CAL STATE FULLERTON

Loss or Theft of University Issued Equipment

Appropriate administrators are responsible for ensuring employees complete University reporting procedures.

________________________ ________________________ ____________________

Employee Name Campus ID Number Date

________________________ ________________________

Department ______________ Immediate Supervisor ______________ Direct Administrator______________

A. Please Complete:

1. Employee has contacted local police: _____Yes _____No Department Name____________________

Police Report Taken? _____Yes ____No Date Filed ______________

Police Report Number __________________________ State Property Tag #:______________

Device Mfg Name:____________ Device Make:______________ Device Model#:_____________

2. Employee has contacted campus Helpdesk: Yes_____ No_____ Date Contacted ___________

*(**Please check all that apply**)*

Campus Rollout? ______ Campus Owned Non-Rollout? _____ Personally Owned System? ___________

Hard Disk Password Enabled? _____ Encryption Enabled? ______ Bios Password Enabled? ________

□ Any Alterations (Please Specify)____

Device Type

□ Desk Top System □ Laptop System □ PDA □ BlackBerry

□ Portable Drive □ Flash Drive □ Other (Please Specify) _________________

3. Brief Description of Event:

4. Information/Data Contained on System **(Refer to Attached Pages for description of Levels)**

Campus/CSU defined Protected Information/data? _______ Non-Protected Information/Data? _______

_____Level I _____Level 2 _____Level 3

Data Types: ______Student _____Staff/Management _____Public Information

______Financial _____Operational

By signing below, I hereby attest the above information is true and correct:

________________________ ________________________ ____________________

Name	Signature	Date

Please FAX signed and completed form to Information Security Office at 278-1100

Classification	Description	Examples
Level 1	This is information can cause the most serious harm to individuals and to the campus as a result of unauthorized access. Much of this information is protected by statutes, regulation, other legal obligation or mandate. The CSU has identified specific guidelines regarding the disclosure of much of this information to parties outside of the university and controls needed to protect the unauthorized access, modification, transmission, storage, or other use.	• Passwords or credentials • PINs (Personal Identification Numbers) • Birth date combined with last four of SSN and name • Credit card numbers with cardholder name • Tax ID with name • Driver's license number, state identification card, and other forms of national or international identification (such as passports, visas, etc.) in combination with name • Social Security number and name • Medical records related to an individual • Psychological Counseling records related to an individual • Bank account or debt card information • Vulnerability/security information related to a campus or system
Level 2	This is information that must be guarded due to proprietary, ethical or privacy considerations.	**Identity Validation Keys** • Birth date (full: mm-dd-yy) • Birth date (partial: mm-dd only) • Mother's maiden name **Student Information** • Educational records (Excludes directory information) – Grades – Courses taken – Schedule – Test Scores – Advising records – Educational services received – Disciplinary actions • Non-directory student information may not be released except under certain prescribed conditions **Employee Information** • Employee net salary • Employment history • Home address • Personal telephone numbers • Personal email address • Parents and other family members names • Payment History • Employee evaluations

Classification	Description	Examples
		• Background investigations • Biometric information • Electronic or digitized signatures • Private key (digital certificate) • Birthplace (City, State, Country) • Ethnicity • Gender • Marital Status • Personal characteristics • Physical description • Photograph **Other** • Linking a person with the specific subject about which the library user has requested information or materials. • Legal investigations conducted by the University. • Sealed bids • Trade secrets or intellectual property such as research activities • Location of assets
Level 3	This is information that is regarded as publicly available. These data values are either explicitly defined as public information (e.g., state employee salary ranges), intended to be readily available to individuals both on- and off-campus (e.g., an employee's work email addresses), or not specifically classified elsewhere in the protected data classification standard. Publicly available data may still subject to appropriate campus review or disclosure procedures to mitigate potential risks of inappropriate disclosure.	**Campus Identification Keys** • Campus identification number User ID (do not list in a public or a large aggregate list , protection of SPAM, where it is not the same as the student email address) **Student Information** • Educational directory information (FERPA) • Employee Information • Employee Title • Employee public email address • Employee work location and telephone number • Employing department • Employee classification • Employee gross salary • Name (first, middle, last) (except when associated with protected information) • Financial budget information • Signature (non-electronic)