# Standard: Asset Control

## Executive Summary

The Asset Control Standard defines the requirements for controlling and ensuring all SJSU computing hardware, software, and confidential assets are identified, assigned a Steward, and classified. Assets include, but not limited to all endpoint machines (desktops, laptops, tablets), in addition to all software, servers, confidential data, and supporting network infrastructure devices. Each campus IT department is responsible for producing and maintaining an inventory of their important and critical assets. The assets should first be identified and then maintained in the inventory list. The asset inventory must include all information necessary in order to recover from a natural disaster, including asset type, campus department, physical and data location, backup information, sensitive information contained in asset, and criticality to the IT campus department. The IT Departments must compile and annually update a campus unit inventory of the major SJSU information assets through the annual Risk Assessment process.

# Information Security Standards

## Asset Control

| | | | | | |
|---|---|---|---|---|---|
| Standard # | IS-AC | Effective Date | 11/10/2015 | Email | security@sjsu.edu |
| Version | 3.0 | Contact | Mike Cook | Phone | 408-924-1705 |

### Revision History

| Date | Action |
|---|---|
| 5/26/2014 | Draft sent to Mike |
| 9/2/2015 | Updates – Michael Cook, Information Security Officer |
| 1/22/2015 | Reviewed. Added suggestions and comments. Hien Huynh |
| 2/9/2015 | Updates – Michael Cook, Information Security Officer |
| 11/10/2015 | Incorporated changes from campus constituents – Distributed to Campus. |

## Table of Contents

## Introduction and Purpose

This standard defines the requirements for controlling all San Jose State University (SJSU) computing hardware, software, and confidential assets are identified, assigned a Steward, and classified. Assets include, but are not limited to all endpoint machines (desktops, laptops, tablets), in addition to all software, servers, confidential data and supporting network infrastructure devices

## Scope

This standard applies to all SJSU State, Self-Fund, and Auxiliary ("campus") computer systems and facilities, with a target audience of SJSU Information Technology employees and partners.

## Standard

### Inventory of Assets

Each campus IT department is responsible for producing and maintaining an inventory of their important and critical assets. The important assets should first be identified and then maintained in the inventory list. This list shall include all workstations, servers, laptops and mobile tablets purchased by or for the department.

#### Tracking of Authorized Hardware Assets

Each campus department will actively inventory and track all hardware (desktop, laptop, tablet and servers) devices for as long as they are in the possession of the University.

#### Asset Inventory Contents

An inventory of all SJSU critical assets must be maintained. The asset inventory must include all information necessary in order to recover from a natural disaster, including asset type, campus department, physical and data location, backup information, sensitive information contained in asset, and criticality to the campus department.

#### Asset Inventory for Information

Each department must compile and annually update a campus unit inventory of the major SJSU information assets through the annual Risk Assessment process.

#### Controlling Inventory

SJSU Equipment Custodians must maintain perpetual inventory control, a record of the new location and new Equipment Custodian of all equipment issued to others, and physical security over the equipment in their possession.

#### Hardware and Software Procurement

All hardware and software must be procured in accordance with the Software Procurement and Hardware Procurement Security Standard.

#### Equipment Tracking

All SJSU computer and network equipment must have a unique computer-readable identifier attached to it such that physical inventories can be efficiently conducted. All equipment with purchase price in excess of $5000 must be tagged with a state property tag as issued by the Property Office. All computing equipment (desktops, laptops, tablets and servers) must be

issued either a state property tag or an IT Services property tag as issued by the Information Security Office.

## Ownership of Data

All information and assets associated with information processing facilities should be owned by a designated part of the organization.

### Information Ownership

All production information possessed by or used by a particular campus unit must have a designated Information Owner who is responsible for determining appropriate sensitivity classifications and criticality ratings, making decisions about who can access the information, and ensuring that appropriate controls are utilized in the storage, handling, distribution, and regular usage of information.

### Information Asset Control

Information Owners and Information Systems Department Managers must specifically assign responsibility for the control measures protecting every major SJSU information asset.

### File and Message Ownership

SJSU has legal ownership of the contents of all files and messages stored or transmitted on its computer and network systems, and reserves the right to access this information without prior notice whenever there is a genuine business or legal need, or investigation requirement.

### IT Department Ownership Responsibility

With the exception of operational computer and network information, the campus IT Department must not be the Owner of any production business information except for information specifically relating to computing operations (i.e. Networking, Configuration, etc.).

### Information Custodian

Each significant type of production information must have a designated Custodian who will properly protect SJSU information in keeping with the designated Information Owner's access control, data sensitivity, and data criticality instructions.

### Information Custodian Responsibilities

Information Custodians are responsible for defining specific control procedures, administering information access controls, implementing and maintaining cost-effective information control measures, and providing recovery capabilities. These activities must be consistent with both SJSU information security standards and other internal campus requirements where necessary, as well as with the instructions of Information Owners.

### Information User Responsibilities

All users of SJSU information must comply with the control requirements specified by the information's Owner and/or Custodian.

### Information Ownership Delegation

An Information Owner's responsibility for the specification of appropriate information controls may not be delegated to service providers outside SJSU.