



Security Matrix: Authorized Tool for External Parties

San Francisco State University has authorized the usage of DocuSign as the approved electronic signature tool for transactions with external parties. The security matrix below provides best practices for various types of University processes that involve external parties along with their associated risk levels. When signing documents that involve an external party, please refer to the security matrix and apply the recommended security control based on the risk level for your documents. Please note that if an external party sends a document to an authorized SF State employee for signature, DocuSign remains the preferred tool to complete the transaction.



Risk Level	Low	Medium	High
Document Type	Operating process documents	Operating process documents with confidential information	Contractual and legally binding documents*
Use Case Examples	<ul style="list-style-type: none"> • Employment Offer Letter • Liability Waiver Form • Donor Intent Form 	<ul style="list-style-type: none"> • HR New Hire Paperwork • HR Honorarium Payment Request 	<ul style="list-style-type: none"> • Housing Lease Agreements or Conference Services Contracts • International Recruiting Services Agreements • Grant / Award Agreements
Authorized Tool	DocuSign	DocuSign	DocuSign
Proposed Security Control (SF State initiated)	Automatic self-expiring link to single specific email address**	Automatic self-expiring link to single specific email address	Automatic self-expiring link to single specific email address + access code***

* It is important for the sender to verify with the external party that they will accept electronic signatures via DocuSign.

**DocuSign automatically provides a self-expiring link ([expires after 5 clicks or 48 hours](#)) for email notifications that don't have an access code assigned or SSO login.

***[DocuSign Access Code option](#): The sender must provide an access code to the recipient for them to access the document. The code may be relayed in any way that the sender wishes, such as by phone, a messaging platform, or Zoom. The addition of the access code is meant to simulate two-factor authentication, so the access code should not be provided to the same email address that the self-expiring link has been sent to.