SAN FRANCISCO
STATE UNIVERSITY

Electronic Signatures Practice Directive

Division: Administration & Finance
Department: Information Technology Services
Contact Information: Nish Malik / Associate Vice President and Chief Information Officer, Information Technology Services / (415) 405-4105 / nish@sfsu.edu
Effective Date: September 4, 2018
Revised Date:

DRAFT

Authority:

ICSUAM 8100.00 Electronic and Digital Signatures

CSU Electronic and Digital Signatures Standards and Procedures, 8100.S01

Confidential Data Practice Directive

Responsible Use Practice Directive

Password Practice Directive

Objective:

This Practice Directive will provide guidance to the campus on the appropriate use of electronic signatures. This guidance applies to all faculty and staff at San Francisco State University.

Statement:

I. Appropriate Use of Electronic Signatures

San Francisco State University has elected to use electronic signatures for campus-approved University business processes. Per ICSUAM 8100.00, the campus has developed an Electronic Signature Risk Assessment procedure to identify, evaluate, and document where electronic signatures are permitted. Electronic signatures must only be used on documents that have been approved through the Electronic Signature Risk Assessment.

DRAFT

DocuSign is the approved campuswide electronic signature solution. All faculty and staff will have access to a DocuSign account. The account shall only be utilized for University business purposes and must not be used for personal transactions.

Electronic signatures shall not be used on forms containing Level 1 (Confidential) data.

Electronic signatures are not appropriate for documents that are external (involve parties other than San Francisco State University faculty and staff) or that are considered to be high risk (see section III of this Practice Directive).

II. Business Process Ownership

Business processes and associated documents are managed by campus process owners. The department that owns a particular business process is the only entity that may modify or upload the document for use in DocuSign. Department business process owners are responsible for initiating an Electronic Signature Risk Assessment (see section III of this Practice Directive) for the use of electronic signatures.

III. Electronic Signature Risk Assessments

The business process owner initiates and is directly involved with the Electronic Signature Risk Assessment process. During the Electronic Signature Risk Assessment, the following topics will be considered:

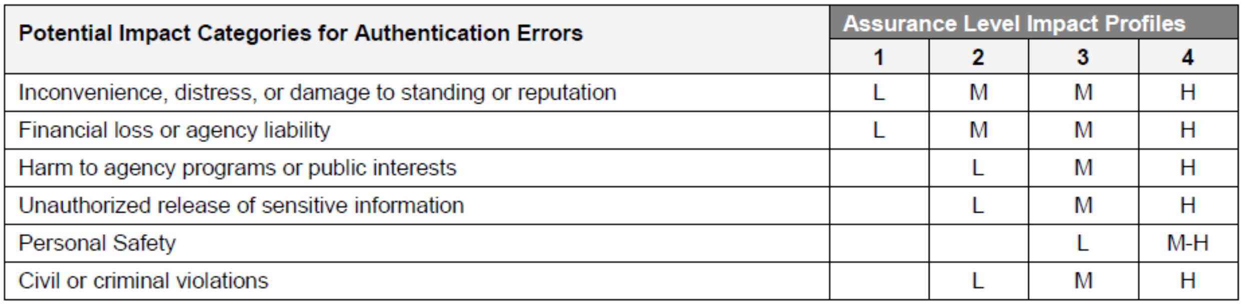
a. The purpose and intent of the document;

b. The parties involved;

c. The routing of the document; and

d. The contents of the document and any other associated attachments.

The Electronic Signature Risk Assessment will determine whether the process and associated documents in question are considered to be low, moderate, or high risk. Six risk impact categories, along with the likelihood of occurrence and potential mitigating factors, are used to assess each form:



Potential Impact Categories for Authentication Errors	Assurance Level Impact Profiles			
	1	2	3	4
Inconvenience, distress, or damage to standing or reputation	L	M	M	H
Financial loss or agency liability	L	M	M	H
Harm to agency programs or public interests		L	M	H
Unauthorized release of sensitive information		L	M	H
Personal Safety			L	M-H
Civil or criminal violations		L	M	H

CSU Electronic and Digital Signatures Standards and Procedures, 8100.S01, Section 6.0, Table 1 - Maximum Potential Impacts for Each Assurance Level.

The campus has determined that, because faculty and staff will authenticate their identity through single sign-on, there is a “**Level 3**: high confidence in the asserted identity’s validity.”[1] Therefore, should any of these risk impact categories receive a rating of high, the document will not be permitted to be used with electronic signatures. If all categories receive a risk rating of low to moderate, the document will be

[1] See CSU Electronic and Digital Signatures Standards and Procedures, 8100.S01, Section 6.0.

approved for use with electronic signatures. The campus may then begin utilizing electronic signatures on that particular document.

IV. Record Storage and Maintenance

Departments shall continue to maintain their records in accordance with the appropriate record retention policy and ITS-recommended file storage solutions. DocuSign shall not be used as a file storage solution.

Upon the completion of the transaction, the responsible department(s) should download both the completed document and any supporting documents for storage in accordance with best practices and in a way that is easily auditable. It is also recommended that the department download the accompanying certificate of completion, which will act as a supporting document and provide a digital audit trail.

V. Account Access and Management

San Francisco State University staff and faculty will be able to utilize electronic signatures through DocuSign by logging in with their SF State ID and password.

As a best practice, users should set up their signature the first time they log in and should not alter their defined signature once it has been created.

For consistency, users should utilize the same name used for University business purposes.

Non-Compliance:

Noncompliance with applicable policies and/or practices may result in removal of DocuSign account access. In addition, disciplinary action may be applicable under other University policies, guidelines, implementing procedures, or collective bargaining agreements.

Procedures:

Please visit the DocuSign web page for more information and help guides (link to be provided when website goes live).

Searchable Words:

Electronic signature, DocuSign, Digital signature.

DRAFT