**Appendix B:**

**Campus Incident Response Team (CIRT) Report**

To be completed by UCSC IT Security or IT Policy, who will review and submit to the Vice Chancellor, Information Technology as soon as possible after breach is ***resolved***. Due care should be taken to ensure accuracy in completing this form, as reasonably possible under the circumstances.

Date:

*From Initial Incident Report:*

Associated IT Request ticket # (if applicable):

Date/time the incident was suspected/discovered:

Date/time the incident was first reported to security@ucsc.edu:

Contact information of incident reporter (name, email, phone, location):

Types of data involved:

\_\_\_\_ Electronic Protected Identity Information (PII)

\_\_\_\_ Electronic Protected Health Information (ePHI)

\_\_\_\_ Payment Card Information (PCI)

\_\_\_\_ Confidential Student Record Data (FERPA-protected data)

\_\_\_\_ Other Restricted Data (please specify)

INCIDENT DESCRIPTION:

|  |  |
| --- | --- |
| Incident description/cause: |  |
| How the incident was discovered: |  |
| Impacted systems: |  |
| Data at possible risk - including whether restricted data may be at risk; if so, specify data types: |  |
| Affected population(s): |  |
| Remedial actions taken since incident discovery, including actions taken to prevent further breaches of security: |  |
| Time to resolve incident |  |

**The CIRT has reviewed and agrees with above scope and affected population:** Yes/No (circle one)

FACTORS to CONSIDER for NOTIFICATION

(from <http://www.ucop.edu/information-technology-services/policies/ucop-it-policies-and-guidelines/uc-it-security-information/determining_notification.pdf>)

1. *Indications that the information is in the physical possession and control of an unauthorized person*
2. *Indications that the information has been downloaded or copied*
3. *Indications that the information was used by an unauthorized person*
4. *Duration of exposure*
5. *The number of individuals affected*
6. *The number of different types of information that may have been acquired*
7. *The extent to which the compromise indicates a directed attack*
8. *Indication that the attack intended to seek and collect personal information*
9. *Risk of loss or harm to the individuals impacted by the breach*

*If notification will take place, identify source of notification addresses and alternatives.*

-----

Portions of this report will be included in the VC IT’s Closure report to UCOP.

*Note 1: For breaches that were initially thought to involve Restricted Data that are determined not to involve that type of data, conclude with the following sentence:*

“The threshold for launching the campus incident response process was not met, as there was no suspected security breach of restricted data.”

*Note 2: For suspected and confirmed breaches of FERPA-protected data, conclude with the following sentence, and forward a copy of this completed summary report to UCSC Registrar:*

“This incident report is being shared with the Registrar’s office for handling with regard to FERPA.”

-----

HISTORY and/or TECHNICAL DETAILS

*Provide if available and relevant*