**Information Security Office**

**Unauthorized Access Form**

Date Reported to ISO: \_\_\_\_\_\_\_\_

Date Form Completed: \_\_\_\_\_\_\_

Name of Reporter: \_\_\_\_\_\_\_\_\_\_ \_\_\_\_ Reporter Phone: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Event Type: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_ Date of Event: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Owners: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Incident Description: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Incident Location: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\*Sensitive Data: Information of a confidential or proprietary nature and other information that would not be routinely published for unrestricted public access or where disclosure is prohibited by laws, regulations, contractual agreements or University policy. This includes (but is not limited to) full name or first initial and last name and employee ID (in combination), identifiable medical and health records, grades and other enrollment information, credit card, bank account and other personal financial information, social security numbers, grant reviews, dates of birth (when combined with name, address and/or phone numbers), user IDs when combined with a password, etc.

Please answer the following questions regarding the event:

1. Was sensitive\* data in view or potentially accessed? Yes/No/Don’t know
2. Was viewable data regulated (HIPAA, PCI, FERPA,HB5)? Yes/No/Don’t know
3. If the data was regulated, under what regulation(s)? HIPAA/FERPA/PCI/HB5/Rsrch
4. Where computing devices involved/accessed? Yes/No/Don’t know
5. Where computing devices University owned? Yes/No/Don’t know
6. Where the devices encrypted? Yes/No/Don’t know
7. Did devices contain sensitive data?\* Yes/No/Don’t know
8. Did the devices contain regulated data (HIPAA, PCI, FERPA,HB5)? Yes/No/Don’t know
9. If the data was regulated, under what regulation(s)? HIPAA/FERPA/PCI/HB5/Rsrch
10. Approximately how many regulated records were involved? None or Number: \_\_\_\_
11. Were password(s) attached to or in view of the devices? Yes/No
12. What physical security safeguards where in place (locks, etc.)? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Comments: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\*Note: The above questions assume any data or device that may have been accessed without authorization was either owned by the University or being used for University purposes. If personally owned and used solely for personal reasons, please note this in the ‘comment’ section and do not complete the questions.

For questions, contact the University Information Security Office at [isopol@exchange.louisville.edu](mailto:isopol@exchange.louisville.edu) or Kim Adams - 502/852-6692.