STATE MODEL
CLOUD COMPUTING SERVICES SPECIAL PROVISIONS
(Software as a Service)

THESE SPECIAL PROVISIONS ARE ONLY TO BE USED FOR SOFTWARE AS A SERVICE (SaaS), AS DEFINED BELOW. THESE SPECIAL PROVISIONS ARE TO BE ATTACHED TO THE GENERAL PROVISIONS – INFORMATION TECHNOLOGY AND ACCOMPANIED BY, AT MINIMUM, A STATEMENT OF WORK (SOW) AND SERVICE LEVEL AGREEMENT (SLA). STATE AGENCIES MUST FIRST:

A. CLASSIFY THEIR DATA PURSUANT TO THE CALIFORNIA STATE ADMINISTRATIVE MANUAL (SAM) 5305.5;

B. CONSIDER THE FACTORS TO BE TAKEN INTO ACCOUNT WHEN SELECTING A PARTICULAR TECHNOLOGICAL APPROACH, IN ACCORDANCE WITH SAM 4981.1, 4983 AND 4983.1 AND THEN;

C. MODIFY THESE SPECIAL PROVISIONS THROUGH THE SOW AND/OR SLA TO MEET THE NEEDS OF EACH ACQUISITION.

1. DEFINITIONS:

a. “Authorized Persons” means the Service Provider’s employees, Contractors, subcontractors or other agents who need to access the State’s Data to enable the Service Provider to perform the services required.

b. “Data Breach” means the unauthorized access that results in the use, disclosure, destruction, modification, loss or theft of the State’s unencrypted Personal Data or Non-Public Data.

c. “Individually Identifiable Health Information” means Information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

d. “Non-Public Data” means data, other than Personal Data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the State because it contains information that is exempt by statute, regulation or policy from access by the general public as public information.

e. “Personal Data” means data that includes information relating to a person that identifies the person by name and has any of the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver’s license, passport); financial account information, including account number, credit or debit card numbers; or protected health information (PHI) relating to a person.

f. “Protected Health Information” (PHI) means Individually Identifiable Health Information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA) as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer.

g. Software-as-a-Service (SaaS) means the capability provided to the consumer to use the Service Provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user- specific application configuration settings.

h. “State Data” means all data created or in any way originating with the State, and all data that is the output of computer processing of or other electronic manipulation of any data that was created by or in any way originated with the State, whether such data or output is stored on the State’s hardware, the Service Provider’s hardware or exists in any system owned, maintained or otherwise controlled by the State or by the Service Provider.

i. “State Identified Contact” means the person or persons designated in writing by the State to receive Security Incident or Data Breach notification.

j. “Security Incident” means the potentially unauthorized access to Personal Data or Non-Public Data the Service Provider believes could reasonably result in the use, disclosure or theft of the State’s unencrypted Personal Data or Non-Public Data within the possession or control of the Service Provider. A Security Incident may or may not turn into a Data Breach.

k. “Service Level Agreement” (SLA) means a written agreement between both the State and the Service Provider that is subject to the terms and conditions in this document that unless otherwise agreed to includes (1) the technical service level performance promises, (i.e. metrics for performance and intervals for measure), (2) description of service quality, (3) identification of roles and responsibilities, (4) security responsibilities and notice requirements, how disputes are discovered and addressed, and (6) any remedies for performance failures.

l. “Service Provider” means the Contractor and its employees, subcontractors, agents and affiliates who are providing the services agreed to under the Contract.

m. “Statement of Work” (SOW) means a written statement in a solicitation document or Contract that describes the State’s service needs and expectations.

2. DATA OWNERSHIP:

The State will own all right, title and interest in State Data that is related to the services provided by this Contract. The Service Provider shall not access State user accounts or State Data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Contract, (4) at the State’s written request or (5) as required by law.

3. DATA PROTECTION:

Protection of personal privacy and data shall be an integral part of the business activities of the Service Provider to ensure there is no inappropriate or unauthorized use of State information at any time. To this end, the Service Provider shall safeguard the confidentiality, integrity and availability of State information within its control and comply with the following conditions:

a. In addition to the Compliance with Statues and Regulations provisions set forth in the General Provisions – Information Technology
   i. The California Information Practices Act (Civil Code Sections 1798 et seq).
   ii. Security provisions of the California State Administrative Manual (Chapters 5100 and 5300) and the California Statewide Information Management Manual (Sections 58C, 58D, 66B, 5305A, 5310A and B, 5325A and B, 5330A, B and C, 5340A, B and C, 5360B)
   iii. Privacy provisions of the Federal Privacy Act of 1974.

b. All State Data obtained by the Service Provider within its control in the performance of this Contract shall become and remain the property of the State.

c. All Personal Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Service Provider is responsible for encryption of the Personal Data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the SOW and/or SLA, or otherwise made a part of this Contract.

Encryption of Data at Rest: The Service Provider shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Personal Data and Non-Public Data, unless the State approves the storage of Personal Data on a Service Provider portable device in order to accomplish work as defined in the SOW and/or SLA.

d. Unless otherwise stipulated, it is the State’s responsibility to identify data it deems as Non-Public Data to the Service Provider. The level of protection and encryption for all Non-Public Data shall be identified and made a part of this Contract.

e. At no time shall any data or processes — which either belong to or are intended for the use of State or its officers, agents or employees — be copied, disclosed or retained by the Service Provider or any party related to the Service Provider for subsequent use in any transaction without the express written consent of the State.

f. The Service Provider shall not use any information collected in connection with the service issued from this proposal for any purpose other than fulfilling the service.

4. DATA LOCATION:

The Service Provider shall provide its services to the State and its end users solely from data centers in the continental United States. Storage of State Data at rest shall be located solely in data centers in the continental United States. The Service Provider shall not allow its personnel or contractors to store State Data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Service Provider shall permit its personnel and contractors to access State Data remotely only as required to provide technical support. The Service Provider may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in this Contract.

5. SECURITY INCIDENT OR DATA BREACH NOTIFICATION:

The Service Provider shall inform the State of any Security Incident or Data Breach.

a. Incident Response: The Service Provider may need to communicate with outside parties regarding a Security Incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing Security Incidents with the State should be handled on an urgent as-needed basis, as part of Service Provider communication and mitigation processes as mutually agreed, defined by law or contained in the Contract.

b. Security Incident Reporting Requirements: The Service Provider shall report a Security Incident to the appropriate State Identified Contact immediately as defined in the SOW and/or SLA.

c. Breach Reporting Requirements: If the Service Provider has actual knowledge of a confirmed Data Breach that affects the security of any State content that is subject to applicable Data Breach notification law, the Service Provider shall (1) promptly notify the appropriate State Identified Contact within 24 hours or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the Data Breach in a timely manner.

6. DATA BREACH RESPONSIBILITIES:

This section only applies when a Data Breach occurs with respect to Personal Data and/or Non-Public Data within the possession or control of a Service Provider.

a. The Service Provider, unless stipulated otherwise in the SOW and/or SLA, shall immediately notify the appropriate State Identified Contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a Security Incident.

b. The Service Provider, unless stipulated otherwise in the SOW and/or SLA, shall promptly notify the appropriate State Identified Contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it confirms that there is or reasonably believes that there has been a Data Breach. The Service Provider shall (1) cooperate with the State as reasonably requested by the State to investigate and resolve the Data Breach; (2) promptly implement necessary remedial measures, if necessary; and (3) document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

c. Service Provider will provide daily updates, or more frequently if required by the State, regarding findings and actions performed by Service Provider to the State's contact or designee until the Data Breach has been effectively resolved to the State's satisfaction.

d. Service Provider shall quarantine the Data Breach, ensure secure access to Data, and repair SaaS as needed in accordance with the SOW and/or SLA. Failure to do so may result in the State exercising its options for assessing damages or other remedies under this Contract.

e. Unless otherwise stipulated in the SOW and/or SLA, if a Data Breach is a direct result of the Service Provider's breach of its Contract obligation to encrypt Personal Data and/or Non-Public Data otherwise prevent its release, the Service Provider shall bear the costs associated with (1) the investigation and resolution of the Data Breach; (2) notifications to individuals, regulators or others required by State law; (3) a credit monitoring service required by State (or Federal) law; (4) a website or a toll-free number and call center for affected individuals required by State law; and (5) complete all corrective actions as reasonably determined by the Service Provider based on root cause; all [(1) through (5)] subject to this Contract's Limitation of Liability provision as set forth in the General Provisions – Information Technology.

7. NOTIFICATION OF LEGAL REQUESTS:

The Service Provider shall contact the State upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the State's Data under this Contract, or which in any way might reasonably require access to State's Data. The Service Provider shall not respond to subpoenas, service of process and other legal requests related to the State without first notifying the State, unless prohibited by law from providing such notice. Service Provider agrees to provide its intended responses to the State with adequate time for the State to review, revise and, if necessary, seek a protective order in a court of competent jurisdiction. Service Provider shall not respond to legal requests directed at the State unless authorized in writing to do so by the State.

8. DATA PRESERVATION AND RETRIEVAL:

a. For ninety (90) days prior to the expiration date of this Contract, or upon notice of termination of this Contract, Service Provider shall assist the State in extracting and/or transitioning all State Data in the format determined by the State ("Transition Period").

b. The Transition Period may be modified in the SOW and/or SLA or as agreed upon in writing by the parties in a Contract amendment.

c. During the Transition Period, SaaS and State Data access shall continue to be made available to the State without alteration.

d. Service Provider agrees to compensate the State for damages or losses the State incurs as a result of Service Provider's failure to comply with this section in accordance with the "Limitation of Liability" provision set forth in the General Provisions - Information Technology.

e. The State at its option, may purchase additional transition services as agreed upon in the SOW and/or SLA.

f. During any period of suspension, the Service Provider shall not take any action to intentionally erase any State Data.

g. The Service Provider will impose no fees for access and retrieval of digital content to the State.

h. After termination of the Contract and the prescribed retention period, the Service Provider shall securely dispose of all State Data in all of its forms, such as disk, CD/ DVD, backup tape and paper. State Data shall be permanently deleted and shall not be recoverable, according to NIST-approved methods. Certificates of destruction shall be provided to the State.

9. BACKGROUND CHECKS:

As permitted by law, the Service Provider shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Contract who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or any misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Service Provider shall promote and maintain an awareness of the importance of securing the State's information among the Service Provider's employees and agents.

10. ACCESS TO SECURITY LOGS AND REPORTS:

a. The Service Provider shall provide reports to the State in a format as specified in the SOW and/or SLA and agreed to by both the Service Provider and the State. Reports will include latency statistics, user access, user access IP address, user access history and security logs for all State files related to this Contract.

11. CONTRACT AUDIT:

The Service Provider shall allow the State to audit conformance to the Contract terms. The State may perform this audit or Contract with a third party at its discretion and at the State's expense.

12. DATA CENTER AUDIT:

The Service Provider shall undergo an annual Statement on Standards for Attestation Engagements (SSAE) No. 16 Service Organization Control (SOC) 2 Type II audit of its data centers at its own expense. The Service Provider shall provide a redacted version of the audit report and Contractor's plan to correct any negative findings upon request. The Service Provider may remove its proprietary information from the redacted version.

13. CHANGE CONTROL AND ADVANCE NOTICE:

The Service Provider shall give advance notice (as agreed to by the parties and included in the SOW and/or SLA) to the State of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware ware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

14. SECURITY PROCESSES:

The Service Provider shall disclose its non-proprietary security processes and technical limitations to the State such that adequate protection and flexibility can be attained between the State and the Service Provider. The State and the Service Provider shall understand each other's roles and responsibilities, which shall be set forth in the SOW and/or SLA.

15. NON-DISCLOSURE AND SEPARATION OF DUTIES:

The Service Provider shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, including those that may be required by the State, and limit staff knowledge of State Data to that which is absolutely necessary to perform job duties.

16. IMPORT AND EXPORT OF DATA:

The State shall have the ability to import or export data in whole or in part at its discretion without interference from the Service Provider. This includes the ability for the State to import or export data to or from other Service Providers.

17. RESPONSIBILITIES AND UPTIME GUARANTEE:

The Service Provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environment are the responsibility of the Service Provider. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and shall provide service to customers as defined in the SOW and/or SLA.

18. STRATEGIC BUSINESS PARTNER DISCLOSURE:

The Service Provider shall identify all of its strategic business partners related to services provided under this Contract, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Service Provider, and who shall be involved in any application development and/or operations.

19. RIGHT TO REMOVE INDIVIDUALS:

The State shall have the right at any time to require the Service Provider remove from interaction with State any Service Provider representative who the State believes is detrimental to its working relationship with the Service Provider. The State shall provide the Service Provider with notice of its determination, and the reasons it requests the removal. If the State signifies that a potential security violation exists with respect to the request, the Service Provider shall immediately remove such individual. The Service Provider shall not assign the person to any aspect of the Contract or future work orders without the State's consent.

20. BUSINESS CONTINUITY AND DISASTER RECOVERY:

The Service Provider shall provide a business continuity and disaster recovery plan upon request and shall ensure that it achieves the State's Recovery Time Objective (RTO), as agreed to by the parties and set forth in the SOW and/or SLA.

a. In the event of disaster or catastrophic failure that results in significant State Data loss or extended loss of access to State Data, Service Provider shall notify the State by the fastest means available and also in writing, with additional notification provided to the Chief Information Security Officer or designee of the Contracting agency. Service Provider shall provide such notification within twenty-four (24) hours after Service Provider reasonably believes there has been such a disaster or catastrophic failure. In the notification, Service Provider shall inform the State of:
   - i. The scale and quantity of the State Data loss;
   - ii. What Service Provider has done or will do to recover the State Data and mitigate any deleterious effect of the State Data loss; and
   - iii. What corrective action Service Provider has taken or will take to prevent future Data loss.
   - iv. If Service Provider fails to respond immediately and remedy the failure, the State may exercise its options for assessing damages or other remedies under this Contract.

b. Service Provider shall restore continuity of SaaS, restore State Data in accordance with the RTO as set forth in the SOW and/or SLA, restore accessibility of State Data, and repair SaaS as needed to meet the performance requirements stated in the SOW and/or SLA. Failure to do so may result in the State exercising its options for assessing damages or other remedies under this Contract.

c. Service Provider shall conduct an investigation of the disaster or catastrophic failure and shall share the report of the investigation with the State. The State and/or its authorized agents shall have the right to lead (if required by law) or participate in the investigation. Service Provider shall cooperate fully with the State, its agents and law enforcement.

21. COMPLIANCE WITH ACCESSIBILITY STANARDS:

The Service Provider shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973.

22. WEB SERVICES:

The Service Provider shall use Web services exclusively to interface with State Data in near real time when possible.

STATEMENT OF WORK AND SERVICE LEVEL AGREEMENT

I. Service Delivery Sites

- Services shall be provided remotely over the telephone, electronic mail or online webshare to the Monterey County Information Technology Department.
- The service delivery site shall be the Monterey County Information Technology Department (ITD) Facility, 1590 Moffett Street, Salinas, California 93905.

II. Scope of Services

A. CONTRACTOR shall provide the COUNTY with DocuSign Enterprise Pro Software for Government as a Service (SaaS) electronic signature service, with capabilities that include:

1. Flexible, mobile workflows support for agreement or approval processes.
2. Visibility and control across all of COUNTY's accounts and users.
3. 99.99% platform availability and peak performance at any scale.
4. Application AES[1] 256 encryption and security certification such as ISO27001, AICPA[2] SOC[3] 1 and 2, xDTM[4] and PCI[5] DSS[6].
5. Full digital audit trail for compliance and legal enforceability.

In addition, the software shall have all of the features identified with a checkmark (✓) in Exhibit A, including DocuSign Product Features Set, plus the SharePoint Connector that integrates the DocuSign with SharePoint Online Document Libraries.

B. CONTRACTOR shall provide the COUNTY with the capability to issue DocuSign Enterprise Pro for Government Envelopes with Adoption Accelerator. Adoption Accelerator allows for unlimited overage for year one.

C. CONTRACTOR shall provide the COUNTY with DocuSign Adoption Consulting services, as described in Exhibit B.

D. CONTRACTOR shall provide the COUNTY with assistance in configuring Single Sign On (SSO) with COUNTY's Active Directory Federation Services (ADFS) with Microsoft, as described in Exhibit C.

E. CONTRACTOR shall provide the COUNTY with Premier Support to troubleshoot and resolve issues related to the COUNTY's DocuSign implementation and/or other information technology infrastructure, as described in Exhibit D.

[1] Advanced Encryption Standard
[2] American Institute of Certified Public Accountants, Inc.
[3] System and Organization Controls
[4] Digital Transaction Management
[5] Payment Card Industry
[6] Data Security Standard

F. CONTRACTOR warrants that it has the necessary qualifications, certifications, and experience to provide the implementation, support services and the services described in this Statement of Work and Service Level Agreement, including Exhibits A through D.

III. Term of the Agreement

The term of this Agreement shall be from October 31, 2018 to October 30, 2019 unless sooner terminated pursuant to the terms of this Agreement.

IV. Payment Provisions

A. For the services described in this Agreement, CONTRACTOR shall bill the COUNTY as follows:

DocuSign Enterprise Pro for Gov Envelopes with Adoption Accelerator	7,500.00
Premier Support	900.00
Adoption Consulting	1,000.00
SSO Implementation Services	0.00
SharePoint Connector	0.00
TOTAL	$9,400.00

The sum total of all billing shall not exceed the **maximum amount of $9,400.00**.

B. Invoices shall be mailed to:

Monterey County Information Technology
1590 Moffett Street
Salinas, CA 93905
Attn: Accounts Payable

EXHIBIT A

Category	Feature Set	Business Pro	Enterprise Pro
DOCUMENT	Extensive File Support	✓	✓
	Automatic Tag Anchoring	✓	✓
	Basic Fields: Name, Signature, Date	✓	✓
	Business Fields: Initial, Company, Title, Email, Text, Data, Check Box	✓	✓
	DocuSign Connect	✓	✓
	PDF Form Conversion	✓	✓
	Form Fields: Radio Button, Drop Down, Note	✓	✓
	Field Formatting, Approve/Decline, Optional Signature	✓	✓
	Advanced Fields: Formula, Custom Field, Third-Party Data, Linked, Conditional, Collaborative	✓	✓
	Signer Attachments	✓	✓
	Data Validation	✓	✓
WORKFLOW	Users per account	Multiple *	Multiple
	Reminders & Notifications	✓	✓
	Serial, Parallel, & Branched Routing	✓	✓
	Comments	✓	✓
	Correct Documents (Adv. Correct)	✓	✓
	Templates	✓	✓
	PowerForms	✓	✓
	Bulk Recipients	✓	✓
	Advanced Workflow: Signing Groups, Supplemental Documents, Workspaces, Field Mark-Up, Draft Watermark, Document Visibility, Auto Navigate, Envelope Custom Metadata, Certified Delivery/Acknowledge receipt	$ *	✓
AUTHENTICATION	Email-Based Authentication	✓	✓
	Access Code Authentication	✓	✓
	Geolocation Capture	✓	✓
	Persistent Authentication	✓	✓
	SMS Authentication	$ *	100/user/yr
	Authentication: ID Check (KBA), Phone, Social, 3rd Party	$ *	$
	eNotary [3rd party fees may apply] (effective 3/26/17)		✓
SIGNATURE	Mobile Applications	✓	✓
	Accessibility	✓	✓
	Multiple Languages (13+ Sending, 43+ Signing)	✓	✓
	In-Person Signing	✓	✓
	Sign on Paper	✓	✓
	Offline Mobile (sign, send)	✓	✓
SERVICES	Fax-Back	$ *	$
	Payments [3rd party fees may apply]	✓ *	✓
REPORTS	Data Export	✓	✓
	Real Time Reporting & Analysis	✓	✓
COMPLIANCE	Compliance: Tamper Sealed Documents, Audit Trail, Certification of Completion, Electronic Record Disclosure	✓	✓
	Advanced Compliance: Masked Fields, Read Only Fields, Locked Templates, Address Book Off		✓
	Access Management (w/ Single Sign-on [SSO])	$ *	✓
	Organization Management		Future: ✓
	Mobile Device Management [3rd Party Services required]		✓

Category	Feature Set	Business Pro	Enterprise Pro
RETENTION	Document Retention Policies		✓
	Email Archiving (BCC)		$
	Document Custody Management		$
	Authoritative Copy		$
CUSTOMIZATION	Shared Templates, Folders, Tags	✓	✓
	Company Branding (1 brand: sender, signer)	✓	✓
	Expanded Branding (multiple brands, resource file)	$ *	✓
	Password Policy Management		✓
	Advanced Roles & Permissions		✓
	Signature Customization: Signature Configure; Signature Pads		✓
	Recipient Language Lock		$
INTEGRATION	Productivity: Google, MSOffice365, Evernote	✓	✓
	Storage: Box, DropBox	✓	✓
	DocuSign Retrieve	$ *	$
	Connectors: CRM, ERP, SharePoint	$ *	$
DEVELOPMENT	API Access (Available in Direct or API plans only)	✓ *	✓
	Developer Sandbox	✓	✓
	QA Sandbox	$ *	1
	High Performance Sandbox		$
REGIONAL MODULES	Advanced Electronic Signatures (AES)	$ *	$
	Qualified Electronic Signatures (QES)	$ *	$
	eHanko, Personal	✓	✓
APPLIANCES	Security Appliance		$
	Signature Appliance		$
	Storage Appliance		$
SERVICE & SUPPORT	Account Manager [Thru Direct Sales]	✓	✓
	Standard Support	✓	✓
	Premium Support Plans: Plus, Premier, Enterprise Premier	$ *	$
	Professional Services	$ *	$
	DocuSign University	$ *	$

✓ = Included in base edition $ = Additional fees may apply *Not available when purchasing online

EXHIBIT B
DOCUSIGN ADOPTION CONSULTING

Accelerate deployment and achieve your desired business outcomes faster.

Onboarding Tools for Rapid Adoption

Our Adoption Consulting program offers a combination of consulting services, onboarding resources, and engaging enablement tools including guided learning paths and a dedicated Adoption Consultant to help get your DocuSign solution live and moving at the same speed as your business.

Benefits of Working with an Adoption Consultant

Trust our DocuSign experts to provide the support you need to make your implementation a success. By combining industry best practices, adoption tools, and the resources gathered from thousands of successful customer engagements into a simple onboarding experience, you're able to drive greater awareness and adoption of DocuSign with your workforce.

Every engagement is led by a dedicated Adoption Consultant that guides you through:

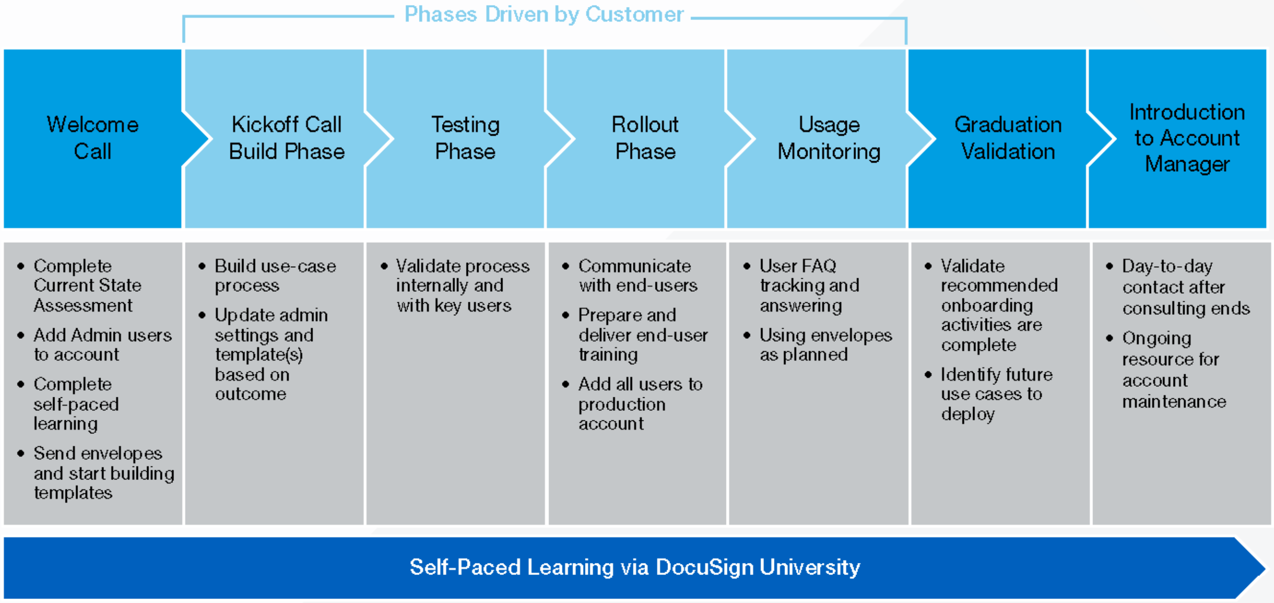
- Initial use case design and optimization
- Business and technical readiness
- Best practices on out-of-the-box configurations
- Mentoring on the product, your roll-out and adoption strategy

In the First 90 Days

What's Included:

- Guidance from 1 dedicated Adoption Consultant
- 10 hrs. of 1:1 consulting
- Login access and guidance through self-paced learning paths
- Recommendations on enablement resources to explore

Our Approach to Adoption Consulting



Phases Driven by Customer

Welcome Call	Kickoff Call Build Phase	Testing Phase	Rollout Phase	Usage Monitoring	Graduation Validation	Introduction to Account Manager
• Complete Current State Assessment • Add Admin users to account • Complete self-paced learning • Send envelopes and start building templates	• Build use-case process • Update admin settings and template(s) based on outcome	• Validate process internally and with key users	• Communicate with end-users • Prepare and deliver end-user training • Add all users to production account	• User FAQ tracking and answering • Using envelopes as planned	• Validate recommended onboarding activities are complete • Identify future use cases to deploy	• Day-to-day contact after consulting ends • Ongoing resource for account maintenance

Self-Paced Learning via DocuSign University

Accelerate Your Business

We realize that a critical step to accelerating your business with DocuSign is often the first one. Our Adoption Consulting service gives you the solid business and technical foundation needed to get started on a successful path to preparing, signing, enacting, and managing agreements with DocuSign.

EXHIBIT C
SINGLE SIGN ON IMPLEMENTATION

OVERVIEW: DocuSign Single Sign On

Single Sign On, also known as Federation, provides a secure way to exchange authentication information between two parties, a Service Provider and an organization's Identity Provider, allowing a single set of credentials to be used to access multiple applications. When an organization enables Single Sign On (SSO) for their DocuSign account, it allows members to use their organization's credentials to access DocuSign.

Project Approach

The approach and tasks to test and enable SSO includes:

1. Determine customer specific SSO requirements
2. Review DocuSign standard SSO functionality
   - DocuSign allows administrators to manage users in a specific email domain.
   - Mandatory Just in Time user provisioning
3. Prepare Organization structure, associated accounts, and Org Admins
4. Review Domain settings
   - Always require login when opening envelopes
   - Prevent unmanaged sign-ups
   - Require all users to authenticate with Identity Provider
5. Present Identity Provider requirements and settings
   - Identity Provider Issuer
   - Security Assertion Markup Language (SAML) Authentication Request URL
   - AuthN Request[7] settings
   - Endpoint URLs
6. Review SAML requirements
   - Claimed email domains
   - Required Attributes
     NameID
     DocuSign User First Name
     DocuSign User Last Name
     User's Email Address
   - Optional Attributes
     AccountID
     PermissionProfileID
     Attribute Mapping
     X509 Certificate
7. Obtain Organization details and setup Demo environment for customer testing
   - Debugging assistance on malformed SAML Assertions.
   - Once testing passes, setup Production Organization.

[7] SAML message that initiates authentication

EXHIBIT D
DOCUSIGN CUSTOMER SUPPORT: PREMIER SUPPORT

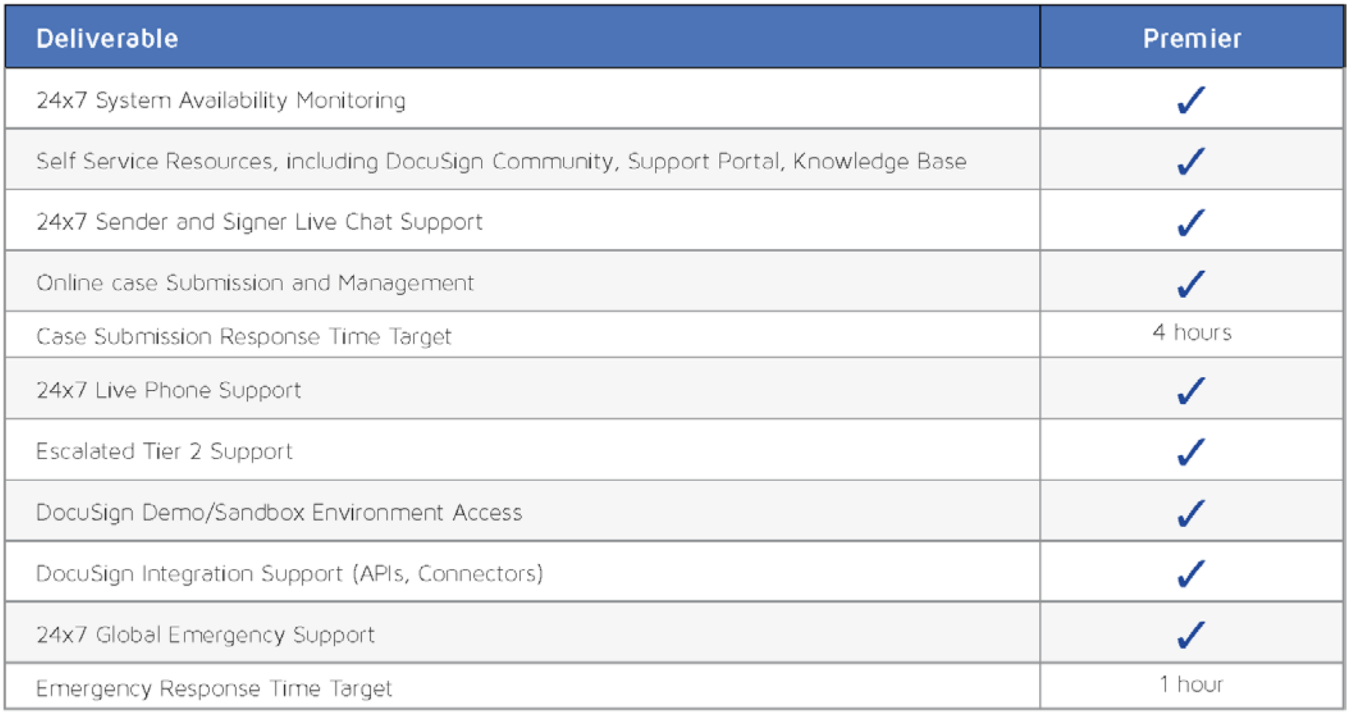
As a global company, your business is running around the clock and around the world. DocuSign Customer Support provides the assistance you need so that you get the results you expect. As an enterprise customer, your business is running around the clock and around the globe. Our industry-leading, global support model is there to back you up, no matter where you do your business.

We provide you access to the expertise you want, whether through our communities, our knowledge base and on-demand training, or our team of experienced technical support professionals, who know you and your solutions.

We provide fast response times to your questions and cases, whether online or by phone, including 24x7 global emergency support. If an issue arises, you can count on rapid response from DocuSign. We provide escalated support and response times within four hours during your business day, helping you keep your business moving.

As a Premier Support customer, you get a committed partner that provides you the business grade support you’d expect while running your critical business processes. Our online case submission and management tools let you keep track of your most urgent questions through resolution. And our knowledge base, communities and online training make it easy for you to get the answers you need quickly.

While DocuSign is powerful as an out-of-the-box solution, integrating with your CRM, ERP, and HRM systems increases the value of those investments. When you integrate DocuSign with your existing business applications, DocuSign Customer Support is there to make sure things go smoothly. Premier Support provides access our demo sandbox as well as experts who understand your specific integration, using our connectors and open APIs, allowing you to get back to business.



Deliverable	Premier
24x7 System Availability Monitoring	✓
Self Service Resources, including DocuSign Community, Support Portal, Knowledge Base	✓
24x7 Sender and Signer Live Chat Support	✓
Online case Submission and Management	✓
Case Submission Response Time Target	4 hours
24x7 Live Phone Support	✓
Escalated Tier 2 Support	✓
DocuSign Demo/Sandbox Environment Access	✓
DocuSign Integration Support (APIs, Connectors)	✓
24x7 Global Emergency Support	✓
Emergency Response Time Target	1 hour

EXHIBIT D
DOCUSIGN CUSTOMER SUPPORT: PREMIER SUPPORT

Deliverable Description:

24x7 System Availability Monitoring – DocuSign Trust Site for real-time system status and notifications

Support Portal and Knowledge Base – Search for answers and submit Support requests

DocuSign Community - Q&A community staffed by DocuSign employees and power users of our product

24x7 Sender and Signer Live Chat Support - Chat Support for simple questions on signing, sending and account management

Online Case Submission and Management – Submit cases online for assistance from our Support Team

24x7 Live Phone Support - Talk to our DocuSign Support Team for technical DocuSign questions, billing inquiries and account support

Escalated Tier 2 Support – Direct access to senior technical resource as part of standard support escalation process.

DocuSign Demo/Sandbox Environment Access – Test your current code against upcoming releases or add your new code to test prior to releasing into production

DocuSign Integration Support (Connectors) – Support for connections to complementary solutions such as Salesforce, Microsoft and Google

24x7 Emergency Support – 1 hour response to Severity 1 technical incidents