

Both information and software applications reside on many memory devices such as computer hard drives, magnetic disks, flash memory devices, CDs and DVDs, PDAs, Zip disks, and USB storage devices.

California Civil Code 1798.29, 1798.82, 1798.84, and 1798.85 regulates the maintenance and dissemination of personal information by state agencies, and requires each agency to keep an accurate account of disclosures of personal information. This code requires all organizations electronically storing personal information on California residents to notify residents if their information is unencrypted and is accessed by someone unauthorized to do so. Other federal and state laws and regulations also govern the handling, storage, and dissemination of confidential information.

Software applications are licensed by agreements that may contain some or all of the following restrictions: proprietary applications use; limited quantity of permitted installations; limited quantity of concurrent users; expiration periods; and/or redistribution prohibitions.

Information about this form

Data sanitization is the process of deliberately, permanently, and irreversibly removing or destroying the data stored on a memory device. A device that has been sanitized has no usable residual data remaining and even advanced forensic tools should never be able to recover erased data.

All memory devices must be sanitized before reassignment to another employee, transfer between departments or divisions, disposal, or donation to another agency.

Instructions for Departments

- Departments are responsible for ensuring that all memory devices moved, transferred, donated, or disposed are data sanitized prior to the action.
- Departments must contact their assigned Information Technology Consultant or ITS to arrange for the data sanitization.
- No University property will be transferred, donated, or disposed by Property Management without this completed form.
- For equipment that is transferred to another employee or another department, retain a signed copy of this form in the event it is required for future information security audits.

Instructions for Information Technology Services and Information Technology Consultants

- All individuals responsible for data sanitization must read and follow sanitization guidelines as outlined in ITS-1021-G User Guidelines for Data Sanitization.
- All individuals performing the data sanitization procedure must complete and sign one copy of this form for each memory device sanitized.
- All individuals performing the data sanitization procedure for a group of memory devices (e.g., computer labs, TEC rooms, Baseline replacement) must complete and sign one copy of this form for all devices in the group.
- The signed form must be submitted to Property Management for devices being disposed or donated.
- The signed form must be returned to the department for devices being transferred or reallocated to new users.

Instructions for Property Management

- Proceed with no disposals or donations of electronic memory devices until receiving this signed form.
- Attach a copy of this form to the Property Disposal forms in the event it is required for future information security audits.

Contact Information *(To be completed by the Department)*

Department	Equipment Location
Contact Name	Contact Extension
Reason for Data Sanitization	
Redeployment <input type="checkbox"/> Transfer <input type="checkbox"/> Donation <input type="checkbox"/> Disposal <input type="checkbox"/>	

System Information *(to be completed by ITS or ITC)*

Equipment Description	Quantity <i>(if more than one device)</i>
State Tag Number	Serial Number
Sanitization Method	Date Sanitized
Sanitized By	Extension



Electronic Data Sanitization Verification



By signing this form, I certify that I have read, understood, and followed all the data sanitization procedures outlined in ITS-1021-G User Guidelines for Data Sanitization that are appropriate for the above described equipment. I further verify that all data, programs, software applications, and operating systems have been removed, as required, from this computer or media device in accordance with these procedures and information security best practices.

Print Name: _____

Signature: _____ Date: _____

OFFICE USE ONLY

Signed form returned to:	Date Sent	Date Received
<input type="checkbox"/> Property (Disposal/donation) <input type="checkbox"/> Requesting Department (Transfer/ reassignment)		