IMPORTANT—PLEASE READ THIS SECTIGO CERTIFICATE SUBSCRIBER AGREEMENT CAREFULLY BEFORE APPLYING FOR, ACCEPTING, OR USING A SECTIGO CERTIFICATE OR BEFORE CLICKING ON "I ACCEPT". YOU AGREE THAT BY APPLYING FOR, ACCEPTING, OR USING A SECTIGO CERTIFICATE, YOU HAVE READ THIS AGREEMENT, YOU UNDERSTAND IT, AND YOU AGREE TO ITS TERMS. IF YOU ARE APPLYING FOR, ACCEPTING, OR USING A SECTIGO CERTIFICATE ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU ARE AN AUTHORIZED REPRESENTATIVE OF SUCH ENTITY AND HAVE THE AUTHORITY TO ACCEPT THIS AGREEMENT ON SUCH ENTITY'S BEHALF. IF YOU DO NOT HAVE SUCH AUTHORITY OR IF YOU DO NOT ACCEPT THIS AGREEMENT, DO NOT APPLY FOR, ACCEPT, OR USE A SECTIGO CERTIFICATE AND DO NOT CLICK "I ACCEPT".

SECTIGO CERTIFICATE SUBSCRIBER AGREEMENT

This Sectigo Certificate Subscriber Agreement (this "**Agreement**") is between a natural person or the legal entity who applies for and is issued, or identified on, the Certificate(s) resulting from this Agreement ("**Subscriber**") and Sectigo Limited, a limited company formed under the laws of England and Wales with registered number 04058690 and registered offices Sectigo Limited, Exmouth House, 3/11 Pine Street, London, England, EC1R 0JHUnited Kingdom ("**Sectigo**"). This Agreement governs Subscriber's application for and use of a Certificate issued from Sectigo. Subscriber and Sectigo agree as follows:

1. Definitions.

1.1. "**Application Software Suppliers**" means a developer of Internet browser software or other software that displays or uses Sectigo's Certificates and distributes Sectigo's root Certificates, such as Google Inc., Microsoft Corporation, Mozilla Foundation, etc..

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

1.3. "**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 (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*.

1.4. "**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.

1.5. "**Certificate Approver**" means a natural person who is either Subscriber, employed by Subscriber, or an authorized agent who has express authority to represent Subscriber to (i) act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and (ii) to approve Certificate Requests for EV Certificates or QWAC's submitted by other Certificate Requesters.

1.6. "**Certificate Requester**" means a natural person who is either the Subscriber, employed by the Subscriber, an authorized agent who has express authority to represent the Subscriber, or a third party (such as an ISP or hosting company) that completes and submits a Certificate Request on behalf of Subscriber.

1.7. "**Certificate Policy and Certification Practices Statement**" or "**CP/CPS**" means the latest version of the Sectigo document(s) posted in the Repository that explains Sectigo's policies and practices of how the applicable Publicly-Trusted Certificate is created, issued, managed, and used..

1.8. "**Code Signing Certificate**" means a Certificate that is issued for purposes of signing software objects and code.

1.9. "**Combined Mark**" means a mark consisting of a graphic design, stylized logo, or image, with words and/or letters having a particular stylized appearance. For greater certainty, a "Combined Mark" includes marks made up of both word and design elements.

1.10. "**Confidential Information**" means all material, data, systems, technical operations, and other information concerning Sectigo's business operations that is not known to the general public, including all information about the Certificate issuance services (such as all Private Keys, personal identification numbers and passwords).

1.11. "**Client Certificate**" means a 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 access to Subscriber's secure domains.

1.12. "**Delegated RA**" means a legal entity that is responsible for identification and authentication of subjects of Mark Certificates and may assist in the application and/or revocation process.

1.13. "**Design Mark**" means mark consisting of a graphic design, stylized logo, or image, without words and/or letters. For greater certainty, a "Design Mark" includes marks made up solely of design elements.

1.14. "**Digital Signature"** means an encrypted electronic data file which may be 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.

1.15. "**Document Signing Certificate**" means a Certificate that is used to sign documents (e.g., PDF).

1.16. "**DV Certificate**" means a Certificate that is validated by confirming the domain name listed in the Certificate.

1.17. "**eIDAS Regulation**" means Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014

on electronic identification and trust services for electronic transactions in the internal market, as amended.

1.18. "**ETSI**" means the European Telecommunications and Standards Institute, an independent, non-for-profit, standardization organization for the information and communications technology industry.
1.19. "**ETSI Standards**" means those Industry Standards developed by ETSI.
1.20. "**EV Certificate**" means a Certificate signed by Sectigo's EV root Certificate and that complies with CABF Standards.
1.21. "**EV Code Signing Certificate**" means a Code Signing Certificate issued in compliance with CABF Standards.
1.22. "**Industry Standards**" mean, individually or collectively, the CABF Standards, the ETSI Standards or any other standards, rules, guidelines, and requirements applicable to a Certificate.
1.23. "**Mark**" means a Combined Mark, Design Mark, or Word Mark. Such Marks may either be 1. registered with a Trademark Office (Registered Mark) or created through government action (Government Mark); or 2. a mark or logo which qualifies to be included in a Mark Certificate.
1.24. "**Mark Certificate**" means a certificate that contains subject information and extensions specified in the VMC Requirements and that has been verified and issued by a Certificate Authority in accordance with the VMC Requirements. Additionally, the certificate contains a Mark Representation that has been verified as a Registered Mark or Government Mark.
1.25. "**Mark Representation**" means digital representation of a Combined Mark, Design Mark, or Word Mark such as a digital or computer file, containing structured binary or textual data which can be interpreted to recreate (render) a visual representation of the mark so that it can be seen.
1.26. "**OV Certificate**" means a Certificate that is validated by confirming the existence of the entity named in the Certificate and the domain name listed in the Certificate.
1.27. "**Privacy Policy**" means Sectigo's policies and practices about information privacy accessible via the website: https://sectigo.com/privacy-policy.
1.28. "**Private Key**" means a confidential encrypted electronic data file designed to interface with a Public Key using the same encryption algorithm and which may be used to create Digital Signatures, and decrypt files or messages which have been encrypted with a Public Key.
1.29. "**Public Key**" means a publicly available encrypted electronic data file designed to interface with a Private Key using the same encryption algorithm and which may be used to verify Digital Signatures and encrypt files or messages.
1.30. "**Qualified Certificate**" refers to a Certificate issued according to the requirements of the eIDAS Regulation.
1.31. "**Qualified Website Authentication Certification**" or "**QWAC**" means a Qualified Certificate used for website authentication.
1.32. "**Registered Mark**" means a Mark that has been registered as a trademark with a Trademark Office, and in particular, as the Mark appears in the official database of the applicable Trademark Office.
1.33. "**Relying Party**" means an entity, other than Subscriber, that relies on a valid Certificate and that meets the conditions found in the Relying Party Agreement.
1.34. "**Relying Party Agreement**" refers to an agreement located in the Sectigo Repository that governs a Relying Party's use of a valid Certificate.
1.35. "**Relying Party Warranty**" refers to a warranty offered by Sectigo to a Relying Party under the terms and conditions found in the Sectigo Relying Party Agreement in connection with the Relying Party's use of a valid Certificate.
1.36. "**Repository**" means a publicly available collection of information and databases relating to Sectigo's Certificate practices and which is available at https://sectigo.com/legal.
1.37. "**Services**" means the Certificates ordered hereunder along with any related TrustLogos and/or Sectigo software, and documentation.
1.38. "**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.
1.39. "**Token**" means a certified hardware cryptographic device (FIPS and/or CC) containing a single Customer Code Signing Certificate, Document Signing Certificate, or eIDAS Certificate.
1.40. "**TLS**" Transport Layer Security is a cryptographic protocol designed to provide communications security over a network. Websites use this protocol to secure all communications between their servers and the web browsers.
1.41. "**TLS Certificates**" means, individually and collectively, a DV Certificate, OV Certificate, EV Certificate, and QWAC.
1.42. ""**Trademark Office**" means an intellectual property office recognized by the World Intellectual Property Organization for registration of trademarks (see names of intellectual property offices as listed in the column "Office" at https://www.wipo.int/directory/en/urls.jsp.
1.43. "**TrustLogo**" means a logo provided by Sectigo for use on a Subscriber's site in connection with an issued Certificate.
1.44. "**VMC Requirements**" a set of guidelines for the issuance and management of Mark Certificates, as set forth and maintained by AuthIndicators Working Group.

2. Subscription Service and Products.

2.1. Request. When applying for a Certificate, Subscriber shall submit a certificate request in a form specified by Sectigo for each ordered Certificate ("**Certificate Request**"). Forms for a Certificate Request are available on Sectigo's website and may be completed electronically.
2.2. Appointment. When submitting a Certificate Request for an EV Certificate or QWAC Certificate, Subscriber shall designate, and thereby appoint, a Certificate Requester and Certificate Approver. Subscriber shall provide each natural person to be

designated a Certificate Requester or Certificate Approver a copy of, or an opportunity to review, this Agreement and the Privacy Policy prior to such appointment. Unless such appointment is revoked by Subscriber sending notice to Sectigo, such appointment lasts for the duration of this Agreement.

2.3. Validation. Upon Sectigo's acceptance of Subscriber's Certificate Request, Sectigo shall attempt to validate the information provided in accordance with the Sectigo CP/CPS and Industry Standards. If Sectigo chooses to accept the application and can validate Subscriber to Sectigo's satisfaction, Sectigo shall issue the ordered Certificate(s) to Subscriber. Sectigo may reject a Certificate Request and refuse to issue any ordered Certificate in its sole discretion.

2.4. Multiple Certificates. This Agreement applies to multiple future Certificate Requests and any resulting Certificates, regardless of when the Certificate is requested or issued.

2.5. Tokens. If Customer purchases Code-Signing Certificates, Document Signing Certificate, and/or eIDAS Certificates from Sectigo it may also purchase the corresponding Token. Customer shall purchase one (1) Token for each Code Signing Certificate, Document Signing Certificate, or eIDAS Certificate that it purchases. If Customer purchases a Token(s) from Sectigo for the delivery of Customer's Code Signing Certificate, Document Signing Certificate, or eIDAS Certificate, Customer shall not:

(i) permit any third party to use or access the Token; or
(ii) sell, lend, lease, and/or transfer the Token to any third party.

If a Customer Token is lost and/or stolen, Customer must immediately notify Sectigo once Customer becomes aware that the Token is lost and/or stolen. Customer may then pay for the replacement of the lost/stolen Token.

2.6. Mark Certificates. If Subscriber purchases any Mark Certificates through Sectigo, it agrees to comply with all guidelines concerning Mark Certificates which are contained in the SSL.com Certificate Policy and Certification Practices Statement. The current edition of the CP/CPS is available for inspection at SSL.com/repository. Subscriber acknowledges that it is buying such Mark Certificates through Sectigo acting as the Delegated RA for SSL.com.

2.7. Mark Certificate Roles. Applicant must designate the natural persons who will occupy the following roles: (i) Signatory. "Signatory", as used herein, shall mean either the Applicant, employed by the Applicant, and/or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to sign subscriber agreements; (ii) Certificate Requester; and (ii) Certificate Approver. The Applicant may authorize one individual to occupy two or more of these roles, and/or may authorize more than one individual to occupy any of these roles.

3. Licenses and Restrictions.

3.1. Certificate License. Subject to the terms and conditions stated herein, after issuance of a Certificate, Sectigo grants Subscriber a revocable, non-exclusive, non-transferable, limited license to use the issued Certificate (i) on the server hosting the domain name(s) listed in the Certificate, if the Certificate is a TLS Certificate, (ii) for purposes of encrypting and digitally signing email messages, if the Certificate is a Client Certificate, (iii) to sign software objects or code, if the Certificate is a Code Signing Certificate, (iv) to sign PDF documents, if the Certificate is a Document Signing Certificate, each only for Subscriber's legitimate business purposes, in accordance with the CP/CPS, until the earlier of expiration or revocation of the Certificate or termination of this Agreement as provided herein. All rights not expressly granted herein to Subscriber are reserved to Sectigo.

3.2. TrustLogo License. To the extent included with the purchased Services, Sectigo grants Subscriber a revocable, non-exclusive, non-transferable, limited license to display each purchased TrustLogo on domain(s) secured by a Sectigo TLS Certificate. When revoking a Certificate, Sectigo may also revoke any TrustLogos issued to the same site. Subscriber shall not modify a TrustLogo in any manner. Subscriber shall not display or use a TrustLogo 1) to represent that Sectigo guarantees any non-Sectigo products or services, 2) on a site that is misleading, defamatory, libelous, disparaging, obscene or otherwise objectionable to Sectigo, or 3) in a way that harms Sectigo's rights to its trademarks or harms Sectigo's business reputation.

3.3. 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 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 or receive unsolicited bulk correspondence or 5) create a Private Key that is substantially similar to a Sectigo or third party's Private Key; and/or

(x) make representations regarding the Service to any third party except as agreed to in writing by Sectigo.

3.4. Revocation. Subscriber is hereby informed, and acknowledges understanding, of the reasons for revoking a Certificate, including those stated in the CP/CPS, which is incorporated herein by reference and made a part of this Agreement. In addition, Sectigo may revoke a Certificate if Sectigo believes or has reason to believe that:

(i) Subscriber requested revocation of the Certificate;
(ii) Subscriber did not authorize the Certificate Request and has not retroactively granted authorization;
(iii) Subscriber breached the terms of this Agreement, or any warranty or restriction provided therein;
(iv) the Private Key corresponding to the Public Key in the Certificate has been disclosed, compromised, or no longer complies with Industry Standards;
(v) the Private Key of the subordinate Certificate used to issue the Certificate has been compromised or no longer complies with Industry Standards;
(vi) the Certificate has been 1) misused, 2) used contrary to law, rule, regulation, or Industry Standard or 3) used, directly or indirectly, for illegal or fraudulent purposes;
(vii) information in the Certificate is inaccurate, misleading, or infringes the intellectual property rights of a third party;
(viii) the technical content or the format of the Certificate presents an unacceptable risk, in Sectigo's opinion, to Application Software Suppliers or Relying Parties;
(ix) for TLS Certificates, Subscriber loses exclusive control over a domain name listed in the Certificate;
(x) the Certificate was not issued or used in accordance with this Agreement, Sectigo's CP/CPS, or Industry Standards;
(xi) Sectigo 1) ceased operations or 2) is no longer allowed to issue the Certificate, and no other certificate authority has agreed to provide revocation support for the Certificate;
(xii) for wildcard Certificates, the Certificate has been used to authenticate a fraudulently misleading subordinate fully-qualified domain name;
(xiii) Subscriber is 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;
(xiv) the Certificate was issued to publishers of Suspect Code, or may have been used to sign Suspect Code, if the Certificate is a Code Signing Certificate;
(xv) Sectigo's CP/CPS authorizes revocation of the Certificate;
(xvi) the use of an email address associated with the Certificate is no longer legally permissible or should not be relied on; or
(xvii) the Certificate, if not revoked, will compromise the trust status of Sectigo.

After revoking a Certificate, Sectigo may, in its sole discretion, reissue the Certificate to Subscriber and/or terminate this Agreement.

4. Subscriber Obligations.

4.1. Warranties and Covenants. Subscriber warrants and covenants:

(i) to provide accurate and complete information at all times to Sectigo in the Certificate Request and as otherwise requested in connection with the issuance of Certificates;
(ii) to 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;
(iii) to install and use each TLS Certificate 1) only on domains owned or controlled by Subscriber and 2) only on the server(s) accessible at the subjectAltName(s) listed in the Certificate;
(iv) the subject named in each ordered TLS Certificate has exclusive control of the domain name(s) listed in such Certificate;
(v) to 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 the Certificates, 2) Subscriber's conduct and its website maintenance, operation, development, and content;
(vi) to 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;
(vii) to use the following to generate each Code Signing Certificate and/or Document Signing, and to protect each Code Signing Certificate and/or Document Signing Certificate) 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;
(viii) to use Document Signing Certificates solely for signing PDF documents in connection with its legitimate business purposes;
(ix) it 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, this Agreement and Sectigo's Privacy Policy;
(x) to promptly inform Sectigo if Subscriber becomes aware of any misuse of a Certificate and assist Sectigo in preventing, curing, and rectifying any misuse;
(xi) to 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;

(xii) to cease all use of the Certificate and its Private Key upon expiration or revocation of the Certificate;
(xiii) to comply with all regulations, policies, and procedures of its networks while using Certificates and obtain and keep in force any consent, authorization, permission or license that may be required for Subscriber's lawful use of the Certificates;
(xiv) to abide by this Agreement, the CP/CPS applicable to the Certificate, which is incorporated herein by reference, and all applicable laws, rules, regulations, and guidelines when using the Services;
(xv) to respond to Sectigo's instructions concerning Certificate misuse within five (5) days of such instruction;
(xvi) Subscriber has full power and authority to enter into this Agreement and perform its obligations hereunder;
(xvii) it manifests assent to this Agreement as a condition of obtaining a Certificate;
(xviii) install and use each email Certificate only on the mailbox address(es) listed in the Certificate;
(xix) the individual accepting this Agreement is expressly authorized by Subscriber to sign this Agreement for Subscriber;
(xx) to use one of the following options to generate a Qualified Certificate and to protect each Qualified Certificate: 1) a hardware crypto module listed as a QSCD according to eIDAS regulation; or 2) another type of hardware crypto module with at least FIPS 140-2 Level 3 or Common Criteria EAL 4+ certification and;
(xxi) to not permit third parties access, use, or control of any Token purchased from Sectigo

5. Fees.

5.1. Payment. Subscriber shall pay all applicable fees for the Services before the Certificate is issued. Certificate fees are provided to Subscriber during the application process. All payments are non-refundable, except that the Certificate's seller will refund a payment if, before twenty (20) business days after the Certificate's purchase, the Subscriber has 1) not used the Certificate, and 2) made a written request to Sectigo for the Certificate's revocation. Provided Subscriber purchased one or more Services through a Sectigo-authorized reseller ("**Reseller**"), Subscriber shall pay such Reseller in accordance with the payment terms established between Subscriber and Reseller. 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.

5.2. Subscription Fees. Certificates are purchased on a subscription basis. Subscriber agrees to make such payments to Sectigo for access to the Certificate(s) as a Service during the Term. The quantity of Certificates ordered shall represent the total number of Active Certificates that Subscriber may hold at any given time during the Term. "Active Certificate(s)" as used herein shall mean an issued Certificate with a currently active lifecycle. Active Certificates do not include a Certificate that was previously active but has since been revoked or has expired.

5.3. Late Fees. In addition to any other rights set forth herein, if Subscriber fails to remit payment for Services to Sectigo for fifteen (15) days after Subscriber has received notice of a delinquent payment, Sectigo may, at its sole discretion, charge Subscriber interest for late fees at the lesser of: (i) one and one half percent (1.5%) per month; or (ii) the maximum rate permitted by law.

5.4. Auto-Renewal. If the Services renew automatically, then the Services shall continue in effect (instead of expiring) for continuous periods, for either monthly or yearly periods depending on the Service, unless otherwise cancelled.

5.5. Taxes. All amounts payable by Subscriber under this Agreement are net amounts and are payable in full, without deduction for taxes or duties of any kind. Subscriber will be responsible for, and will promptly pay, all required taxes and duties of any kind (including, but not limited to, sales, use and withholding taxes) associated with this Agreement, except for taxes based on Sectigo's net income. If Sectigo is required to collect, or pays on Subscriber's behalf, any taxes or duties for which Subscriber is responsible, then Subscriber will pay or reimburse Sectigo, as the case may be, for all such amounts.

5.6. Amendments. Sectigo may establish, change, alter, or amend, in its sole discretion, the prices for the Services, as well as the terms of this Agreement and any documents in the Repository or on another Sectigo website. All changes are effective upon the earliest of Sectigo's posting of the changes on its website or Subscriber's receipt of such changes. Subscriber's continued use of Certificates shall constitute Subscriber's acceptance of the amendments.

6. Term and Termination.

6.1. Term. Unless otherwise terminated as allowed herein, this Agreement is effective upon Subscriber's acceptance and lasts for as long as a Certificate issued under this Agreement is valid.

6.2. Termination. Either party may terminate this Agreement with twenty (20) business days' notice for convenience. Sectigo may terminate this Agreement immediately without notice if

(i) Subscriber breaches the terms of this Agreement, or any of the warranties provided herein,
(ii) Sectigo revokes all Certificates issued to Subscriber, as allowed herein,
(iii) Sectigo rejects Subscriber's initial Certificate Request,
(iv) Sectigo cannot satisfactorily validate Subscriber in accordance with section 2.3, or
(v) Industry Standards change in a way that affects the validity of the Certificates ordered by Subscriber.

6.3. Events Upon Termination. After termination, Sectigo may revoke any other Certificates issued to Subscriber without further notice. Subscriber shall pay any amounts still owed for the Certificates. Sectigo is not obligated to refund any payment made by Subscriber upon termination of this Agreement.

6.4. Modifications. If Industry Standards change and require the purchase of additional software or hardware in order for a Certificate to be compliant, Sectigo may provide such software or hardware to Subscriber at an additional cost.

7. Intellectual Property Rights.

7.1. Sectigo IP Rights. Sectigo retains, and Subscriber shall not obtain or claim, all title, interest, and ownership rights in:
(i) the Services, including issued Certificates,
(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 materials provided by Sectigo, and
(iv) all of Sectigo's copyrights, patent rights, trade secret rights and other proprietary rights.

7.2. Trademarks. Subscriber shall not use a Sectigo trademark without Sectigo's written consent. Sectigo consents to Subscriber's display of the Sectigo trademark provided with purchased TrustLogos until termination of this Agreement or revocation of the TrustLogo or associated Certificate.

7.3. Subscriber IP. Subscriber grants Sectigo a worldwide, non-exclusive, non-sublicensable right, to use any Subscriber trademark, service mark or tradename, to perform its obligations under this Agreement, and to identify Subscriber in Sectigo's customer lists and other marketing and promotional materials and communications referencing Subscriber as a customer of Sectigo.

8. Confidentiality.

8.1. Except as allowed herein, a party (the "**Receiving Party**") shall not use or disclose any Confidential Information provided by the other party (the "**Disclosing Party**") other than for the purpose of performing its obligations under this Agreement. The Receiving Party shall take reasonable measures to prevent unauthorized disclosure and shall ensure that any person receiving Confidential Information complies with the restrictions in this section. The Receiving Party may disclose Confidential Information if the information:
(i) is already possessed by the Receiving Party before receipt from the Disclosing Party;
(ii) is or becomes public domain without fault of the Receiving Party;
(iii) 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,
(iv) is disclosed in response to the requirements of a law, governmental order, regulation, or legal process and the Receiving Party first gives prior notice to the Disclosing Party of the requirement to disclose the information, or
(v) is disclosed under operation of law to the public without a duty of confidentiality.

8.2. A party asserting one of the exceptions to Confidential Information above shall prove the assertion using verifiable documentary evidence. The confidentiality obligations contained in this section apply for the duration of this Agreement plus five years after its termination; provided, however, with respect to Confidential Information that constitutes a trade secret, for as long as that Confidential Information remains a trade secret.

9. Privacy and Data Protection.

9.1. Privacy Policy. Sectigo shall follow its Privacy Policy when processing Subscriber's information. Sectigo may amend its Privacy Policy at any time in accordance with the process outlined therein. Subject to Section 9.2, Sectigo shall use reasonable efforts in protecting Subscriber's information. Subscriber acknowledges that risks remain that are beyond Sectigo's reasonable control and waives all liability of Sectigo for these risks.

9.2. 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. Subscriber consents to a) Sectigo disclosing Subscriber's information publicly by embedding the information in issued Certificates, and b) Sectigo disclosing and transferring Subscriber's information to third parties located outside of the European Union as necessary to validate and issue Certificates.

9.3. Retention. Information provided by Subscriber for the validation of a Certificate shall be retained by Sectigo in accordance with the CP/CPS and Industry Standards 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 valid, expired, or revoked. The event logs are retained for not less than two (2) years.

10. Indemnification.

10.1. Indemnification. Subscriber shall indemnify Sectigo and its affiliates and their respective directors, officers, employees, and agents (each an "**Indemnified Person**") against all liabilities, losses, expenses, or costs (including reasonable attorney's fees) that, directly or indirectly, are based on Subscriber's breach of this Agreement, information provided by Subscriber, or Subscriber's or its customers' infringement on the rights of a third party.

10.2. Indemnification Procedure. Sectigo shall notify Subscriber promptly of any demand for indemnification. However, Sectigo's failure to notify will not relieve Subscriber from its indemnification obligations except to the extent that the failure to provide timely notice materially prejudices Subscriber. Subscriber 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 Indemnified Person in good faith. Subscriber may not settle any claim, action, suit or proceeding related to this Agreement unless the settlement also includes an unconditional release of all Indemnified Persons from liability.

10.3. Additional Liability. The indemnification obligations of Subscriber are not Sectigo's sole remedy for Subscriber's breach and are in addition to any other remedies Sectigo may have against Subscriber under this Agreement. Subscriber's

indemnification obligations survive the termination of this Agreement.

11. Disclaimers and Limitation of Liability.

11.1. Relying Party Warranties. Subscriber acknowledges that the Relying Party Warranty is only for the benefit of Relying Parties. Subscriber does not have rights under the warranty, including any right to enforce the terms of the warranty or make a claim under the warranty.

11.2. Exclusion of Warranties. THE SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE". SECTIGO EXPRESSLY DISCLAIMS ALL IMPLIED AND EXPRESS WARRANTIES IN THE SERVICES. THIS DISCLAIMER INCLUDES ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT AND IS EFFECTIVE TO THE MAXIMUM EXTENT ALLOWED BY LAW. SECTIGO DOES NOT GUARANTEE THAT 1) THE SERVICES WILL MEET SUBSCRIBER'S REQUIREMENTS OR EXPECTATIONS OR 2) THAT ACCESS TO THE SERVICES WILL BE UNINTERRUPTED, TIMELY, SECURE, OR ERROR-FREE.

11.3. Free On-Board Origin. If Customer purchases a Token from Sectigo, all title and risk of loss for all Tokens shall pass from Sectigo to the Subscriber at the point of shipment. Sectigo shall package the Tokens for shipment with a reputable carrier and arrange for transportation, but all costs and risks of transportation shall be borne by the Subscriber. Delivery shall be deemed to be complete upon the Tokens being placed on board the carrier at the point of shipment. Sectigo shall not be liable for any loss, damage or delay that occurs during transportation. Subscriber shall be responsible for obtaining any necessary licenses, permits, or approvals for the importation of the Tokens. In the event of a damaged, lost or missing shipment, Sectigo shall, at Subscriber's specific, written request and discretion, submit a claim on behalf of the Subscriber with the carrier, and ensure the claim is resolved to Subscriber's reasonable satisfaction.

11.4. Limitation on Liability. SUBJECT TO SECTION 11.5, THE TOTAL LIABILITY OF SECTIGO AND ITS AFFILIATES, AND EACH OF THEIR OFFICERS, DIRECTORS, PARTNERS, EMPLOYEES, AND CONTRACTORS, RESULTING FROM OR CONNECTED TO THIS AGREEMENT IS LIMITED TO THE AMOUNT PAID BY SUBSCRIBER FOR THE SERVICES GIVING RISE TO THE LIABILITY. SUBSCRIBER WAIVES ALL LIABILITY FOR ANY 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 any claims, 3) the extent or nature of the damages, and 4) whether any other provisions of this Agreement have been breached or proven ineffective.

11.5. Exception. Nothing in this 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.

12. Miscellaneous.

12.1. Relationship of the Parties. The status of a party under this Agreement shall be that of an independent contractor. Nothing contained in this Agreement shall be construed as creating a partnership, joint venture or agency relationship between the parties or, except as otherwise expressly provided in this Agreement, as granting either party the authority to bind or contract any obligation in the name of or on the account of the other party or to make any statements, representations, warranties or commitments on behalf of the other party. All persons employed by a party shall be employees of such party and not of the other party and all costs and obligations incurred by reason of any such employment shall be for the account and expense of such party.

12.2. Force Majeure and Internet Frailties. Other than for payment obligations by Subscriber, neither party will be liable for a delay or failure to perform an obligation to the extent that the delay or failure is caused by an occurrence beyond the 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.

12.3. Opt-out. Subscriber may opt-out of having information used for purposes not directly related to the Services by emailing a clear notice to optout@sectigo.com. By clicking "I AGREE", Subscriber affirmatively consents to receiving Sectigo's and its affiliates marketing material.

12.4. Injunctive Relief. Subscriber acknowledges that its breach of this Agreement 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 obtain an injunctive order against a breach or threatened breach of this Agreement.

12.5. Limitation on Actions. Except for actions and claims related to a party's indemnification and confidentiality obligations, all claims and actions arising from this Agreement must be brought within one (1) year from the date when the cause of action occurred.

12.6. Remedy. Subscriber's sole remedy for a defect in the Services is to have Sectigo use reasonable efforts to correct the defect. Sectigo is not obligated to correct a defect if (i) the Service was misused, damaged, or modified, (ii) Subscriber did not immediately report the defect to Sectigo, or (iii) Subscriber breached any provision of this Agreement.

12.7. Notices. Subscriber shall send all notices to Sectigo by first class mail in writing in English, with return receipt requested, to the address listed in the introductory paragraph ATTN: Legal Department, and a copy to legalnotices@sectigo.com. Sectigo shall send all notices to Subscriber by first class mail in writing in English to (i) the address listed below Subscriber's signature line, if listed, or (ii) the address listed in the introductory paragraph or by email or facsimile to Subscriber's contact information listed on its Certificate Request.

12.8. Entire Agreement. This Agreement and all documents referred to herein constitutes the entire agreement between the

parties, superseding all other agreements that may exist with respect to the subject matter. Section headings are for reference and convenience only and are not part of the interpretation of this Agreement.

12.9. Amendments. Sectigo may amend this Agreement, the CP/CPS, the Relying Party Agreement, the Relying Party Warranty, its website, and any documents listed in its Repository at any time by posting either the amendment or the amended document in the Repository. Subscriber shall periodically review the Repository to be aware of any changes. Subscriber may terminate this Agreement if Subscriber does not agree to the amendment. Subscriber's continued use of the Services after an amendment is posted constitutes Subscriber's acceptance of the amendment.

12.10. Rules of Interpretation. Except as otherwise expressly provided in this Agreement, the following rules of interpretation apply to this Agreement: (i) the singular includes the plural and the plural includes the singular; (ii) "or" and "any" are not exclusive and "include" and "including" are not limiting; (iii) a reference to any agreement or other contract includes permitted supplements and amendments thereto; (iv) a reference to a law includes any amendment or modification to such law and any rules or regulations issued thereunder; (v) a reference to a person or entity includes its permitted successors and assigns; and (vi) a reference in this Agreement to an Article, Section, Annex, Exhibit or Schedule is to the Article, Section, Annex, Exhibit or Schedule of this Agreement.

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

12.12. Assignment. Subscriber may not assign any of its rights or obligations under this Agreement without the prior written consent of Sectigo. Any transfer without consent is void. Sectigo may assign its rights and obligations without Subscriber's consent.

12.13. Governing Law and Venue. This Agreement and any disputes relating to 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.

12.14. 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. If reformation is not possible, the provision is deemed omitted and the balance of this Agreement remains valid and enforceable.

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

12.16. Rights of Third Parties. Except for Application Software Suppliers, nothing in this 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 this Agreement.

12.17. Counterparts; Integration; Effectiveness. This Agreement may be executed by written, facsimile or electronic means, and in one or more counterparts (and by different parties hereto in different counterparts), each of which shall constitute an original, but all of which when taken together shall constitute a single contract.

ACCEPTANCE

BY CLICKING ON "I ACCEPT", YOU AGREE THAT YOU HAVE READ AND UNDERSTAND THIS AGREEMENT AND THAT YOU WILL BE BOUND BY AND COMPLY WITH ALL OF ITS TERMS AND CONDITIONS. DO NOT CLICK THE "I ACCEPT" BUTTON IF YOU DO NOT AGREE TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT.