

TCS Certificate Terms of Use*Consolidated version – customarily presented to Applicants and Subscribers in electronic form*

Page 1/2

The following terms apply to the use of any Certificate provided under this agreement. These terms survive any termination of this agreement until all Certificates are revoked or expired.

1. **Information.** The Subscriber must provide accurate, complete, and non-misleading information to DigiCert at all times. If any information provided to DigiCert changes or becomes misleading or inaccurate, the Subscriber must promptly inform DigiCert and update the information.
2. **Key Pairs.** The Subscriber must (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 the Subscriber suspects misuse or Compromise of a Private Key, and use reasonable measures to protect Private Keys from disclosure. The Subscriber must 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. The Subscriber is solely responsible for any failure to protect its Private Keys. The Subscriber may only generate and store key pairs for Adobe Signing Certificates and EV Code Signing Certificates on a FIPS 140-2 Level 2 device. Private keys of all other Certificate types may be stored on secure software or hardware systems.
3. **Review.** The Subscriber may not install or use a Certificate until after it has reviewed and verified the accuracy of the data included in the Certificate. The Subscriber must promptly inform DigiCert if the Subscriber becomes aware of any breach of this agreement or misuse of a Certificate, Private Key, or its account.
4. **SSL 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>.
5. **Limitations on License.** A Subscriber may request SSL Certificates only for domain names registered to (i) the Subscriber, (ii) Subscriber’s affiliates, or (iii) an entity that expressly authorized the Subscriber, in writing, to obtain and manage Certificates for the domain name in the Certificate.
6. **Certificate Approvers.** During the term of this agreement, the Subscriber expressly authorizes the individuals appointed as “Certificate Approvers” or “Administrators” in Subscriber’s account (the designation of which is expressly incorporated into this agreement) to request and approve EV Certificates on behalf of the Subscriber. With respect to DigiCert’s obligations under the EV Guidelines and other industry standards, the Subscriber expressly authorizes 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. The Subscriber is responsible for all EV certificates requested by a Certificate Approver until such Certificate Approver’s EV authority is revoked. A Subscriber may revoke a certificate Approver’s EV Authority by emailing DigiCert at admin@digicert.com. The Subscriber must periodically review and update the individuals authorized to approve EV Certificate orders.
7. **Representations.** The Subscriber represents that (a) the Subscriber has the right to use the domain name, common name, and organization name listed in the Certificate (if applicable), (b) if Subscriber represents an entity applying for or that will be named in the Certificate, then the Subscriber is expressly authorized to sign this agreement on behalf of that entity and will make the entity aware of each Certificate request, (c) the Subscriber has read, understood, and agreed to the CPS and this agreement, (d) the Subscriber 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.
8. **Acceptance.** For EV Certificates: By ordering a Certificate, the Subscriber is entering into a legally valid and enforceable agreement to obtain a form of digital identity. The requester acknowledges that he/she has the authority to obtain the digital equivalent of a company stamp, seal, or (where applicable) officer’s signature to establish the authenticity of the Certificate’s Subject (“Subject”) website or signed code, and that the Subscriber is responsible for all uses of its EV Certificate. By accepting this agreement on behalf of the Subject, the Subscriber represents that he/she (i) is acting as an authorized representative of the Subject, (ii) is expressly authorized by the Subject to agree to the applicable terms and approve EV Certificate requests on behalf of the Subject, and (iii) if applicable, has confirmed the Subject’s exclusive right to use the domain(s) to be included in any issued EV Certificates.
9. **Publication of Certificate.** The Subscriber consents to (i) DigiCert’s public disclosure of information embedded in an

issued Certificate, and (ii) DigiCert's transfer of Subscriber's 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 CPS and applicable privacy laws. Except where such information is included as part of the Certificate, DigiCert shall treat information submitted to it through an Account as Confidential Information and protect all such information from disclosure.

10. Rights of Third Parties. Application Software Vendors and Relying Parties are express third party beneficiaries of Subscriber's obligations and representations with respect to the Certificate.