1. Sectigo Certificate Manager (SCM).

1.1. Account. Sectigo shall create an account within SCM that Subscriber may use to request Certificates. Access to SCM and login credentials are Confidential Information. Subscriber shall not allow any third party to access SCM and shall be responsible for all orders placed through SCM, regardless of whether the order was approved or authorized by Subscriber.

1.2. License. Subject to the terms herein, Sectigo hereby grants Subscriber a limited, revocable, non-exclusive, non-transferable license to use SCM during the Term to request, revoke, and manage Certificates issued by Sectigo to Subscriber. All rights not expressly granted herein are reserved to Sectigo.

1.3. Limitations; Restrictions. Subscriber may not transfer or provide access to SCM to a third party. Sectigo shall host SCM at all times within its infrastructure. Subscriber shall access SCM only by connecting remotely over the Internet to Sectigo's servers. Subscriber shall not attempt to copy, reproduce, reverse engineer, disassemble, decompile, customize, translate, or alter SCM or attempt to unlock or by-pass any access prevention device in SCM or have anyone else do so. Subscriber may incorporate APIs included in SCM into its own software, provided that such software is not provided to any third party. Subscriber shall not alter, obscure, amend, or interfere with Certificate agreements presented through SCM. These limitations survive termination of the Agreement.

1.4. Roles. Subscriber shall designate in SCM a natural person (or persons) as an MRAO, a Certificate Approver, and Certificate Requester(s) (collectively, "SCM Administrators"). Unless each designation is revoked by Subscriber deactivating such person's account access privileges, such designation lasts for the greater of: (i) the remaining Term, and (ii) expiration or revocation of all Certificates issued under the Agreement.

1.5. Trial/Beta Services. Sectigo may from time to time, permit Subscriber to register for Trial Services or invite Subscriber to try Beta Services. Subscriber may accept or decline any such invitation in its sole discretion. Trial Services and Beta Services will terminate on the earlier of: (i) the end of the trial or beta period for which Subscriber registered or continues to evaluate such services; or (ii) the start date of the Initial Term for purchased Services previously made available as Trial Services or Beta Services. Trial Services and Beta Services are provided for evaluation purposes and not for production use, are not supported, may contain bugs or errors, and may be subject to additional terms. Trial Services and Beta Services are provided solely and exclusively "AS IS" with no express or implied warranty of any kind. SUBSCRIBER ASSUMES AND UNCONDITIONALLY RELEASES SECTIGO FROM ALL RISKS ASSOCIATED WITH THE USE OF ANY TRIAL SERVICES AND/OR BETA SERVICES. Sectigo may discontinue the Trial Services or Beta Services at any time in its sole discretion. Sectigo does not promise or represent that Beta Services will be made generally available.

1.6. Reporting of Errors. Subscriber shall document and promptly report to Sectigo any errors or malfunctions in the Certificates or SCM. Upon Sectigo's reasonable request, Subscriber shall assist Sectigo in rectifying such errors or malfunctions.

2. Certificates (General).

2.1. Registration. The licenses granted herein are contingent upon Sectigo's successful validation of Subscriber. Subscriber authorizes Sectigo to carry out a background check, a credit check, or both as part of the validation process. Subscriber shall provide additional information reasonably requested by Sectigo.

2.2. Request. When applying for a Certificate, Subscriber shall submit a certificate request in SCM by an individual with the authority to order Certificates on behalf of the entity to be listed in the Certificate.

2.3. Certificate Validation. Subscriber represents and warrants that it shall only request DV, OV, and EV Certificates for domains that are owned or controlled by Subscriber or its Affiliates. Subscriber shall assist, if necessary, Sectigo to validate each Certificate ordered through SCM. When validating orders for Publicly-Trusted Certificates, Sectigo shall follow the processes and procedures in the CPS, which requires among other things that Sectigo perform all domain validation using its DCV system. Sectigo shall not invoice Subscriber for any Certificates failing validation. For Privately-Trusted Certificates, Subscriber shall create internal procedures that set forth its processes for requesting, renewing, and validating each such Certificate, and shall validate all information submitted by Applicants for such Certificates in accordance with such internal procedures prior to issuing the Certificate. Subscriber shall ensure that all personnel performing validation duties for Privately-Trusted Certificates receive and possess sufficient training and skill to perform the validation required for such Certificate.

2.4. Restrictions. Subscriber shall not: (i) impersonate or misrepresent Subscriber's affiliation with any entity, (ii) modify, sub-license, create a derivative work of, or transfer to any non-Affiliate third party any Certificate (except as required to use the Certificate) or the associated Private Key; (iii) install or use an issued Certificate until after Subscriber has reviewed and verified the Certificate data's accuracy; (iv) use a Certificate, if Subscriber reasonably believes 1) any information in the Certificate is, or becomes, incorrect or inaccurate, 2) there is evidence that the Certificate was used to sign Suspect Code, if the Certificate is a Code Signing Certificate, or 3) the Private Key associated with the Public Key contained in the Certificate was misused or compromised; (v) use a Certificate with any on-line control equipment in hazardous environments requiring fail-safe performance where the failure of the Certificate could lead directly to death, personal injury, or severe physical or environmental damage; (vi) use a Certificate, or the associated Private Key, to upload or distribute any files or software that may damage the operation of another's computer; (vii) apply for a Code Signing Certificate if the Public Key in the Certificate is or will be used with a non-Code Signing Certificate; (viii) use a Code Signing Certificate, or the associated Private Key, to sign software that contains Suspect Code; (ix) use the Services to 1) engage in conduct that is offensive, abusive, contrary to public morality, indecent, defamatory, obscene, or menacing, 2) breach the confidence of a third party, 3) cause Sectigo or a third party distress, annoyance, denial of any service, disruption or inconvenience, 4) send unsolicited bulk correspondence or 5) create a Private Key that is substantially similar to a Sectigo or third party's Private Key; (x) make representations regarding the Service to any third party except as agreed to in writing by Sectigo. (xi) take any action that imposes an unreasonably or disproportionately large load on Sectigo's infrastructure; (xii) use or submit a Private Root CA Certificate as the basis, or as part, of an application to have a Private Root CA Certificate become Publicly-Trusted, or even generally trusted outside the Subscriber's own organization; (xiii) create or attempt to create a CA Certificate from the Intermediary CA Certificate or the Private Root CA Certificate; (xiv) sell, rent, lease, license, assign, or otherwise transfer the Intermediary CA Certificate or the Private Root CA Certificate to any third party; (xv) use a Certificate after its expiration or its revocation, or the termination of the Agreement; or (xvi) compromise any Private Key or use a Certificate if Subscriber has reason to believe that such Certificate, or the associated Private Key, has been compromised.

2.5. Revocation. Sectigo may revoke a Certificate for the reasons stated in the CPS. In addition, Sectigo may revoke a Certificate if Sectigo reasonably believes that: (i) Subscriber requests revocation of a Certificate; (ii) if the Agreement or a separate subscriber agreement applicable to the Certificate terminates; (iii) the original Certificate request was not authorized and authorization is not retroactively granted; (iv) Confidential Information related to the Certificate is misused or compromised, or Confidential Information could be disclosed if the Certificate is not revoked; (v) Subscriber violates a material obligation under the Agreement; (vi) Subscriber has used the Certificate contrary to industry standards or applicable laws, rules, or regulations; (vii) the Certificate is being used, directly or indirectly, to engage in illegal or fraudulent activity; (viii) inaccurate or incomplete information is present in the Certificate; (ix) the Certificate was not issued in accordance with the applicable validation guidelines, or the Certificate was issued as a result of fraud or negligence; (x) Sectigo's Certificate operations cease, and Sectigo has not arranged for another certificate authority to provide revocation support for the Certificate; (xi) Sectigo's right to issue Certificates under applicable guidelines has been revoked or terminated; (xii) Subscriber has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of Sectigo's jurisdiction of operation; (xiii) the Certificate was issued to a publisher of Suspect Code or may have been used to sign Suspect Coe; (xiv) the CA Certificate to which the Certificate is chained is revoked, or (xv) the Certificate, if not revoked, will compromise the trust status of Sectigo. Subscriber shall revoke Private End-Entity Certificates by following its internal procedures regarding Private End-Entity Certificates and shall revoke any Private End-Entity Certificate upon Sectigo's written request.

2.6. Discontinued Certificates. Sectigo may modify or discontinue any type of Certificate. Unless the modification or discontinuance is caused by a change in industry standards, Sectigo shall replace any discontinued Certificate type with a similar Certificate.

2.7. Hosting. Sectigo shall generate and host all Private Keys for each CA Certificate created in its secure systems at all times. Subscriber may not remove any Private Key for a CA Certificate from Sectigo's systems for any

reason. All such Private Keys that Sectigo generates are non-exportable.

3. Publicly-Trusted Certificates.

3.1. Publicly-Trusted End-Entity Certificates. Subject to the terms herein, after a Publicly-Trusted Certificate has been successfully validated and issued by Sectigo, Sectigo grants Subscriber a revocable, non-exclusive, non-transferable license to use the issued Certificate: (i) on the server hosting the domain name(s) listed in the Certificate, if the Certificate is a DV Certificate, OV Certificate, or EV Certificate, (ii) to sign and encrypt email messages, if the Certificate is a Client Certificate, (iii) to sign software objects or code, if the Certificate is a Code Signing Certificate, or (iv) to sign PDF documents for Subscriber's legitimate business purposes, if the Certificate is a Document Signing Certificate, until the earlier of expiration or revocation of the Certificate or termination of the Agreement as provided herein.

3.2. Public Intermediary CA Certificates. Subject to the terms herein, and provided Subscriber has purchased and paid for the Public Intermediary CA Certificate, after Sectigo's creation of a Public Intermediary CA Certificate pursuant to the Agreement, Sectigo grants Subscriber a limited, revocable, non-exclusive, non-transferable license during the Term to (i) use the Public Intermediary CA Certificate to sign and issue End-Entity Certificates to Applicants who have passed the validation requirements described in section 2.3, and (ii) download a copy of each Public Intermediary CA Certificate to confirm the validity of each End-Entity Certificate. Each copy of a Public Intermediary CA Certificate must include all copyright notices, restricted rights legends, proprietary markings and the like exactly as they appear on the Certificate delivered by Sectigo. The profile of each Public Intermediary CA Certificate will be finalized by Sectigo, and will include Basic Constraints, Name Constraints, and Policy Constraints (all as defined in RFC-5280), which are intended to limit the useful capability of Subscriber to issue Certificates only for those purposes, domain names, and subject details as are pre-validated by Sectigo. Subscriber expressly agrees that each Public Intermediary CA Certificate (including any related intellectual property rights) is owned by Sectigo or its third-party licensors and will remain the sole and exclusive property of Sectigo and its third-party licensors. No rights or licenses with respect to a Public Intermediary CA Certificate, or in any related patents, trademarks, copyrights and proprietary and trade secret rights, are granted or deemed granted hereunder or in connection herewith, other than those rights expressly granted in the Agreement. Except for Public Intermediary CA Certificate capable of issuing EV Certificates, Subscriber may re-brand Certificates issued from a Public Intermediary CA Certificate with Subscriber's names, brands, marks, logos and graphics ("Branding"), provided that such Branding is approved by Sectigo in writing prior to the dissemination of the branded Certificates and provided that the Branding does not violate or infringe upon any third party's rights, including trademark, copyright, patent, and other intellectual or proprietary rights.

3.3. Subscriber Agreement. The Agreement is the subscriber agreement required by CPS for all Publicly-Trusted Certificates issued to Subscriber and applies to multiple future Certificates requested or issued during the Term.

3.4. Lifecycle. Subscriber may order Publicly-Trusted End-Entity Certificates with lifecycles equal to the lesser of: (i) the maximum lifecycle allowed by the CPS, or industry standards, or (ii) the remaining Term rounded up to a whole year. Sectigo may modify Certificate lifecycles as necessary to comply with changes in industry standards, third parties chained to Sectigo's Root CA Certificates, Sectigo's auditors, and Application Software Suppliers.

3.5. Enterprise EV RA. Subject to Sectigo's sole and absolute discretion and provided Subscriber has a currently valid Sectigo EV Certificate, Sectigo appoints Subscriber as an Enterprise EV RA and grants Subscriber a limited, revocable, non-exclusive, non-transferable license to manage, request, revoke, and assist in the validation of Enterprise EV Certificates for Subscriber's own use. As an Enterprise EV RA, Subscriber shall: (i) follow CABF Standards when validating Enterprise EV Certificates, (ii) validate and approve the issuance of Enterprise EV Certificates (a) only through SCM, (b) only for domains that are owned or directly controlled by Subscriber, and (c) only where the subject of the Enterprise EV Certificate is an organization previously issued a Sectigo EV Certificate, and (iii) not request the issuance of an Enterprise EV Certificate at the third or higher domain levels to any subject other than Subscriber or an Affiliate. Sectigo may revoke Subscriber's appointment as an Enterprise EV RA at any time on written notice to Subscriber, after which Sectigo shall validate all EV Certificates ordered by Subscriber. Subscriber shall not validate or cause to issue top level domain EV Certificates.

3.6. Document Retention. Subscriber shall retain any documentation used to validate an Enterprise EV Certificate for at least two years after the expiration of the Certificate and shall make such documentation available promptly upon Sectigo's written request. Sectigo may inspect, if necessary, Subscriber's validation process with respect to Enterprise EV Certificates by requesting that Subscriber provide electronic documents showing compliance with the CPS. Subscriber shall provide all such documents within five (5) business days. This section survives the Agreement pursuant to section 16.11 (Survival).

4. Private CA Managed Services. This section shall apply provided that Subscriber has purchased and paid for the Private CA Managed Services.

4.1. Private CA Certificates. Subject to the terms herein, after Sectigo's creation of a Private Root CA Certificate or Private Intermediary CA Certificate pursuant to the Agreement, Sectigo grants Subscriber a limited, revocable, non-exclusive, non-transferable license during the Term to: (i) use the Private Root CA Certificate and Private Intermediary CA Certificate to sign and issue Private End-Entity Certificates to Applicants who have passed the validation requirements described in section 2.3, and (ii) download a copy of each Private Root CA Certificate and Private Intermediary CA Certificate to confirm the validity of each Private End-Entity Certificate. Each copy of a Private Intermediary CA Certificate or Private Root CA Certificate must include all copyright notices, restricted rights legends, proprietary markings and the like exactly as they appear on the Certificate delivered by Sectigo.

4.2. Private End-Entity Certificates. Subject to the terms herein, Sectigo grants Subscriber a limited, revocable, non-exclusive, non-transferable license during the Term to use each issued Private End-Entity Certificate on the device, or server hosting the domain name(s), listed in the Private End-Entity Certificate. Subscriber shall validate, issue, and renew all Private End-Entity Certificates through SCM and shall only issue a Private End-Entity Certificate for Subscriber's own use.

4.3. CRL/OCSP Service. Sectigo shall provide and host CRL/OCSP services for Subscriber and shall continue to provide the CRL/OCSP services until the earlier of: (i) termination of the Agreement, and (ii) expiration or revocation of all Private End-Entity Certificates issued under the Agreement.

5. Support.

5.1. Standard. Sectigo shall provide standard Sectigo-branded customer support at no extra charge.

5.2. Premier Support Services. Provided Subscriber purchases and pays for Premier Support Services, Sectigo shall provide the Premier Support Services for the subscription term stated on the Order Form, in accordance with terms of this Agreement and the Addendum available here: https://sectigo.com/uploads/files/SCM-ECA-Addendum-Premier-Support-Services-v1.2.pdf, which is incorporated herein by reference. Sectigo reserves the right to modify the Premier Support Services in its discretion

6. Subscriber Responsibility.

6.1. Obligations. Subscriber warrants, and covenants throughout the Term, to: (i) in connection with the issuance of a Certificate, to provide accurate and complete information at all times to Sectigo in the Certificate request and as otherwise requested; (ii) install and use each DV Certificate, OV Certificate, and EV Certificate 1) only on domains owned or controlled by Subscriber and 2) only on the server(s) accessible at the domain name listed in the Certificate; (iii) review and verify the accuracy of the data in each Certificate prior to installing and using the Certificate, and immediately inform Sectigo if any data listed in a Certificate changes or ceases to be accurate; (iv) be responsible, at Subscriber's expense, for 1) all computers, telecommunication equipment, software, access to the Internet, and communications networks (if any) required to use SCM or Certificates, 2) the conduct of MRAO and all SCM Administrators, and 3) Subscriber's conduct and its website maintenance, operation, development, and content; (v) use one of the following options to generate and protect each Code Signing Certificate and Document Signing Certificate: 1) a trusted platform module (TPM) that generates and secures a key pair and that can document protection of the Private Key through a TPM key attestation; 2) a hardware crypto module with a unit design form factor certified as conforming to at least FIPS 140 Level 2, Common Criteria EAL 4+, or equivalent; or 3) if 1) and 2) are not feasible, another type of hardware storage token with a unit design form factor of SD Card or USB token (not necessarily certified as conformant with FIPS 140 Level 2 or Common Criteria EAL 4+); (vi) use each Document Signing Certificate solely for signing PDF documents in connection with its legitimate business purposes; (vii) promptly inform Sectigo if Subscriber becomes aware of any misuse of the Certificates and

assist Sectigo in preventing, curing, and rectifying any misuse; (viii) take all reasonable measures to assure control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in a Certificate; (ix) immediately cease using a Certificate and the related Private Key and request revocation of the Certificate if 1) any information in the Certificate is or becomes incorrect or inaccurate, or 2) there is any actual or suspected misuse or compromise of the Private Key associated with the Certificate; (x) cease all use of the Certificate and its Private Key upon expiration or revocation of the Certificate; (xi) comply with all regulations, policies, and procedures of its networks while using SCM and Certificates, and obtain and keep in force any authorization, permission or license necessary for Subscriber to use the Certificates and SCM; and (xii) abide all applicable laws, rules, regulations, and guidelines when using SCM and the Certificates.

6.2. Representations. Subscriber represents and warrants that: (i) Subscriber has full power and authority to enter into the Agreement and perform its obligations hereunder; and (ii) Subscriber has all necessary consents to appoint each Certificate Requester and Certificate Approver, and that each Certificate Requester and Certificate Approver has been provided a copy of, or an opportunity to review, the Privacy Policy.

6.3. Compliance. Subscriber shall abide by all applicable laws, regulations, and rules when using SCM and Certificates, including the export and import regulations promulgated by Subscriber's government, the U.S. Dep't of Commerce, the U.S. Dep't of Treasury, and the U.K. Dep't for International Trade. Subscriber is solely responsible for procuring and renewing any required export or import licenses.

7. Pricing and Payment Terms.

7.1. Generally. Subscriber shall pay all applicable fees for the Services before the Services are rendered. For the purchase of Certificates and access to SCM, Subscriber shall pay: (i) the prices listed in the Order Form (for the Initial Term) or renewal Addendum (for a Renewal Term) in accordance with the payment terms in the Agreement, provided Subscriber purchases directly from Sectigo, or (ii) in accordance with the payment terms established between Subscriber and Reseller, provided Subscriber purchases from a Reseller. For each ordered Certificate not listed, Subscriber shall pay the prices listed on the website www.enterprisessl.com or enter into a new order with Sectigo for the purchase of additional Certificates. Subscriber acknowledges and agrees that if Subscriber or Reseller (if Subscriber purchased the Services through Reseller) does not pay Sectigo the applicable fees for the Services, Subscriber may not use the Services, and Sectigo may revoke issued Certificates, for which the applicable fees remain unpaid.

7.2. Deposits. For payments listed as a deposit, Subscriber agrees to make such payments to Sectigo in consideration for the discounted Certificate prices listed therein during the Term. Upon receipt of payment, Sectigo will credit Subscriber's balance with the amount of such payment. All amounts credited to Subscriber's balance will roll-over during each contract year of the Term; however, all amounts credited to Subscriber's balance are non-refundable and may only be used by Subscriber to purchase Certificates during the Term. At the end of the Term, all amounts remaining will be forfeited.

7.3. Subscription Fees. For payments listed as a subscription fee, Subscriber agrees to make such payments to Sectigo in consideration for access to SCM and use of the Certificates listed therein during the Term. All fees are paid annually and in advance. If the Agreement renews automatically, the parties agree that subscription fees for the upcoming Renewal Term may be increased, but only up to a maximum of 5% over the previous year's fees, unless otherwise prohibited by law. All fees are non-refundable, regardless of the number of Certificates actually utilized by Subscriber.

7.4. Taxes. Prices do not include any sales, use, excise, transaction, or similar taxes. If such taxes are applicable, Sectigo will separately state them on the invoice. Except for any taxes on Sectigo's income, Subscriber shall pay all taxes resulting from Subscriber's possession and use of SCM and the Certificates issued under the Agreement.

7.5. Fee Adjustment. In the event of any material increase in Subscriber's, or its Affiliates', use of the Services resulting from an acquisition, merger, or otherwise, the parties shall, upon written notice by Sectigo, negotiate in good faith a proportionate fee adjustment commensurate with the increase in usage.

8. Marketing.

8.1. License. Subject to sections 8 and 9, Sectigo hereby grants Subscriber a non-exclusive, non-transferable, non-sublicensable, royalty-free license during the Term to display Sectigo's trademarks and other marketing material in connection with its use of the Certificates.

8.2. Restrictions. Subscriber shall not publish any marketing material or documentation that refers to Sectigo, its Certificates, or SCM without receiving written prior approval from Sectigo, which Sectigo shall not unreasonably withhold. Subscriber shall use only facts that Sectigo itself uses in its non-confidential written materials when referring to SCM or Certificates.

8.3. Sectigo Marketing. Subscriber grants Sectigo a non-exclusive, non-transferable, non-sublicensable, royalty-free worldwide license during the Term to use Subscriber's name and logo on Sectigo's customer list and marketing materials. The goodwill associated with such use shall inure solely to the benefit of Subscriber.

9. Intellectual Property Rights.

9.1. Sectigo IP Rights. Sectigo retains, and Subscriber shall not obtain or claim, all title, interest, and ownership rights in: (i) the Services, including all techniques and ideas embedded therein; (ii) all copies or derivative works of the Services, regardless of who produced, requested, or suggested the copy or derivative work; (iii) all documentation and marketing materials provided by Sectigo to Subscriber; and (iv) all of Sectigo's copyrights, patent rights, trade secret rights and other proprietary rights. All derivative works or modifications to SCM made or suggested by Subscriber or Sectigo will be owned by Sectigo. Subscriber owns any software incorporating the APIs, but the APIs themselves remain the property of Sectigo.

9.2. Restrictions. The parties shall protect each other's intellectual property, goodwill, and reputation. Subscriber shall not use the Certificates, or Sectigo's trademark, in a way that might diminish or damage Sectigo's reputation, including using the Certificates on a website that infringes the rights of a third party or could be considered associated with a crime. Sectigo may terminate the Agreement or restrict access to SCM or the Certificates if Sectigo reasonably believes that SCM or Certificates are being used to post or make accessible any material that infringes a third party's rights.

10. Confidentiality. The parties agree that: (i) neither party ("Receiving Party") may use or disclose any Confidential Information provided by the other party or its affiliates (the "Disclosing Party") other than for the purpose of performing its obligations under the Agreement, except as allowed herein; (ii) the Receiving Party shall take reasonable measures to prevent unauthorized disclosure of Confidential Information and shall ensure that any person receiving Confidential Information complies with the restrictions in this section; (iii) the Receiving Party may disclose Confidential Information if the information: (a) is already possessed by the Receiving Party before receipt from the Disclosing Party; (b) is or becomes public domain without fault of the Receiving Party; (c) is received by the Receiving Party from a third party who is not under an obligation of confidentiality or a restriction on the use and disclosure of the information; (d) is disclosed in response to the requirements of a law, governmental order, regulation, or legal process if the Receiving Party first gives prior notice to the Disclosing Party of the requirement to disclose the information; or (e) is disclosed under operation of law to the public without a duty of confidentiality; and (iv) a party asserting one of the exceptions to Confidential Information above shall prove the assertion using verifiable documentary evidence.

11. Privacy and Data Protection.

11.1. Privacy Policy. Sectigo shall follow its Privacy Policy when receiving and using information about Subscriber. Sectigo may amend its Privacy Policy at any time in accordance with the process outlined therein. Subject to Section 11.2 below, Sectigo shall use reasonable efforts in protecting Subscriber's information. Subscriber acknowledges that risks remain that are beyond Sectigo's reasonable control.

11.2. Disclosures. Subscriber acknowledges and understands that (i) issued Certificates are embedded with information about Subscriber (such as Subscriber's domain name, jurisdiction of incorporation, or email address), which varies depending on the type Certificate ordered by Subscriber, (ii) issued Certificates may be logged in publicly-accessible Certificate transparency databases for purposes of detecting and preventing phishing attacks and other forms of fraud, and (iii) Certificates logged in publicly-accessible Certificate transparency databases cannot be removed, modified, or redacted.

11.3. Retention. Information provided by Subscriber for the validation of a Publicly-Trusted Certificate shall be retained by Sectigo in accordance with the CPS for not less than seven (7) years, or as necessary to comply with applicable laws. The retention period shall begin on the date of the rejection, expiration, or revocation of a Certificate. Copies of Certificates are held, regardless of their status, whether active, expired or revoked.

12. Term and Termination.

12.1. Term. The Agreement shall commence on the Effective Date and

continue in effect for the Term.

12.2. Auto-Renewal. If the Order Form states that the Agreement renews automatically, then, upon completion of the Initial Term or then-current Renewal Term, the Agreement shall continue in effect (instead of expiring) for successive Renewal Terms unless either party provides the other with thirty (30) days' prior written notice that the Agreement shall expire instead of renewing at the start of the upcoming Renewal Term.

12.3. Termination. Without prejudice to any rights or remedies, a party may terminate the Agreement: (i) if the other party materially breaches the Agreement and fails to remedy the breach upon ten (10) days written notice; (ii) immediately, if the other party violates the limitations on the licenses granted herein, its duty of confidentiality, its duty to adhere to industry standards, or any of the representations it made herein; (iii) immediately, if Subscriber issues a Certificate to a third party; (iv) immediately, if Subscriber engages in illegal or fraudulent activity or an activity that could harm Sectigo's business practices; (v) immediately, if Subscriber fails in its capacity as an Enterprise EV RA (if applicable) to follow the CPS when validating and authorizing the issuance of Certificates; (vi) if Subscriber (a) has a receiver, trustee, or liquidator appointed over substantially all of its assets, (b) has an involuntary bankruptcy proceeding filed against it that is not dismissed within 30 days of filing, (c) files a voluntary petition of bankruptcy or reorganization, (d) assigns the Agreement, or (e) undergoes a change of control where more than fifty percent ownership is transferred to a third party; or (vii) upon reasonable notice, if Sectigo is no longer allowed to issue Certificates or if a change in industry standards, regulations, or law prevents further use or issuance of Certificates.

12.4. Events upon Termination. Upon termination or expiration of the Agreement, all rights and licenses granted herein to Subscriber terminate and revert to Sectigo. In addition, Subscriber shall: (i) immediately cease validating and issuing Certificates; (ii) immediately discontinue all statements that imply a relationship exists between Sectigo and Subscriber; (iii) immediately cease using Sectigo's trademarks and make any transfers reasonably requested by Sectigo to ensure that all trademark rights remain with Sectigo; and (iv) continue to comply with its confidentiality obligations under the Agreement. Subscriber may continue to use all End-Entity Certificates issued during the Term until the earlier of revocation of the Certificate, as provided herein, or the end of the Certificate's lifecycle.

13. Indemnification.

13.1. Subscriber Indemnification. Subscriber shall defend, indemnify, and hold harmless Sectigo, its Affiliates, and their respective directors, officers, employees, and agents from and against any and all third-party claims, liabilities, losses, expenses, and costs (including reasonable attorney's fees) (collectively "Losses") that arise out of or relate to, directly or indirectly: (i) Subscriber's breach of the Agreement; (ii) Subscriber's violation of the licenses and restrictions herein; (iii) Subscriber's failure to disclose a material fact related to the issuance or use of a Certificate; or (iv) Subscriber's infringement on the rights of a third party. Subscriber shall reimburse each Sectigo Indemnitee for all Losses as they are incurred.

13.2. Sectigo Indemnification. Sectigo shall indemnify Subscriber from and against any and all Losses incurred by Subscriber that are based on Sectigo's infringement or misappropriation of a trade secret of a third party or any U.S. patent, registered copyright, or registered trademark related to a Certificate. Sectigo's indemnification obligations shall not apply to the extent any such infringement or misappropriation is the result of: (a) Subscriber's independent modification of a Certificate, or any other product, software or service provided under the Agreement, where without such modification the Certificate or other product would not infringe, (b) Subscriber's combination or use of a Certificate or any other product, software or service provided under the Agreement with any other third-party product, or (c) Sectigo's adherence to Subscriber's express written instructions where such instructions, or any modifications, changes, or combinations made as a result of said instructions, are responsible for the claim of infringement.

13.3. Indemnification Procedure. A party seeking indemnification must notify the indemnifying party promptly of a demand for indemnification. However, such party's failure to notify the indemnifying party will not relieve the indemnifying party of its indemnification obligations, unless such failure to notify materially prejudices the indemnifying party. The indemnifying party may assume the defense of any action, suit, or proceeding giving rise to an indemnification obligation unless assuming the defense would result in potential conflicting interests as determined by the indemnitee in good faith. The indemnifying party may not settle any claim, action, suit or proceeding related to the Agreement unless the settlement also includes an unconditional release of all indemnitees from liability.

14. Disclaimer and Limitation of Liability.

14.1. Relying Party Warranty. Subscriber acknowledges that the Relying Party Warranty is only for the benefit of Relying Parties. Subscriber does not have rights under the Relying Party Warranty, including any right to enforce the terms or make a claim. Sectigo shall manage any claims or disputes arising from the Relying Party Warranty in accordance with both the CPS and Relying Party Agreement.

14.2. Internet. Subscriber acknowledges that Certificates and SCM are subject to the operation and telecommunications infrastructures of the Internet and the operation of Subscriber's Internet connection services, all of which are beyond Sectigo's control.

14.3. Warranty Disclaimers; Assumption of Risk. EXCEPT AS SPECIFICALLY STATED OTHERWISE IN THE AGREEMENT, SECTIGO EXPRESSLY DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES IN THE CERTIFICATES AND SCM. THIS DISCLAIMER IS EFFECTIVE TO THE MAXIMUM EXTENT ALLOWED BY LAW AND INCLUDES ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. THE CERTIFICATES AND SCM ARE NOT TO BE USED FOR, OR RELIED UPON AS, CONTROL EQUIPMENT IN HAZARDOUS CIRCUMSTANCES OR CIRCUMSTANCES REQUIRING FAIL-SAFE PERFORMANCE, SUCH AS OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, AIR TRAFFIC CONTROL SYSTEMS, WEAPONS CONTROL SYSTEMS, OR WHERE FAILURE COULD LEAD DIRECTLY TO DEATH, PERSONAL INJURY, OR SEVERE ENVIRONMENTAL DAMAGE, EACH OF WHICH IS AN UNAUTHORIZED USE OF A CERTIFICATE AND FOR WHICH A CERTIFICATE IS NEITHER DESIGNED NOR INTENDED. AS SUCH, SECTIGO DOES NOT WARRANT THAT 1) THE CERTIFICATES OR SCM WILL MEET SUBSCRIBER'S REQUIREMENTS OR MEET SUBSCRIBER'S EXPECTATIONS OR 2) THAT ACCESS TO SCM WILL BE UNINTERRUPTED, TIMELY, SECURE, OR ERROR-FREE.

14.4. Damage Limitation. THE AGGREGATE LIABILITY OF SECTIGO, ITS AFFILIATES, AND THEIR OFFICERS, DIRECTORS, PARTNERS, EMPLOYEES, AND CONTRACTORS, RESULTING FROM OR CONNECTED TO THIS AGREEMENT, INCLUDING ANY AND ALL CLAIMS FOR INDEMNIFICATION FOR DAMAGES CAUSED BY INFRINGEMENT PURSUANT TO SECTION 13, SHALL BE LIMITED IN THE AGGREGATE TO THE AMOUNT PAID OR PAYABLE BY SUBSCRIBER UNDER THE AGREEMENT DURING THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE EVENTS GIVING RISE TO A CLAIM. SUBSCRIBER WAIVES ALL LIABILITY FOR SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES. THIS WAIVER INCLUDES ALL DAMAGES FOR LOST PROFITS, REVENUE, USE, OR DATA AND APPLIES EVEN IF SECTIGO IS AWARE OF THE POSSIBILITY OF SUCH DAMAGES. These limitations apply to the maximum extent permitted by law regardless of 1) the reason for or nature of the liability, including tort claims, 2) the number of claims, 3) the extent or nature of the damages, and 4) whether any other provisions of this Agreement have been breached or proven ineffective.

14.5. Exceptions. If any legal right disallows an exclusion of warranties or disallows limiting certain damages, then the disclaimers of warranty and limitations on liability herein apply to the maximum extent allowed by law. Nothing in the Agreement excludes or limits the liability of either party for death or personal injury resulting from the negligence of that party or for any statements made fraudulently by either party.

15. Remedy.

15.1. Injunctive Relief. Subscriber acknowledges that a breach of Subscriber confidentiality obligations or Subscriber's obligations with respect to the use of a Certificate will result in irreparable harm to Sectigo that cannot adequately be redressed by compensatory damages. Accordingly, in addition to any other legal remedies which may be available, Sectigo may seek and may obtain an injunctive order against a breach or threatened breach of the Agreement.

15.2. Limitations on Actions. Except for actions and claims related to a party's indemnification and confidentiality obligations, all claims and actions arising from the Agreement must be brought within one year from the date when the cause of action accrued.

15.3. Remedy. Subscriber's sole remedy for a defect in a Certificate is for Sectigo to use commercially reasonable efforts to cure the defect after receiving notice of the defect. Sectigo is not obligated to correct a defect if: (i) Subscriber misused, damaged, or modified the Certificate, (ii) Subscriber did not promptly report the defect to Sectigo, or (iii) Subscriber has breached

any provision of the Agreement.

16. Miscellaneous.

16.1. Industry Standards. The parties shall comply with all industry standards applicable to the Certificates, including the CABF Standards. If industry standards change, Sectigo and Subscriber shall work together in good faith to amend the Agreement to comply with such changes.

16.2. Independent Contractors. Sectigo and Subscriber are independent contractors and not agents or employees of each other. Neither party has the power to bind or obligate the other and each party shall bear its own costs and expenses in performing this Agreement.

16.3. Notices. All notices to either party must be in writing, in English, and sent by first class mail, return receipt requested, to the applicable address listed on the Order Form.

16.4. Entire Agreement. The Agreement constitutes the entire agreement between the parties with respect to the subject matter herein, superseding all prior or contemporaneous oral or written communications, proposals, representations and other agreements that may exist between the parties, and prevails over any conflicting terms of any quote, order, acknowledgment, or similar communications between the parties. Terms in any purchase order that conflict with, or are in addition to, the Agreement are null and void. The Order Form and each Addendum executed by the parties are incorporated herein by reference. In the event of a conflict between the terms of the documents comprising the Agreement, the order of precedence shall be these Terms and Conditions, then an Addendum, then the Order Form. Section headings are for reference and convenience only and are not part of the interpretation of the Agreement.

16.5. Modifications. Except as otherwise allowed herein, neither party may amend the Agreement unless the amendment is both in writing and signed by the parties. In Sectigo's sole discretion, Sectigo may amend any products or services. If this Agreement is translated in any language other than English, the English version shall prevail in all respects.

16.6. Waiver. A party's failure to enforce a provision of the Agreement will not waive the party's right to enforce the same provision later or the party's right to enforce any other provision of the Agreement. To be effective, all waivers must be both in writing and signed by the party benefiting from the waived provision.

16.7. Force Majeure and Internet Frailties. Other than for payment obligations by Subscriber, neither party will be liable under the Agreement for a delay or failure to perform an obligation to the extent that the delay or failure is caused by an occurrence beyond a party's reasonable control. Each party acknowledges that the operation of the Internet is beyond the other party's reasonable control, and neither party will be liable for a delay or failure caused by an interruption or failure of telecommunication or digital transmission links, Internet slow-downs or failures, or other such transmission failure.

16.8. Governing Law; Venue. The Agreement and any disputes relating to SCM and the Certificates provided hereunder shall be governed and interpreted according to each of the following laws, respectively, without regard to its conflicts of law provisions: (a) the laws of the State of New Jersey, if Subscriber is located in North America; or (b) the laws of England and Wales, if Subscriber is located outside of North America. The parties agree to the exclusive jurisdiction of (a) the courts of New Jersey if Subscriber is located in North America, or (b) the courts of England and Wales if the Subscriber is located outside of North America.

16.9. Assignment. Subscriber shall not assign any of its rights, duties, or obligations under the Agreement without the prior written consent of Sectigo. Any transfer without consent is null and void. Sectigo may assign its rights, duties, and obligations without Subscriber's consent.

16.10. Severability. Any provision determined invalid or unenforceable by rule of law will be reformed to the minimum extent necessary to make the provision valid and enforceable.

16.11. Survival. All provisions of the Agreement related to confidentiality, proprietary rights, indemnification, and limitations of liability survive the termination of the Agreement.

16.12. Rights of Third Parties. Except for Application Software Suppliers, nothing in the Agreement is intended or shall be construed to give any person or entity any legal or equitable right, remedy, or claim under or in respect of the Agreement.

16.13. Execution; Counterparts. The parties agree to the execution of the Agreement in electronic form. The parties may execute one or more counterparts of the Agreement, all of which taken together shall constitute one and the same instrument.

17. Definitions. Unless otherwise specified, capitalized terms in the Agreement will have the meanings attributed to them in this section.

17.1. "Addendum" means a Sectigo-issued addendum that: (i) references the Agreement, and (ii) specifies a Renewal Term, adds products or services, and/or incorporates additional terms and/or modifies terms to the Agreement.

17.2. "Affiliate" means a legal entity controlled by a party as of the Effective Date. For the purposes of this definition, "control" shall mean the possession of more than fifty percent (>50%) of the voting equity securities or equity interests in such entity.

17.3. "Agreement" means the entire Enterprise Certificate Agreement between the parties, consisting of the Order Form, these Terms and Conditions, and any present or future Addendum executed by the parties.

17.4. "Applicant" means the individual or entity to be named in an issued Private End-Entity Certificate.

17.5. "Application Software Supplier" means a developer of Internet browser software or other relying-party software that displays or uses Sectigo's Publicly-Trusted Certificates and distributes Sectigo's Publicly-Trusted Root CA Certificates with Sectigo's participation, such as Google Inc., Microsoft Corporation, Mozilla Foundation, and Opera Software ASA.

17.6. "Beta Services" mean Sectigo products or services that are not yet generally available to customers.

17.7. "CA/Browser Forum" means the association of Certificate issuers and Application Software Suppliers whose website is cabforum.org.

17.8. "CABF Standards" refers to the set of industry standards published by the CA/Browser Forum relating to the issuance and management of Publicly-Trusted Certificates, including but not limited to: (i) the *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates,* (ii) the *Guidelines for the Issuance and Management of Extended Validation Certificates,* and (iii) the *Guidelines for the Issuance and Management of Extended Validation Code Signing Certificates*.

17.9. "CA Certificate" means a Certificate that is not an End-Entity Certificate.

17.10. "Certificate" means a digitally signed document that is a public-key certificate in the version 3 format specified by ITU-T Recommendation X.509. The Digital Signature on the certificate binds a subject's identity and other data items to a public key value, thus attesting to the ownership of the Public Key by the subject.

17.11. "Certificate Approver" means a natural person who: (i) is Subscriber's employee or Subscriber's authorized agent, and (ii) who has Subscriber's express authority to represent Subscriber to approve EV Certificate requests submitted by Certificate Requesters.

17.12. "Certificate Requester" means a natural person who: (i) is Subscriber's employee or Subscriber's authorized agent, and (ii) who has Subscriber's express authority to represent Subscriber to request an EV Certificate on Subscriber's behalf.

17.13. "Certification Practices Statement" or "CPS" means one of several Sectigo documents that are posted in the Repository that discloses validation practices and processes of how Publicly-Trusted Certificates are created, issued, managed, and used.

17.14. "Client Certificate" means a Publicly-Trusted, End-Entity Certificate that is validated by Subscriber and provided by Sectigo that both: (i) encrypts and adds a Digital Signature to emails sent by Subscriber or its employees, agents, or contractors, and (ii) can be used by employees, agents, or contractors of Subscriber to authenticate their access to Subscriber's secure domains.

17.15. "Code Signing Certificate" means a Publicly-Trusted, End-Entity Certificate that is issued for purposes of signing software objects and code.

17.16. "Confidential Information" means all documents, information, or processes disclosed by a party to the other that is not accessible or known to the general public, regardless of whether the information was marked as being confidential, but excludes information contained in an issued Certificate.

17.17. "CRL" means a regularly updated time-stamped list of revoked or invalid Private End-Entity Certificates.

17.18. "Digital Signature" means an encrypted electronic data file which is attached to or logically associated with other electronic data and which identifies and is uniquely linked to the signatory of the electronic data, is created using the signatory's Private Key and is linked in a way so as to make any subsequent changes to the electronic data detectable.

17.19. "Document Signing Certificate" means a Publicly-Trusted, End-Entity Certificate that is used to sign PDF documents.

17.20. "DV Certificate" means a Publicly-Trusted, End-Entity Certificate that is validated by confirming the domain name listed in the Certificate.

17.21. "Effective Date" means the date the Agreement is signed by both Sectigo and Subscriber.

17.22. "End-Entity Certificate" means a Certificate that can neither sign nor issue another Certificate.
17.23. "Enterprise EV Certificate" means an EV Certificate that is contained within the domain of a valid Sectigo EV Certificate issued to Subscriber and that is validated by Sectigo and approved for issuance by Subscriber acting as an Enterprise EV RA.
17.24. "Enterprise EV RA" means a legal entity that is responsible for identification and authentication of subjects of Enterprise EV Certificates and may assist in the application and/or revocation process.
17.25. "EV Certificate" means a Publicly-Trusted, End-Entity Certificate that is signed by a Sectigo extended validation root certificate.
17.26. "EV Code Signing Certificate" means a Code Signing Certificate that has been issued in accordance with CABF Standards.
17.27. "Initial Term" means the duration specified as such on the Order Form commencing on the Service Date.
17.28. "Master Registration Authority Officer" or "MRAO" means an employee of Subscriber who is the highest level of administrator in SCM, has access to all functional areas in SCM, and may delegate management functions and administrative roles.
17.29. "OCSP" means an online Certificate-checking protocol that enables an entity to determine the status of an issued Private End-Entity Certificate.
17.30. "Order Form" means the Sectigo-issued order form referencing these Terms and Conditions and signed by the parties.
17.31. "OV Certificate" means a Publicly-Trusted, End-Entity Certificate that is validated by confirming the existence of the entity named in the Certificate and the domain name listed in the Certificate.
17.32. "Premier Support Services" means the support services selected and identified as such on the Order Form and paid for by Subscriber, as further described in section 5.2.
17.33. "Privacy Policy" means the latest version of Sectigo's policies and practices about information privacy accessible via Sectigo's website.
17.34. "Private CA Managed Services" means the Services related to the Privately-Trusted Certificates, including the OCSP/CRL services, but excludes Services related to Publicly-Trusted Certificates.
17.35. "Private End-Entity Certificate" means a Privately-Trusted, End-Entity Certificate that: (i) is validated by Subscriber, and (ii) is issued from the Private Intermediary CA Certificate.
17.36. "Private Intermediary CA Certificate" means a Privately-Trusted, CA Certificate that is chained to the Private Root CA Certificate and can be used to issue a Private End-Entity Certificate.
17.37. "Private Key" means the key of a key pair that is kept secret by the holder of the key pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.
17.38. "Private Root CA Certificate" means a Privately-Trusted, CA Certificate that is created by Sectigo and signed on behalf of Subscriber, identifies Subscriber and is used to sign a Private End-Entity Certificate.
17.39. "Privately-Trusted" and "Privately-Trusted Certificate" mean a Certificate that is not a Publicly-Trusted Certificate.
17.40. "Public Intermediary CA Certificate" means a Publicly-Trusted, CA Certificate that is chained to a Sectigo Publicly-Trusted Root Certificate and can be used to issue Publicly-Trusted, End-Entity Certificates.
17.41. "Public Key" means the key of a key pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
17.42. "Publicly-Trusted" and "Publicly-Trusted Certificate" mean a Certificate that is trusted by virtue of the fact that its corresponding root CA Certificate is distributed as a trust anchor by Application Software Suppliers in widely-available application software.
17.43. "Relying Party" means any entity other than Subscriber that relies on a valid Publicly-Trusted Certificate and that meets the conditions found in the Relying Party Agreement.
17.44. "Relying Party Agreement" refers to an agreement, available in the Repository, that governs the use of a Publicly-Trusted Certificate by a Relying Party.
17.45. "Relying Party Warranty" refers to a warranty offered by Sectigo to Relying Parties who agree to the terms of the Relying Party Agreement.
17.46. "Renewal Term" means either: (i) the one-year period commencing on the expiration of the Initial Term or then-current Renewal Term provided the Agreement renews automatically, or (ii) the duration specified on a renewal Addendum executed by the parties.
17.47. "Repository" means Sectigo's publicly available collection of databases and documents for storing and retrieving information relating to Certificates accessible via Sectigo's website.
17.48. "Reseller" means the legal entity authorized by Sectigo to resell SCM and Certificates to Subscriber.
17.49. "Sectigo Certificate Manager" or "SCM" means Sectigo's web-based Certificate management and ordering platform, the related APIs, and documentation.
17.50. "Service Date" means the date from which Subscriber accesses SCM, as specified on the Order Form.
17.51. "Services" means SCM, the Certificates, and other products and services ordered and paid for by Subscriber and provided by Sectigo.
17.52. "Subscriber" means the legal entity identified as such on the Order Form.
17.53. "Suspect Code" means code that contains malicious functionality or serious vulnerabilities, including spyware, malware, and other code that installs without the user's consent and/or resists its own removal, and code that can be exploited in ways not intended by its designers to compromise the trustworthiness of the platforms on which it executes.
17.54. "Term" means the period of time from the Effective Date until the earlier of: (i) expiration of the Initial Term and any and all Renewal Terms agreed to between the parties, or (ii) termination of the Agreement as provided herein
17.55. "Trial Services" mean services that are offered to Subscriber on a free-to-try basis for a limited period.