California State University, Fresno
Electronic Data Sanitization and Disposal Guideline

1. Background

Fresno State creates and collects a vast amount of information, much of which is confidential information and vital to the academic and business functions of the institution. All information must be managed with consideration for its confidentiality and sensitivity and needs to suitably sanitized or disposed according to its classification, academic and business requirements, and retention periods.

Data disposal or sanitization is the process of irreversibly removing or destroying data stored in a device (hard drive, flash memory, SSD's mobile devices, DVDs, etc.) or in hard copy form.

2. Guideline

The purpose of this guideline is to protect University data from unauthorized disclosure. Any official University records must be appropriately retained and disposed based on the University's records retention policy prior to cleaning or destruction of the systems, device, or media.

This guideline defines the baseline controls for the sanitization and disposal of information and applies to all data collections including those provided for by statute, held by or within Fresno State organizations.

The data collections include data repositories stored in electronic forms. Records of the disposal activity must be recorded and kept for future reference and accountability.

3. Sanitization or Disposal of Information

Respective institutional information must be sanitized or disposed at the appropriate time using a prescribed method as shown in appendix A that is consistent with the classification of the information as defined in appendix B.

The local department is responsible for ensuring that University data are appropriately removed or destroyed from media before it leaves the control of the department for disposal or reuse. The sanitization method for the media depends on the information stored on the media and its next destination.

3.1. Device Disposal or Transfer Off-Campus

If a device is to be disposed or transferred outside the respective institution, then the device must be sanitized using the licensed tools or physically destroyed.

3.2. Device Transfer Between or Within Institutional Units

Devices containing Level 1 data must be sanitized using the licensed tools. Devices containing Level 2 or Level 3 data must be sanitized using the tools specified in this guideline.

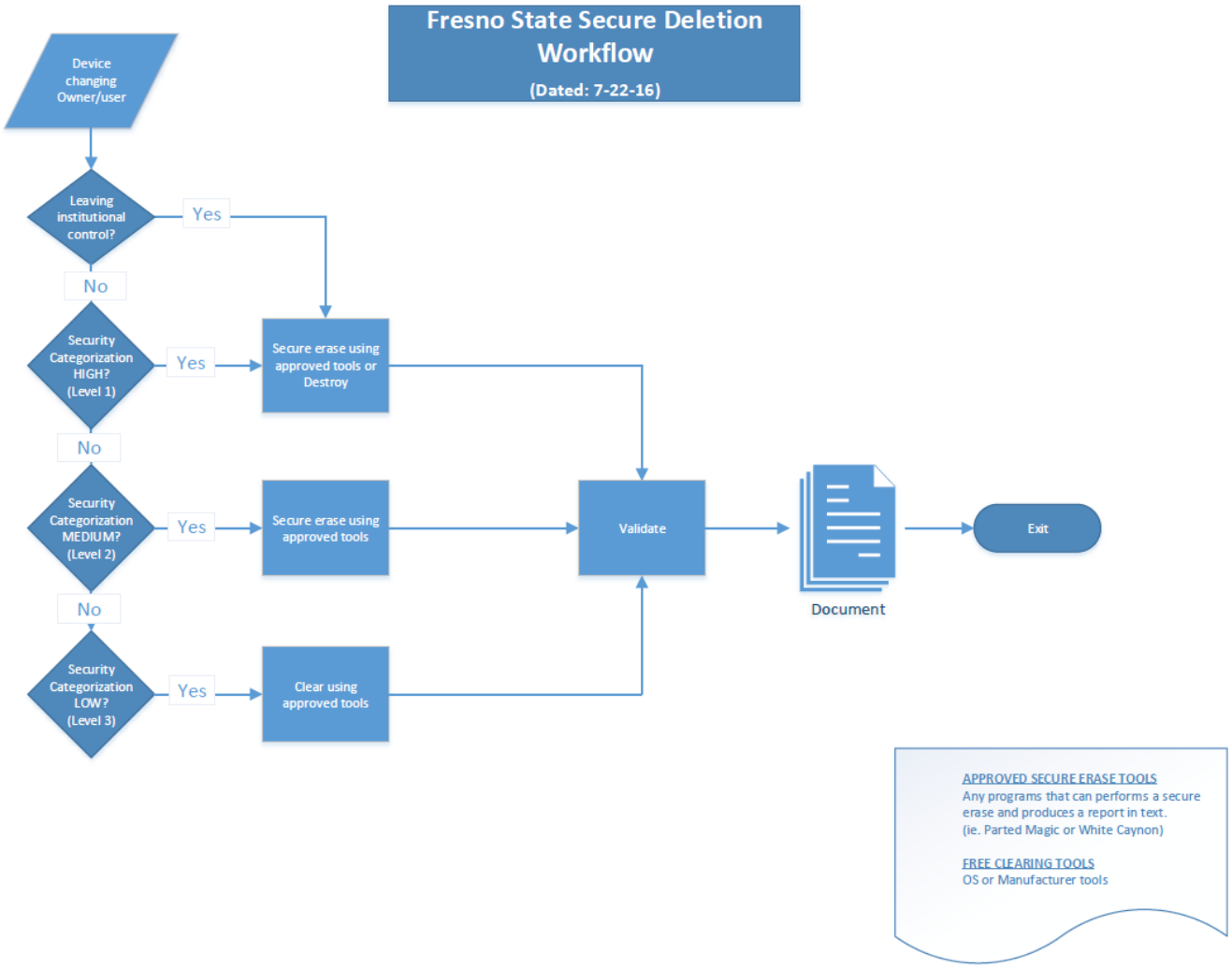
3.3. Personally Owned Device Leaving the Institution

Personally owned devices containing institutional data must be sanitized using the licensed tools.

4. Exceptions

All devices containing institutional data must be sanitized according to the Data Sanitization and Disposal Guideline unless an exception is approved and documented in advance by organization management.

Appendix A: Data Sanitization and Disposal Flow Chart



Appendix B: The California State University
8065.S02 Information Security Data Classification

1.0 Introduction

This document describes the three levels of data classification that the University has adopted regarding the level of security placed on the particular types of information assets. The three levels described below are meant to be illustrative, and the list of examples of the types of data contained below is not exhaustive. Please note that this classification standard is not intended to be used to determine eligibility of requests for information under the California Public Records Act or HEERA. These requests should be analyzed by the appropriate legal counsel or administrator.

Classification Description: Level 1 - Confidential

Access, storage and transmissions of Level 1 Confidential information are subject to restrictions as described in CSU Asset Management Standards.

Information may be classified as confidential based on criteria including but not limited to:

a) Disclosure exemptions - Information maintained by the University that is exempt from disclosure under the provisions of the California Public Records Act or other applicable state or federal laws.

b) Severe risk - Information whose unauthorized use, access, disclosure, acquisition, modification, loss, or deletion could result in severe damage to the CSU, its students, employees, or customers. Financial loss, damage to the CSU's reputation, and legal action could occur.

c) Limited use - Information intended solely for use within the CSU and limited to those with a "business need-to know."

d) Legal Obligations - Information for which disclosure to persons outside of the University is governed by specific standards and controls designed to protect the information.

Examples of Level 1 – Confidential information include but are not limited to:

- *Passwords or credentials that grant access to level 1 and level 2 data*
- *PINs (Personal Identification Numbers)*
- *Birth date combined with last four digits 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*
- *Health insurance information*
- *Medical records related to an individual*
- *Psychological Counseling records related to an individual*
- *Bank account or debit card information in combination with any required security code, access code, or password that would permit access to an individual's financial account*
- *Biometric information*
- *Electronic or digitized signatures*
- *Private key (digital certificate)*
- *Law enforcement personnel records*
- *Criminal background check results*

Classification Description: Level 2 – Internal Use

Access, storage and transmissions of Level 2 - Internal Use information are subject to restrictions as described in CSU Asset Management Standard.

Information may be classified as “internal use” based on criteria including but not limited to:

a) Sensitivity - Information which must be protected due to proprietary, ethical, contractual or privacy considerations.

b) Moderate risk - Information which may not be specifically protected by statute, regulations, or other legal obligations or mandates but for which unauthorized use, access, disclosure, acquisition, modification, loss, or deletion of could cause financial loss, damage to the CSU’s reputation, violate an individual’s privacy rights, or make legal action necessary.

Examples of Level 2 – Internal Use information include but are not limited to:

- *Identity Validation Keys (name with)*
  - *Birth date (full: mm-dd-yy)*
  - *Birth date (partial: mm-dd only)*
- *Photo (taken for identification purposes)*
- *Student Information-Educational Records not defined as “directory” information, typically:*
  - *Grades*
  - *Courses taken*
  - *Schedule*
  - *Test Scores*
  - *Advising records*
  - *Educational services received*
  - *Disciplinary actions*
  - *Student photo*
- *Library circulation information.*
- *Trade secrets or intellectual property such as research activities*
- *Location of critical or protected assets*
- *Licensed software*
- *Vulnerability/security information related to a campus or system*
- *Campus attorney-client communications*
- *Employee Information*
  - *Employee net salary*
  - *Home address*
  - *Personal telephone numbers*
  - *Personal email address*
  - *Payment History*
  - *Employee evaluations*
  - *Pre-employment background investigations*
  - *Mother’s maiden name*
  - *Race and ethnicity*
  - *Parents’ and other family members’ names*
  - *Birthplace (City, State, Country)*
  - *Gender*
  - *Marital Status*
  - *Physical description*
  - *Other*

Classification Description: Level 3 - General

Information, which may be designated by your campus as publicly available and/or intended to be provided to the public.

Information at this level requires no specific protective measures but may be subject to appropriate review or disclosure procedures at the discretion of the campus in order to mitigate potential risks.

Disclosure of this information does not expose the CSU to financial loss or jeopardize the security of the CSU's information assets.

REVISION CONTROL Last Revised:

FINAL: 09/28/11 Revision History