Standard: Electronic and Digital Signatures

Executive Summary

The Electronic and Digital Signature Standard defines the requirements for the usage of electronic and digital signatures both internally within San Jose State University and externally between San Jose State University, its Auxiliaries and outside entities.

Information Security Standards

Electronic and Digital Signature

Standard #	EDS	Effective Date	2/13/2017	Email	security@sjsu.edu
Version	1.0	Contact	Mike Cook	Phone	408-924-1705

Revision History

Date	Action
2/7/2017	Final Draft/Forum Input Added/Release Version Finalized

Table of Contents

Introduction and Purpose

This standard defines the requirements for Electronic and Digital Signatures at San Jose State University (SJSU). In compliance with CSU Information Security Policy 8100.0, Electronic and Digital Signatures, and CSU Electronic and Digital Signatures Standards and Procedures, 8100.S01, SJSU is permitted to use electronic and digital signatures in lieu of handwritten signatures provided they conform to the terms set forth in the policy and the standard.

Scope

This standard applies to all SJSU State, Self-Fund, and Auxiliary ("campus") departments.

Background

The Federal Electronic Signatures in Global and National Commerce Act (Public Law No: 106-229) went into effect on October 1, 2000 and gives electronic contracts the same weight as those executed on paper. Methods may include simply pressing an 'I Accept' button, use of digital certificates, smart cards, and biometrics. Computer generated signatures may be implemented using various methodologies depending on the risks associated with the transaction.

The CSU Electronic and Digital Signature Policy 8100.0 permits the use of electronic or digital signatures in lieu of handwritten; (Wet); signatures. Usage of electronic or digital signatures is at the option of an individual campus/department or the Chancellor's Office provided they conform to the terms set forth.

Refer to the CSU Electronic and Digital Signature Policy 8100.0 and CSU Electronic and Digital Signature Standards and Procedures 8100.S01 for appropriate definitions of terms used in this guideline.

Definitions

Digital Signature

An electronic identifier, key, or file, which when added to a message, allows the recipient to verify the signer and whether the initial message has been altered or the signature forged since the transformation was made. Often, digital signatures are accompanied by electronic signatures.

Electronic Signature

Is an electronic sound (e.g., audio files of a person's voice) or symbol (e.g., a graphic representation of a person in JPEG file) attached to a message with the intent to sign the record. A digitally reproduced (e.g. scanned) physical signature is a common example.

Standard

Classification of Digital Signatures

As digital authenticity mechanisms, digital signatures issued or created by SJSU employees as part of their job duties are considered property of the CSU and are for University business only. Private keys used for digital signatures are considered 'Level 1' confidential data whose unauthorized use, access, disclosure, acquisition, modification, loss, or deletion could result in severe damages to the CSU, its students, its employees, or its customers.

Digital Signatures Using Self-Signed Certificates

Electronic signatures (i.e. scanned images of signatures) for low risk documents, may make use of Self-Signed certificates only when used internally to the campus at the discretion of the department accepting the completed document.

All documents signed for external and high-risk internal purposes must make use of digital signatures backed by an external signatory authority. Such authorities must be approved by the California Secretary of State (i.e. InCommon, Docusign) and must not be backed by self-signed or self-created certificates. SJSU Employees shall not use Self-Signed certificates to digitally sign documents including those generated by Adobe Acrobat for high-risk documents, or documents with any third party. Please contact the Information Security Office for further information or to obtain a compliant digital certificate.

Authorized Software for Agreements within SJSU and/or its Auxiliaries - Internal Use

Electronic signatures (scanned images of a signature) are permitted for the following:

- Internal campus or Chancellor's Office uses involving low risk forms, letters, requisitions, surveys, etc.
    - Departments accepting documents may choose to accept or deny electronic signatures at their discretion, based on level of risk from authentication errors.

Digital signatures (Docusign) are required for the following:

- Records or documents where a signature is required by federal law, California law, or CSU Policy.
- Records or documents exchanged with external third parties.
- Internal documents whenever the level of risk from authentication errors is high. (i.e. CMS System Access Form)

Authorized Software for High Risk Agreements and with Third Parties

SJSU has authorized the usage of DocuSign as the primary mechanism for providing Digital Signatures for high risk agreements or those with external entities.

All other Digital and Electronic signature methods, including Adobe Sign/Echosign/Acrobat, are prohibited for use with third parties and on high-risk documents without prior authorization from the Vice President for Administration and Finance/Chief Financial Officer and Information Security Office (ISO).

The Information Security Office shall ensure compliance of authorized software based on authorization from the California Secretary of State and conform to technologies capable of creating digital signatures as set forth in California Government Code Section 16.5.

1. It is unique to the person using it;
2. It is capable of verification;

3. It is under the sole control of the person using it;
4. It is linked to data in such a manner that if the data are changed, the digital signature is invalidated; and
5. It conforms to regulations adopted by the Secretary of State – California Code of Regulations Title 2, Division 7, Chapter 10.

Maintenance and Recordkeeping

A review of the campus electronic and digital signature standard will be conducted periodically, but no less than every three years, by the Vice President for Administration and Finance/Chief Financial Officer and Information Security Officer. This will include an evaluation of the electronic and digital signature use and tools to determine whether any applicable legal, business, or data requirements have changed. A determination will be made as to the continued appropriateness of the risk assessment and electronic or digital signature implementation method.

A record of this review will be documented and filed as part of the official record for the electronic and digital signature maintained by the Information Security Office. If as a result of the periodic review the risk level changes, a new risk assessment must be completed, including review and approval.

At this time, all documents internal and external have been authorized for the usage of electronic signatures with the exception of especially high-risk new hire documentation as specified by Human Resources (I-9, etc.). Please contact Human Resources for more information.