**Information Security Office**

**Computing Device Theft Form**

Date reported to ISO: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date form completed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name of Claimant: \_\_\_\_\_\_\_\_\_\_\_\_\_ Claimant Phone: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Device Type: \_\_\_\_\_\_\_\_ Date of Theft: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Device Owner: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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 stolen device:

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

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

\*Note: The above questions assume the stolen device was either owned by the University or being used for University purposes. If the device is personally owned and used solely for personal data, 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 or Kim Adams - 502/852-6692.