

**Appendix B-Alt:
Alternate CIRT Report**

To be used for breaches of systems that are determined not to contain or access PII, ePHI, PCI, or FERPA-protected data.

(See Appendix C for breaches involving PII, ePHI, PCI, or FERPA-protected data.)

To be developed by the members of the IT Policy Office in conjunction with System Steward or designee and UCSC Security Team as soon as possible after breach is **resolved or is determined not to involve PII, ePHI, PCI, or FERPA-protected data.**

Relates to:

- Electronic Protected Identity Information (PII)*
- Electronic Protected Health Information (ePHI)*
- Payment Card Information (PCI)*
- Confidential Student Record Data (FERPA-protected Data)*
- Other Restricted Data*

SUMMARY

Provide a summary of the outcome of the data breach. Include any or all of the following information, as relevant. Expected length: approx ½ page.

- How the breach was discovered*
- Scope of breach*
- Source of breach*
- Description of data compromised*
- Affected population*
- Actions taken to prevent further breaches of security*
- Time to resolve breach*

Note: For breaches that were initially thought to involve PII, ePHI, or PCI that are determined not to involve these types 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 PII, ePHI, or PCI.

Note: 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