

**Appendix B:
Campus Incident Response Team (CIRT) Report**

*To be used for suspected or confirmed breaches of PII, ePHI, PCI, and FERPA-protected data,
or of systems containing or accessing these types of data
(See Appendix B-Alt for other types of breaches.)*

To be submitted by UCSC Security Team or the IT Policy Office to Vice Chancellor,
Information Technology as soon as possible after breach is **resolved**.

<i>Scope of breach</i>	
<i>Source of breach</i>	
<i>Description of data compromised</i>	
<i>Population</i>	
<i>Actions taken to prevent further breaches of security</i>	
<i>Time to resolve breach</i>	

FACTORS to CONSIDER for NOTIFICATION

- 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*

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

HISTORY and/or TECHNICAL DETAILS
Provide if available and relevant