CERTIFICATE SUBSCRIBER AGREEMENT

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE PROCEEDING. YOU MUST CHECK "I AGREE" BELOW TO ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO IT. IF YOU DO NOT ACCEPT THIS AGREEMENT, DO NOT ORDER OR APPROVE THE ISSUANCE OF A DIGITAL CERTIFICATE. IF YOU HAVE ANY QUESTIONS REGARDING THIS AGREEMENT, PLEASE E-MAIL DIGICERT AT LEGAL@DIGICERT.COM OR CALL 1-800-896-7973. **THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE**

These certificate terms of use are between DigiCert, Inc., a Utah corporation (**"DigiCert"**) and the entity applying for a Certificate, as identified in the account or issued certificates. **"Certificate"** means a digitally signed electronic data file issued by DigiCert to a person, group, or role in order to confirm your authorization for use of the Private Key corresponding to the Public Key contained in the certificate. You and DigiCert agree as follows:

1. **Use**

1.1. Applicability. These terms cover each Certificate issued by DigiCert to you, regardless of (i) the Certificate type (email, code signing, Direct, or TLS/SSL), (ii) when you request the Certificate, or (iii) when the Certificate actually issues.

1.2. Information. You will provide accurate, complete, and non-misleading information to DigiCert at all times. If any information provided to DigiCert changes or becomes misleading or inaccurate, you will promptly inform DigiCert and update the information. You may not request a certificate with contents that infringe on the intellectual property rights of another entity. All certificate request data is incorporated into this document as part of these terms.

1.3. Key Pairs. A **"Private Key"** means the key that is kept secret by you that is used to create Digital Signatures and/or decrypt electronic records or files that were encrypted with the corresponding Public Key. A "**Public Key**" means your publically disclosed key that is contained in your Certificate and corresponds to the secret Private Key that you use. Subscribers should (i) generate key pairs using trustworthy systems, (ii) use key pairs that are at least the equivalent of RSA 2048 bit keys, (iii) keep all Private Keys confidential, (iv) within one working day, notify DigiCert, cease using the Certificate, and request Certificate revocation if you suspect misuse or compromise of a Private Key, and use reasonable measures to protect Private Keys from disclosure. You will promptly cease using the Certificate and corresponding Private Key upon the earlier of (i) revocation of the Certificate, (ii) termination of this agreement, (iii) expiration of the Certificate, or (iv) industry standards no longer permit use of the Certificate or Private Key. You are solely responsible for any failure to protect your Private Keys. You may only generate and store key pairs for Adobe Signing Certificates and EV Code Signing Certificates on a FIPS 140-2 Level 2 device. All other Certificate types may be stored on secure software or hardware systems.

1.4. Issuance. After you request a Certificate, DigiCert will verify an entity in accordance with DigiCert's CPS and applicable industry standards. If verification is completed to DigiCert's sole satisfaction, then DigiCert will issue the requested Certificate and deliver the Certificate to you using an appropriate delivery mechanism as selected by DigiCert. Typically, DigiCert delivers Certificates either through your online DigiCert account or via a provided email address. DigiCert may refuse to accept a Certificate request or issue a Certificate in its sole discretion. DigiCert will notify you through the account if your request is refused but DigiCert is not required to provide a reason for the refusal.

1.5. IGTF Certificates. The following applies to IGTF Certificates:

(i) Private Key Generation. For IGTF compliant Certificates, you must keep all Private Keys confidential and use reasonable measures to protect the Private Key from disclosure. You must request revocation of the Certificate within one working day of any suspected misuse

or compromise of a Certificate or Private Key. You must generate your key pair using one of the following methods: (i) inside a secure hardware token, (ii) using trustworthy cryptographic software on a local computer system where you are the sole user and administrator, (iii) on a computer system administered by your sponsor or a third party if (a) the key material is generated using trustworthy cryptographic software, (b) access is limited to designated individuals, who are subject to and aware of applicable privacy rules and a professional code of conduct, (c) the private key and pass phrase are not sent in clear text over a network, (d) the encrypted private key file is not sent over the network unprotected, (e) the system is located in a secure environment, where access is controlled and limited to only authorized personnel, and (f) a system does not persistently keep pass phrases or plain text private keys for longer than 24 hours.

(ii) IGTF Private Key Storage. For IGTF compliant Certificates, you may store your Private Key using one of the following methods: (i) protected by a pass phrase on a hardware token from which the Private Key cannot be extracted, (ii) in a persistently encrypted form on a computer system where you are the sole user and administrator, or (iii) on a computer system administered by your sponsor or a third party if (a) the Private Key is stored in a persistently encrypted form and protected by a pass phrase, (b) data needed to decrypt or use the private key is present only as a result of your action and only for as long as you are using the system, (c) administrative access is limited to designated individuals who are subject to and aware of applicable privacy rules and a professional code of conduct, (d) the systems are located in a secure environment, where access is controlled and limited to only authorized personnel, (e) the private key and pass phrase are not sent in clear text over a network, (f) the encrypted private key file is not sent over the network unprotected, and (g) the system does not persistently keep pass phrases or plain text private keys for longer than 24 hours. For IGTF passphrases, you must use pass phrases that are at least 12 characters long and follow the industry's current best practices. If a third party is involved in generating or storing a Private Key, the third party must have a defined data privacy and security policy that provides reasonable assurance of data security. You shall make this policy available to DigiCert upon request.

1.6. SSL and Code Signing Certificates. **"EV Certificate"** means a Certificate that contains the DigiCert Extended Validation Certificate Policy Object Identifier as set forth in the CPS and is issued in accordance with the EV Guidelines. EV Certificates include both SSL Certificates and Code Signing Certificates. **"EV Guidelines"** means the *Guidelines for Extended Validation Certificates* as officially published, amended, and updated by the CA/Browser Forum at http://www.cabforum.org. **"CPS"** refers to DigiCert's written statements of the policies and procedures used to operate its Public Key infrastructure. DigiCert's CPS documents are available at http://www.digicert.com/ssl-cps-repository.htm.

(i) Certificate Transparency. To ensure Certificates function properly throughout their lifecycle, DigiCert may log SSL Certificates with a public certificate transparency database. Because this will become a requirement for Certificate functionality, you cannot opt out of this process. Log server information is publicly accessible. Once submitted, information cannot be removed from a log server.

(ii) Limitations on License. DigiCert may reject any request for an SSL Certificates only for domain names registered to (i) you, (ii) your affiliates, or (iii) an entity that expressly authorized, in writing, you to obtain and manage Certificates for the domain name in the Certificate.

(iii) Certificate Approvers. During the term of this agreement, you expressly authorize the individuals appointed as "Certificate Approvers" or "Administrators" in your account (the designation of which is expressly incorporated into this agreement) to request and approve EV Certificates on your behalf. With respect to DigiCert's obligations under the EV Guidelines and other industry standards, you expressly authorize DigiCert to rely on any

representations made by a Certificate Approver in connection with an ordered Certificate, including verification of your exclusive right to use the domain name listed in the Certificate. You are responsible for all EV Certificates requested by a Certificate Approver until such Certificate Approver's EV authority is revoked. You may revoke a certificate Approver's EV authority by emailing DigiCert at admin@digicert.com. You are responsible for periodically reviewing and updating the individuals authorized to approve EV Certificate orders.

(iv) Representations. You represent that (a) you have the right to use the domain name, common name, and organization name listed in the Certificate (if applicable), (b) if you represent an entity applying for or that will be named in the Certificate, you are expressly authorized to sign this agreement on behalf of that entity and will make the entity aware of each Certificate request, (c) you have read, understand, and agree to the CPS and this agreement, (d) you will make sure the organization included in the Certificate and the registered domain name holder (if a domain name is included the Certificate) will be aware of and approve each Certificate request.

(v) Acceptance. For EV Certificates: By accepting these terms, you are entering into a legally valid and enforceable agreement to obtain a form of digital identity for the Certificate's subject. You acknowledge that you have the authority to obtain the digital equivalent of a company stamp, seal, or (where applicable) officer's signature to establish the authenticity of the subject's website or signed code, and that you are responsible for all uses of its EV Certificate. By accepting this agreement on behalf of the subject, you represent that you (i) are acting as an authorized representative of the subject, (ii) are expressly authorized by subject to sign Subscriber agreements and approve EV Certificate requests on subject's behalf, and (iii) if applicable, have confirmed subject's exclusive right to use the domain(s) to be included in any issued EV Certificates.

1.7. License. Effective immediately after delivery and continuing until the Certificate expires or is revoked, DigiCert grants you a revocable, non-exclusive, non-transferable license to use, for the benefit of the subject, each issued Certificate and the corresponding Key Sets in accordance with the CPS and the terms of this agreement. You are responsible for any use of the Certificate and any equipment and software required to use the Certificate. You may not install or use a Certificate until after you have reviewed and verified the accuracy of the data included in the Certificate. You will promptly inform DigiCert if you become aware of any breach of this agreement or misuse of a Certificate, Private Key, or your account. You are responsible for obtaining and maintaining any authorization or license necessary to use a Certificate.

1.8. Restrictions. You should not (a) share your Certificate or Private Key with another user except where permitted by the CPS, (b) use a Certificate or Private Key to operate nuclear power facilities, air traffic control systems, aircraft navigation systems, weapons control systems, or any other system requiring failsafe operation whose failure could lead to injury, death or environmental damage, (c) modify, sub license, reverse-engineer or create a derivative work of any Certificate (except as required to use the Certificate for its intended purpose) or Private Key, (d) use or make representations about a Certificate except as allowed in the CPS, (e) impersonate or misrepresent your affiliation with any entity or use a Certificate in a manner that could reasonably result in a civil or criminal action being taken against you or DigiCert, (f) use a Certificate to send or receive unsolicited bulk correspondence, sign or distribute any files, software, or code that may damage the operation of another's computer or that is downloaded without a user's consent, or breach the confidence of a third party, (g) attempt to use a Certificate to issue other Certificates, or (h) intentionally create a Private Key that is substantially similar to a DigiCert or third party Private Key.

1.9. Revocation. DigiCert may revoke a Certificate without notice for the reasons stated in the CPS, including if DigiCert believes that (a) you or the subject requested revocation of the Certificate or did not authorize the Certificate's issuance, (b) you or the subject breach this agreement or fail to comply with the CPS, (c) a provision of this agreement containing a representation or obligation

related to the issuance, use, management, or revocation of the Certificate terminates or is held invalid, (d) you or the subject are added to a government prohibited person or entity list or are operating from a prohibited destination under the laws of the United States, (e) the Certificate contains inaccurate or misleading information, (f) the Certificate was used outside of its intended purpose or used to sign malicious software, (g) the Private Key associated with a Certificate was disclosed or compromised, (h) this agreement terminates, (i) the Certificate was used or issued, directly or indirectly, contrary to law, the CPS, or industry standards, (j) industry standards or DigiCert's CPS require revocation, or (k) revocation is necessary to protect the rights, confidential information, operations, or reputation of DigiCert or a third party.

1.10. Renewals. DigiCert may send a reminder to you about expiring Certificates, but you are solely responsible for ensuring your Certificates are renewed prior to their expiration.

1.11. Publication of Certificate. You consent to (i) DigiCert's public disclosure of information embedded in an issued Certificate, and (ii) DigiCert's transfer of your information to servers located inside the United States. DigiCert retains a right to use any information provided through the account, provided that all such use is in compliance with its privacy policy as provided on its website. DigiCert may modify the privacy policy in its sole discretion.

1.12. Express Install. DigiCert's may provide an express installation utility as part of its services. Using this utility will automatically configure server settings as appropriate to use the Certificate. A link to express install is provided either in the email providing notification of Certificate issuance or on DigiCert's website. You may (i) not modify, sub-license, reverse engineer, or create a derivative work of the utility and (ii) only use the utility with a DigiCert product or service and not with Certificates, software, or other products or services provided from a third party. You are solely liable for any use of the utility. DIGICERT HEREBY DISCLAIMS ALL WARRANTIES ASSOCIATED WITH THE UTILITY AND ALL LIABILITY FOR YOUR USE OF THE UTILITY.

2. **Term and Termination**

2.1. Term. This agreement is effective upon your acceptance and lasts until the earlier of (i) the expiration date of all Certificates issued under this agreement, or (ii) the termination of this agreement by a party as allowed herein. All rights and licenses granted to you terminate immediately upon termination of this agreement.

2.2. Termination. Either party may terminate this agreement for convenience by providing 30 days prior notice to the other party. DigiCert may terminate the agreement immediately for any reasonable reason related to this Agreement, including, but not limited to (i) you or the subject materially breach this agreement, (ii) you or the subject engaged in illegal or fraudulent activity or an activity that could materially harm DigiCert's business, (iii) DigiCert cannot verify you or the subject to DigiCert's sole satisfaction, or (iv) if you or the subject (a) have a receiver, trustee, or liquidator appointed over substantially all of your or the subject's assets, (b) have an involuntary bankruptcy proceeding filed against you or the subject that is not dismissed within 30 days of filing, (c) file a voluntary petition of bankruptcy or reorganization.

2.3. Survival. All provisions of this agreement that, by their nature, are intended to survive termination of the agreement and continue in full force and effect, including all provisions related to representations by you under the following sections: Publication of Certificate (Section 1.11), Disclaimer of Warranties and Limitations on Liability (Section 3), Indemnity (Section 4), Arbitration (section 5), and the Miscellaneous provisions (Section 6).

3. **Disclaimers of Warranty and Limitations on Liability**

3.1. Relying Party Warranties. You acknowledge that any applicable Relying Party Warranty is only for the benefit of Relying Parties. You do not have rights under the warranty, including any right to enforce the terms of the warranty or make a claim under the warranty. Not all Certificates are

covered by a warranty. **"Relying Party"** means an entity that acts in reliance on a Certificate or a Digital Signature. An Application Software Vendor is not a Relying Party when the software distributed by the Application Software Vendor merely displays information regarding a Certificate or facilitates the use of the Certificate or digital signature. "**Relying Party Warranty**" is a warranty provided by DigiCert against certificate mis-issuance that is available only to Relying Parties who meet the conditions and fulfill all of the terms set forth at http://www.digicert.com/docs/agreements/DigiCert_RPA.pdf. **"Application Software Vendor"** means a software developer that displays or uses Certificates and distributes root certificates.

3.2. Remedy. Your sole remedy for a defect in a Certificate is to have DigiCert use reasonable efforts to correct the defect. DigiCert is not obligated to correct a defect if (i) the Certificate was misused, damaged, or modified, (ii) you did not promptly report the defect to DigiCert, or (iii) you breached any provision of this agreement.

3.3. Warranty Disclaimers. THE CERTIFICATES, AND ANY RELATED SOFTWARE, PRODUCTS, AND SERVICES, INCLUDING THE EXPRESS INSTALL UTILITY, ARE PROVIDED "AS IS" AND "AS AVAILABLE". TO THE MAXIMUM EXTENT PERMITTED BY LAW, DIGICERT DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. DIGICERT DOES NOT WARRANT THAT ANY SERVICE OR PRODUCT WILL MEET YOUR EXPECTATIONS OR THAT ACCESS TO THE ACCOUNT WILL BE TIMELY OR ERROR-FREE. DigiCert does not guarantee the availability of any products or services and may modify or discontinue any product or service offering at any time.

3.4. Limitation on Liability. This agreement does not limit a party's liability for (i) death or personal injury resulting from the negligence of a party, or (ii) fraud or fraudulent statements made by a party. EXCEPT AS STATED ABOVE, DIGICERT'S MAXIMUM LIABILITY RESULTING FROM THESE TERMS IS LIMITED TO THE AMOUNT PAID OR PAYABLE BY YOU TO DIGICERT DURING THE 12 MONTHS PRIOR TO WHEN THE EVENT GIVING RISE TO THE LIABILITY OCCURRED. DIGICERT IS NOT LIABLE FOR ANY INDIRECT, CONSEQUENTIAL, SPECIAL, OR PUNITIVE DAMAGES OR ANY LOSS OF PROFIT, REVENUE, DATA, OR OPPORTUNITY, EVEN IF DIGICERT IS AWARE OF THE POSSIBILITY OF SUCH DAMAGES.

3.5. Liability. You are liable for any claims (including damages, costs, and defense expenses) that are brought by third parties against DigiCert, its agents and assigns, that are result from use of your Certificate or Private Key or that are caused by your intentional or grossly negligent breach of this agreement. DigiCert is not responsible for your employees or agents, including any expenses owed to them.

3.6. Extent. The limitations in this section apply to the maximum extent permitted by law and apply regardless of (i) the reason for or nature of the liability, including tort claims, (ii) the number of claims of liability, (iii) the extent or nature of the damages, or (iv) whether any other provisions of this agreement were breached or proven ineffective.

4. Indemnity

4.1. Obligation. You will indemnify, hold harmless, and defend DigiCert and its employees, officers, directors, shareholders, affiliates, and assigns against all third party claims and all related liabilities, damages, and costs, including reasonable attorneys' fees, arising from (i) your breach of this agreement, (ii) your failure to disclose a material fact related to the issuance of a Certificate or to protect the Authentication Mechanisms used to secure the account, (iii) an allegation that your actions or negligence was the cause of the claim, liability, or cost, (iv) your website, products, and services, or (v) your use of DigiCert's products or services to infringe on the rights of a third party.

4.2. Indemnification Procedure. An entity seeking indemnification under this agreement ("**Indemnified Party**") must notify you promptly of any event requiring indemnification. However, an Indemnified Party's failure to notify will not relieve you from your indemnification obligations, except to the extent that the failure to notify materially prejudices you. You may assume the defense of any proceeding requiring indemnification unless assuming the defense would result in potential conflicting interests as determined by the Indemnified Party in good faith. An Indemnified Party may, at your expense, defend itself until your counsel has initiated a defense of the Indemnified Party. Even after you assume the defense, the Indemnified Party may participate in any proceeding using counsel of its own choice and at its own expense. You may not settle any proceeding related to this agreement unless the settlement also includes an unconditional release of liability for all Indemnified Parties.

4.3. Additions to and Limitations on Liability. Your indemnification obligations are not DigiCert's sole remedy under this agreement and are in addition to any other remedies that DigiCert may have against you. You must commence any claim or action arising from this agreement within one year from the occurrence of events giving rise to a cause of action. You waive your right to any claim that is commenced more than one year from the first date on which the cause of action arose.

5. **Arbitration**

5.1. Requirement. To the maximum extent permitted by law, you will settle any dispute or claim related to this agreement, the CPS, DigiCert's websites, or any Certificate issued under this Agreement using binding arbitration in accordance with the Arbitration Rules of the American Arbitration Association (AAA). The parties shall hold all arbitration proceedings in Lehi, Utah. The parties shall settle all such disputes and claims settled in this manner in lieu of any action at law or equity; except that nothing in this subsection precludes a party from bringing an action for injunctive relief or other equitable relief.

5.2. Proceeding. During arbitration, the parties shall use a single arbitrator appointed by the AAA to arbitrate a dispute or claim. The arbitrator must exhibit a reasonable familiarity with the issues. The award of the arbitrator is binding and final upon all parties. Either party may have a court with proper jurisdiction enter the award. This agreement remains in full force and effect while the outcome of the arbitration proceeding is pending. The arbitrator shall follow applicable law in conducting the arbitration.

5.3. Costs. A party shall pay any costs, including reasonably attorney fees, to which the arbitrator determines that the prevailing party is entitled. Each party shall pay its own costs associated with the arbitration if such costs are not awarded by the arbitrator. The arbitrator may not award punitive damages or speculative damages to either party and does not have the power to amend this agreement.

6. **Miscellaneous**

6.1. Agreement. Unless explicitly stated otherwise, this agreement, along with all documents referred to herein, constitutes the entire agreement between the parties with respect to the issuance and use of the requested Certificate, superseding all other agreements that may exist with respect to that particular Certificate. DigiCert may amend any of its (i) website and any documents listed thereon, (ii) CPS, (iii) fees, (iv) privacy policy, or (iv) the conditions under which you receive a Certificate. Amendments are effective upon the earlier of DigiCert's posting the amendment on its website or your receipt of the amendment. You must periodically review DigiCert's website to be aware of any changes to this agreement or the relevant documents. Your continued use of a Certificate after an amendment is posted constitutes your acceptance of the amendment. If a law or industry standard changes and that change affects the Certificates or other services provided under this agreement, then DigiCert may amend this agreement to the extent necessary to comply with the change. The laws of the state of Utah govern the interpretation, construction,

and enforcement of this agreement and all matters related to it, including tort claims, without regards to any conflicts-of-laws principles. The parties hereby submit to the exclusive jurisdiction of and venue in the state and federal courts located in the State of Utah.

6.2. Waiver. A party's failure to enforce or delay in enforcing a provision of this agreement does not waive (i) the party's right to enforce the same provision later, or (ii) the party's right to enforce any other provision of the agreement. A waiver is only effective if in writing and signed by the party against whom the waiver is claimed.

6.3. Industry Standards. Both parties will comply with all industry and privacy standards applicable to the Certificates. If industry standards change, DigiCert and you will work together in good faith to amend this agreement to comply with the changes.

6.4. Force Majeure and Internet Frailties. Neither party is liable for any failure or delay in performing its obligations under this agreement to the extent that the circumstances causing such failure or delay are beyond a party's reasonably control. You acknowledge that the Certificates are subject to the operation and telecommunication infrastructures of the Internet and the operation of your Internet connection services, all of which are beyond DigiCert's control.

6.5. Notices. You must send all notices in English writing by first class mail with return receipt request to DigiCert, Inc. at 2600 West Executive Parkway, Suite 500, Lehi, Utah 84043. DigiCert will send notices to you either, in DigiCert's discretion, through the account or through your email address (as provided by you). Notices to DigiCert are effective when received. Notices to you are effective when sent.

6.6. Assignment. You may not assign your rights or obligations under this agreement without the prior written consent of DigiCert. Any transfer without consent is void. DigiCert may assign its rights and obligations without your consent.

6.7. Severability. The invalidity or unenforceability of a provision under this agreement, as determined by a court or administrative body of competent jurisdiction, does not affect the validity or enforceability of the remainder of this agreement. The parties will substitute any invalid or unenforceable provision with a valid or enforceable provision that achieves the same economic, legal, and commercial objectives as the invalid or unenforceable provision.

6.8. Rights of Third Parties**.** Application Software Vendors and Relying Parties are express third party beneficiaries of your obligations and representations under this agreement that directly relate to the use or issuance of a Certificate. Other than the Application Software Vendors and Relying Parties, no third parties have any rights or remedies under the agreement.

6.9. Interpretation**.** The definitive version of this agreement is written in English. If this agreement is translated into another language and there is a conflict between the English version and the translated version, the English language version controls.

ACCEPTANCE

BY CHECKING "I AGREE", YOU ACKNOWLEDGE THAT YOU HAVE READ AND UNDERSTAND THIS AGREEMENT AND THAT YOU WILL TO COMPLY WITH ITS TERMS. DO NOT CHECK "I AGREE" AND DO NOT PROCEED IF YOU DO NOT ACCEPT THIS AGREEMENT.