Explain
4. Does your department maintain any COVERED DATA in an electronic format?		
5. If so, can this COVERED DATA be accessed only from terminals within your department or can it be accessed remotely?		
5. Are your department's computer terminals located such that they cannot be used by the public or others who are not authorized to see the COVERED DATA? Please describe where your computer terminals are located.		
6. Are your department's computer screens located such that they cannot be seen by the public/others who are not authorized to see the COVERED DATA?		
7. Does your department maintain a server with COVERED DATA on it that is not under the control of KU's Info Services/LSS department?		
8. If so, where is the server located & who has access to the COVERED DATA on the server?		
9. If your department maintains COVERED DATA on its own server, what steps have been taken to secure the physical location of the server & the COVERED DATA stored on the server?		
10. Is COVERED DATA downloaded to a hard drive—such as the C-drive? • If so, how is it used, protected & secured?		
Is COVERED DATA downloaded to a shared drive—such as the U-drive? Other? • If so, how is it used, protected & secured?		
12. Is COVERED DATA stored on transportable media (such as a CD, PDA, USB/flashdrive,)? • If so, how is it used, protected & secured?		
Is COVERED DATA stored in a location that is Web Accessible? If so, what controls or security to access the information is used?		
13. Does your department use computers other than those owned or leased by KU for any purpose that uses or otherwise involves COVERED DATA?		
14. Describe your department's backup procedures for any COVERED DATA stored electronically on an office server or other office computer.		

KU PRIVACY AUDIT

15. Do faculty or staff in your department take home laptop computers that contain COVERED DATA? If so, describe any precautions taken to protect the COVERED DATA.		
16. Do faculty or staff in your department download COVERED DATA to computers that are not protected by KU's security systems? (such as home units or other devices)		

Access

Access	Yes/No/NA	Explain
17. Who has access to COVERED DATA in your department (either paper or electronic COVERED DATA)?		
18. Does each person identified above need such access to perform his or her job?		
19. Are any of the people with access to COVERED DATA in your department student workers or volunteers? <ul style="list-style-type: none"> If so, what training & supervision do they receive with respect to handling COVERED DATA? 		
20. Does your department collect signed confidentiality agreements from those with access to COVERED DATA in your department?		
21. Does your department have an established practice for training its employees who have access to COVERED DATA?		
22. If your department has training for employees with access to COVERED DATA then who conducts the training?		
23. If your department has training for employees with access to COVERED DATA then how often/frequently is the training conducted?		
24. If your department has training for employees with access to COVERED DATA then how is participation in the training monitored &/or documented?		
25. Does your department employ security practices such as password protected screen savers or automatic system logouts as part of your department's efforts to secure COVERED DATA? Explain.		
26. Does anyone other than those authorized to access COVERED DATA use the workstations where the hard copies or computers containing COVERED DATA are located? <ul style="list-style-type: none"> If so, what measures are taken to 		

KU PRIVACY AUDIT

Access	Yes/No/NA	Explain
limit access to the COVERED DATA in the workstation?		
27. Who, besides those who need access to this COVERED DATA, may have access to the area where the COVERED DATA is stored (including during & after business hours)?		
28. Where is your fax machine located? <ul style="list-style-type: none"> Do employees, students, or others w/o approved access to COVERED DATA see or retrieve faxes on the machine? 		
28. What steps are taken to limit access to COVERED DATA after a person with authorized access no longer needs the access, leaves the department, or is found to have violated either office of university use policies governing confidential or COVERED DATA?		

Use, Disclosure, & Transmission (Access by Third Parties)

Use, Disclosure & Transmission	Yes/No/NA	Explain
29. Does your department release or otherwise make available COVERED DATA to others?		
30. If so, to whom to does your department release or otherwise make available this COVERED DATA (administrators, faculty, students, & other parties)?		
31. Do any non-KU parties create, receive, or otherwise have access to COVERED DATA on your department's behalf? (For example, do students submit credit card information to make tuition payments via the Web to a third-party vendor? Or, by way of further example, does your department engage a third party to make electronic records of any information containing COVERED DATA?).		
32. If your department does provide COVERED DATA to others, in what forms does your department transmit it (e-mail, fax, over the telephone, in person, etc.)?		
33. Who handles requests for COVERED DATA in your department? <ul style="list-style-type: none"> Do the people who handled requests for COVERED DATA in your department undergo specialized training, such as training on how to recognize potentially bogus requests for information via phone or e-mail? 		
34. If any third parties have access to		

KU PRIVACY AUDIT

Use, Disclosure & Transmission	Yes/No/NA	Explain
COVERED DATA, do the contracts with all of these parties cover the security of, & restrict further access to, the COVERED DATA?		
35. Are the contracts with all of these parties reviewed by the Office of the General Counsel?		
36. Does your department use encryption when electronically transmitting COVERED DATA? <ul style="list-style-type: none"> • if so, identify the encryption type? (such as 128 bit) 		
37. Does your department routinely remove, truncate or otherwise shield COVERED DATA (such as Social Security numbers) when completing surveys or reports? Explain.		

Disposal

Disposal	Yes/No/NA	Explain
37. Describe your department's processes for destroying hard copies of COVERED DATA, including who is responsible & how frequently it occurs. <ul style="list-style-type: none"> • If a third-party is used, is there a contract in place? 		
38. Does your department advise those it shares COVERED DATA with to destroy the COVERED DATA when it is no longer needed?		
39. Does your department follow-up or monitor to ensure the destruction occurs as directed?		
40. Describe your department's processes for destroying electronic records containing COVERED DATA, including who is responsible & how frequently it occurs.		
41. Does your department follow the university's policy on equipment disposal to ensure that COVERED DATA is removed prior to disposing of computers & other equipment that may contain COVERED DATA?		
42. Describe your department's processes for disposing of disks, back-up tapes, non-University computers, or other devices that may contain COVERED DATA.		

Miscellaneous

Miscellaneous	Yes/No/NA	Explain
43. Does your department have written		

KU PRIVACY AUDIT

Miscellaneous	Yes/No/NA	Explain
documentation of its processes for:		
a. Properly using COVERED DATA?		
b. Storing active, inactive, & electronic COVERED DATA?		
c. Access to COVERED DATA?		
d. Transmission of COVERED DATA to third parties?		
e. Disposing of COVERED DATA?		
f. Any training related to COVERED DATA?		
44. Have your department's information security practices been reviewed by Internal Audit, Privacy Office, or IT Security Office in the past year? (or ever—specify when & who?)		