

Department of Property Control

# Sensitive Data Affidavit

**Purpose :** The Affidavit is required to capture end user feedback on sensitive data. This document will serve as evidence that the reporting Fiscal Officer / End User acknowledges the information below is correct to the best of their knowledge.

**Definition of Sensitive Data :** An individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name or the data elements are not encrypted:

- 1) Social Security Number.
- 2) Driver's license number or State identification card number.
- 3) Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

## PROCESS

In the event of a stolen desktop cpu, laptop, or iPad, please follow the steps below:

- 1 ) Complete *Property Control Form (A) Lost-Theft Form* and use it to file your Police Report.
- 2 ) Complete the *Sensitive Data Affidavit* and use it to file your Police Report.
- 3) File your Police Report immediately with CSU Police - Use your device ID card as a reference.
- 4) Submit all completed documents above with signatures to **Property Control** immediately for removal from your inventory.

## ASSET DETAILS

PTAG#: \_\_\_\_\_

Contains Sensitive Data: Yes or No

If **YES** what timely measures were taken to wipe or prevent the dissemination of the sensitive data?

---

---

If **NO**, what was the device used for?

---

---

What information was stored on the device?

---

---

To the best of my knowledge I affirm that the information stored on the device was either sensitive and wiped clean of the data or had NO sensitive data stored on the device. In addition, if this device is needed to retain sensitive data for any reason in the future it must be encrypted.

Print Fiscal Officer's Name \_\_\_\_\_

Signature \_\_\_\_\_

Date \_\_\_\_\_