digicert®

DIGITAL CERTIFICATES BY DIGICERT – TERMS OF USE

These Digital Certificates Terms of Use ("**Certificate Terms of Use**") apply to each digital certificate ("**Certificate**"), regardless of Certificate type, whether publicly-trusted TLS/SSL Certificates, Client Certificates (as defined in Section 9), Qualified Certificates (as defined in Section 10), X9 Certificates (as defined in Section 29), or otherwise, issued by DigiCert, Inc., a Utah corporation or any of its affiliates, including its Qualified Trust Service Providers (collectively, "**DigiCert**") to an entity or person ("**Customer**"), as identified in the DigiCert services management portal and/or related API made available to Customer ("**Portal**") or issued Certificate. The Certificate Terms of Use apply regardless of when Customer requested the Certificate or when the Certificate is issued. The account to access and use the Portal on Customer's behalf is referred to herein as the "**Portal Account**."

By accepting or signing an agreement that incorporates these Certificate Terms of Use by reference (such agreement, together with these terms, collectively, the "**Agreement**"), the accepter or signer (the "**Signer**") represents and warrants that he/she (i) is acting as an authorized representative of the Customer on whose behalf the Signer is accepting this Agreement, and is expressly authorized to sign the Agreement and bind Customer to the Agreement, (ii) has the authority to obtain the digital equivalent of a company stamp, seal, or officer's signature to establish (x) the authenticity of Customer's website, and (y) that Customer is responsible for all uses of the Certificate, (iii) is expressly authorized by Customer to approve Certificate requests on Customer's behalf, and (iv) has or will confirm Customer's exclusive right to use the domain(s) to be included in any issued Certificates.

With respect to any Certificates issued by DigiCert to Customer hereunder, the parties acknowledge and agree that the Certificate Terms of Use together with the Agreement constitutes the subscriber agreement, as required under the applicable industry standards, guidelines and requirements related to the issuance of Certificates (including the EV Guidelines, as defined below).

Customer and DigiCert hereby agree as follows:

1. Account Users.

Customer authorizes each individual listed as an administrator in the Portal Account to act as a Certificate Requester, Certificate Approver, and Contract Signer (as defined in the EV Guidelines) and to communicate with DigiCert regarding the management of Certificates and key sets. "**EV Guidelines**" means the Extended Validation Guidelines published by the CA/Browser Forum ("**CAB Forum**") and made publicly available at www.cabforum.org. Customer may revoke this authority by sending notice to DigiCert. Customer is responsible for periodically reviewing and reconfirming which individuals have authority to request and approve Certificates. If Customer wishes to remove a Portal Account user, Customer will take the steps necessary to prevent such user's access to the Portal, including changing its password and other authentication mechanisms for its Portal Account. Customer must notify DigiCert immediately if any unauthorized use of the Portal or Portal Account is detected. Customer affirms that: (i) Customer authorizes DigiCert to scan, gather, and collect data pertinent to DigiCert's services and to automate Certificate renewal and upgrade; (ii) Customer will use the services to scan and automate only the domains, IP addresses, or assets that Customer owns or controls; (iii) Customer will use the services only for its intended purpose as described and marketed by DigiCert and in accordance with the DigiCert Acceptable Use Policy located at https://www.digicert.com/legal-repository.

2. Requests.

Customer may request Certificates only for domain names registered to Customer, an affiliate of Customer, or other entity that expressly authorizes DigiCert to allow Customer to obtain and manage Certificates for the domain name. DigiCert may limit the number of domain names that Customer may include in a single Certificate in DigiCert's sole discretion.

3. Verification.

After receiving a request for a Certificate from Customer, DigiCert will review the request and attempt to verify the relevant information in accordance with the DigiCert Certification Practices Statement and applicable industry standards, guidelines and requirements, including laws and regulations related to the issuance of Certificates ("**Industry Standards**"). Verification of such requests is subject to DigiCert's sole discretion, and DigiCert may refuse to issue a Certificate for any reason or no reason. DigiCert will notify Customer if a Certificate request is refused but DigiCert is not required to provide a reason for the refusal. **"Certificate Practices Statement"** or **"CPS"** means the applicable written statements of the policies and practices used by DigiCert to operate its public key infrastructure ("**PKI**"), including applicable Time-Stamp Policies and

Statements. DigiCert's CPSs are available at https://www.digicert.com/legal-repository. CPSs for services issued from a QTSP (whether acting in its capacity as a QTSP or otherwise) or an affiliate entity are available at https://www.quovadisglobal.com/repository.

4. Certificate Life Cycle.

The lifecycle of an issued Certificate depends on the selection made by Customer when ordering the Certificate, the requirements in the CPS, and the intended use of the Certificate. DigiCert may modify Certificate lifecycles for unissued Certificates as necessary to comply with requirements of: (i) the Agreement; (ii) Industry Standards; (iii) DigiCert's auditors; or (iv) an Application Software Vendor. "**Application Software Vendor**" means an entity that displays or uses Certificates in connection with a distributed root store in which DigiCert participates or will participate. Customer agrees to cease using a Certificate and its related Private Key (defined below) after the Certificate's expiration date or after DigiCert revokes a Certificate as permitted in the Agreement.

5. Issuance.

If verification of a Certificate is completed to DigiCert's satisfaction, DigiCert will issue and deliver the requested Certificate to Customer using any reasonable means of delivery. Typically, DigiCert will deliver Certificates via email to an address specified by Customer as an electronic download in the Portal or in response to an API call made by Customer via the Portal. Publicly-trusted Certificates are issued from a root or intermediate Certificate selected by DigiCert. DigiCert may change which root or intermediate certificate is used to issue Certificates at any time and without notice to Customer. Customer will abide by all applicable laws, regulations and Industry Standards when ordering and using Certificates, including United States export control and economic sanctions laws and regulations. Customer acknowledges that the Certificates are not available in countries or regions restricted by the United States Treasury Department's Office of Foreign Assets Control, the United States Commerce Department, the European Commission, the United Kingdom HM Treasury's Office of Financial Sanctions Implementation, or other applicable governmental agencies having jurisdiction over DigiCert.

6. Certificate License.

Effective immediately upon initiating a request for a Certificate and continuing until the Certificate expires or is revoked, Customer may only use, for the benefit of the Certificate's subject, each issued Certificate and related services (whether performed before or after issuance of the Certificate) and corresponding Key Set for the purposes described in the CPS, in accordance with all applicable laws, regulations, Industry Standards, and with the terms herein. Any Certificates trusted by Application Software Vendors are subject to all applicable Industry Standards requirements, including those found in applicable Application Software Vendor root store policies and the CPS, regardless of how the Certificates are used. Any use that is not allowed by applicable Industry Standards or the CPS is not permitted. DigiCert strongly discourages certificate or key pinning, using Certificates trusted for the web with non-web PKI, or any other use of Certificates that would make it difficult for Customer to meet the revocation timelines or other requirements of the CPS, and any such use will not be considered a sufficient reason to delay revocation. "**Key Set**" means a set of two or more mathematically related keys, referred to as Private Keys or key shares along with a Public Key, wherein (i) the Public Key can encrypt a message which only the Private Key(s) can decrypt, and (ii) even knowing the Public Key, it is computationally infeasible to discover the Private Key(s). Customer will promptly inform DigiCert if it becomes aware of any misuse of a Certificate, Private Key, or the Portal. Customer is responsible for obtaining and maintaining any authorization or license necessary to order, use, and distribute a Certificate to end users and systems, including any license required under United States' export laws. SSL Certificates may be used on one or more physical server or device at a time; however, DigiCert may charge a fee for use of Certificates on additional servers or devices.

7. Key Sets.

A "**Private Key**" means the key that is kept secret by Customer 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 Customer's publicly-disclosed key that is contained in Customer's Certificate and corresponds to the secret Private Key that Customer uses. Customer must (i) generate Key Sets using trustworthy systems, (ii) use Key Sets that are at least the equivalent of RSA 2048 bit keys, and (iii) keep all Private Keys confidential. Customer is solely responsible for any failure to protect its Private Keys. Customer represents that it will only generate and store Key Sets 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. Customer is responsible for ensuring that Customer's acquisition, use, or acceptance of Key Sets generated by DigiCert in accordance with the Agreement complies with applicable local laws, rules and regulations – including but not

limited to export and import laws, rules, and regulations – in the jurisdiction in which Customer acquires, uses, accepts or otherwise receives such Key Sets. If Customer is permitted to import or export Private Keys (including copies) in connection with its use of specific DigiCert services, DigiCert will not be liable to Customer for Customer's use or storage of Private Keys (including copies) that are not created in the applicable Portal or service or that are used outside such Portal or service, including after they are exported from the applicable Portal or service.

8. Publication of Certificate Information.

Notwithstanding anything in these Certificate Terms of Use or any other agreement between Customer and DigiCert to the contrary, Customer consents to: (i) DigiCert's public disclosure of information (such as Customer's domain name, jurisdiction of incorporation, or contact information), embedded in an issued Certificate; and (ii) Customer's Certificates and information embedded therein being logged by or on behalf of DigiCert in publicly-accessible Certificate transparency databases for purposes of detecting and preventing phishing attacks and other forms of fraud, and Customer agrees that such information when logged may not be removed from a log server. Such publication of Certification information will be in accordance with the applicable CPS.

9. Client Certificates.

"**Client Certificate**" means a Certificate that contains any extendedKeyUsage other than codeSigning, timestamping or serverAuthentication. The Client Certificate uses are varied and are defined by the Client Certificate profile. Some of the possible uses defined in a Client Certificate profile may include, digital signature, email encryption, and cryptographic authentication. If Customer wishes to request Client Certificates, Customer must (i) confirm the identity and affiliation of the requester using appropriate internal documentation as prescribed the CPS, and (ii) confirm that the information provided and representations related to or incorporated in any Client Certificate are true, complete, and accurate in all material respects.

10. Qualified Certificates.

"**Qualified Certificate**" means a Certificate (i) that is issued by a Qualified Trust Service Provider pursuant to the requirements of applicable EU or Swiss certification and electronic signature laws, and (ii) that carries the highest assurance level of "qualified" pursuant to such requirements.

"**Qualified Trust Service Provider**" or "**QTSP**" means an affiliate entity of DigiCert that is certified by governmental authorities to issue Qualified Certificates. DigiCert's QTSP's are as follows:

QTSP Entity	**Trusted List**	**Jurisdiction of Supervisory Body**
QuoVadis Trustlink B.V.	Netherlands Trusted List	Netherlands
DigiCert Europe Belgium B.V.	Belgium Trusted List	Belgium
QuoVadis Trustlink Schweiz AG	Swiss Trusted List	Switzerland

"**QTSP Services**" means Services issued by DigiCert's QTSP (as defined above) (whether acting in its capacity as QTSP or otherwise) or its Affiliates.

If Customer purchases QTSP Services, then the applicable CPS for certain such QTSP Services is located at https://www.quovadisglobal.com/repository/. With respect to Qualified Certificates, Customer will (i) where use of a Qualified Signature Creation Device (QSCD) is required by Industry Standards, only use its Qualified Certificates for electronic signatures generated using the QSCD storing the Qualified Certificates, (ii) if Customer is a natural person, maintain and use their Private Keys only under their sole control; and (iii) if Customer is a legal entity or organization, maintain and use its Private Keys only under its control and direction.

11. Management.

DigiCert will generally issue, manage, renew, and revoke a Certificate in accordance with any instructions submitted by Customer through the Portal and may rely on such instructions as accurate. Customer will provide accurate and complete information when communicating with DigiCert and will notify DigiCert within 5 Business Days if any information relating to its account on the Portal changes. Customer will respond to any inquiries from DigiCert regarding the validity of information provided by Customer within 5 Business Days after Customer receives notice of the inquiry. Customer will review and verify the Certificate data prior to using the Certificate for accuracy. Certificates are considered accepted by Customer thirty (30) days after the Certificate's issuance, or earlier upon use of the Certificate when evidence exists that the

Customer used the Certificate. Although DigiCert may send a reminder about expiring Certificates, DigiCert is under no obligation to do so and Customer is solely responsible for ensuring Certificates are renewed prior to expiration. "**Business Day**" means Monday through Friday, excluding U.S. Federal Holidays, which are set forth in 5 U.S.C. § 6103.

12. Registration Authority.

Except for publicly-trusted TLS/SSL Certificates and Qualified Certificates, Customer is appointed as a Registration Authority (and Customer hereby accepts such appointment) pursuant to the terms of the applicable CPS. In connection with publicly-trusted TLS/SSL Certificates, Customer is appointed as an Enterprise RA (and Customer hereby accepts such appointment) pursuant to the terms of the applicable CPS. To the extent that Customer performs any functions of a Registration Authority or Enterprise RA, it will do so in compliance with the applicable CPS, and DigiCert may rely on Customer's actions when acting as a Registration Authority or Enterprise RA. To the extent any third-party claim, suit, proceeding or judgment arises from Customer's failure to strictly comply with the obligations of a Registration Authority or Enterprise RA, Customer must defend, hold harmless, and indemnify DigiCert and its directors, officers, agents, employees, successors and assigns from such claim. If operating as a Registration Authority or Enterprise RA, Customer will cause its subscribers receiving Certificates hereunder to abide by the terms of the DigiCert subscriber agreement, found at https://www.digicert.com/subscriber-agreement. Subscribers of Customer must accept the subscriber agreement before receiving Certificates. "**Enterprise RA**" has the meaning given to it in the current version of the CAB Forum Baseline Requirements, available at https://cabforum.org/baseline-requirements-documents/, as updated from time to time.

13. Security and Use of Key Sets.

Customer will securely generate and protect the Key Sets associated with a Certificate and take all steps necessary to prevent the compromise, loss, or unauthorized use of a Private Key associated with a Certificate. Customer will use passwords that meet the requirements specified by the CAB forum network security requirements and other relevant requirements to meet best practices. Customer will only allow Customer's employees, agents, and contractors to access or use Private Keys if the employee, agent, or contractor has undergone a background check by Customer (to the extent allowed by law) and has training or experience in PKI and other information security fields. Customer will notify DigiCert, request revocation of a Certificate and its associated Private Key, cease using such Certificate and its associated Private Key, and remove the Certificate from all devices where it is installed if: (i) any information in the Certificate is or becomes incorrect or inaccurate, or (ii) there is any actual or suspected misuse or compromise of the Private Key associated with the Public Key included in the Certificate. For code signing Certificates, Customer will promptly cease using a Certificate and its associated Private Key and promptly request revocation of the Certificate if Customer believes that (a) any information in the Certificate is, or becomes, incorrect or inaccurate, (b) the Private Key associated with the Public Key contained in the Certificate was misused or compromised, or (c) there is evidence that the Certificate was used to sign Suspect Code. "**Suspect Code**" means code that contains harmful or malicious functionality of any kind or that contains 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. Customer will not use the same Private Key for different Certificate types. For example, Customer will not use a Private Key that is used for code signing to request a non-code signing Certificate. If DigiCert detects that a Private Key that has been used for a certain Certificate type or action (e.g., code signing) is being used to request a different Certificate type (e.g., TLS/SSL or Client Certificate), then DigiCert will be required to revoke all Certificates associated with such Private Key or related Key Set that are in Customer's related Portal Account or that have otherwise been issued by DigiCert. Customer will respond to DigiCert's instructions concerning Key Set compromise or Certificate misuse within 24 hours. Customer will promptly cease using the Key Set corresponding to a Certificate upon the earlier of (I) revocation of the Certificate, and (II) the date when the allowed usage period for the Key Set expires. After revocation, Customer must cease using the Certificate.

If Customer stores a Private Key that has been generated for a code signing Certificate in an HSM (as defined in the applicable CPS), then Customer agrees with respect to each such Private Key that (w) Customer stores its Private Key securely in an HSM that prevents removal of the Private Key, (x) the HSM is either in sole control of Customer or utilized through an audited cloud (e.g., Azure or AWS), (y) Customer has no cause to believe such Private Key has been or ever will be used outside of the HSM, and (z) the Private Key is protected in a crypto module that meets or exceeds FIPS 140-2 level 2 (or equivalent) or Common Criteria EAL4+.

14. Defective Certificates.

Customer's sole remedy for a defect in a Certificate ("**Defect**") is to require DigiCert to use commercially reasonable efforts to cure the defect after receiving notice of such Defect from Customer. DigiCert is not obligated to correct a Defect if (i)

Customer misused, damaged, or modified the Certificate, (ii) Customer did not promptly report the Defect to DigiCert, or (iii) Customer has breached any provision of the Agreement.

15. Relying Party Warranty.

Customer acknowledges that the Relying Party Warranty is only for the benefit of Relying Parties. "**Relying Party Warranty**" means a warranty offered to a Relying Party that meets the conditions found in the Relying Party Agreement and Limited Warranty posted on DigiCert's website at https://www.digicert.com/legal-repository. The Relying Party Warranty for Certificates issued from a QTSP or a DigiCert affiliate is posted at https://www.quovadisglobal.com/repository. Customer does not have rights under the Relying Party Warranty, including any right to enforce the terms of the Relying Party Warranty or make a claim under the Relying Party Warranty. "**Relying Party**" has the meaning set forth in the Relying Party Warranty. 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.

16. Representations.

For each requested Certificate, Customer represents and warrants that:

a. Customer has the right to use or is the lawful owner of (i) any domain name(s) specified in the Certificate, and (ii) any common name or organization name specified in the Certificate;

b. Customer will use the Certificate only for authorized and legal purposes, including not using the Certificate to sign Suspect Code and will use the Certificate and Private Key solely in compliance with all applicable laws and solely in accordance with the Certificate purpose, the CPS, any applicable certificate policy, and the Agreement;

c. Customer has read, understands, and agrees to the CPS;

d. Customer will immediately report in writing to DigiCert any non-compliance with the CPS or Baseline Requirements; and

e. the organization included in the Certificate and the registered domain name holder is aware of and approves of each Certificate request.

17. Restrictions.

Customer will only use a TLS/SSL Certificate on the servers accessible at the domain names listed in the issued Certificate. Additionally, Customer will not:

a. modify, sublicense, or create a derivative work of any TLS/SSL Certificate (except as required to use the Certificate for its intended purpose) or Private Key;

b. upload or distribute any files or software that may damage the operation of another's computer;

c. make representations about or use a TLS/SSL Certificate except as allowed in the CPS;

d. impersonate or misrepresent Customer's affiliation with any entity;

e. use a Certificate or any related software or service (such as the Portal) in a manner that could reasonably result in a civil or criminal action being taken against Customer or DigiCert;

f. use a Certificate or any related software to breach the confidence of a third party or to send or receive unsolicited bulk correspondence;

g. use code signing Certificates to sign Suspect Code;

h. apply for a code signing Certificate if the Public Key in the Certificate is or will be used with a non-code signing Certificate;

i. interfere with the proper functioning of the DigiCert website or with any transactions conducted through the DigiCert website;

j. attempt to use a Certificate to issue other Certificates;

k. monitor, interfere with or reverse engineer the technical implementation of the DigiCert systems or software or otherwise knowingly compromise the security of the DigiCert systems or software;

l. submit Certificate information to DigiCert that infringes the intellectual property rights of any third party; or

m. intentionally create a Private Key that is substantially similar to a DigiCert or third-party Private Key.

n. Unless expressly authorized by DigiCert, in writing, Customer will not use any end-entity Certificate to sign any Certificate.

18. Certificate Revocation.

DigiCert may revoke a Certificate without notice for the reasons stated in the CPS, including if DigiCert reasonably believes that:

a. Customer requested revocation of the Certificate or did not authorize the issuance of the Certificate;

b. Customer is using the Services, to post or make accessible any material that infringes DigiCert's or any third party's rights;

c. Customer has breached the Agreement or an obligation it has under the CPS;

d. any provision of an agreement with Customer containing a representation or obligation related to the issuance, use, management, or revocation of the Certificate terminates or is held invalid;

e. Customer is added to a government prohibited person or entity list or is operating from a prohibited destination under the laws of the United States;

f. the Certificate contains inaccurate or misleading information;

g. the Certificate was used without authorization, outside of its intended purpose or used to sign Suspect Code;

h. the Private Key associated with the Certificate was disclosed or compromised;

i. the Certificate was (i) misused, (ii) used or issued contrary to law, the CPS, or Industry Standards, or (iii) used, directly or indirectly, for illegal or fraudulent purposes, such as phishing attacks, fraud, or the distribution of malware, other illegal or fraudulent purposes, or any other violations as outlined in the DigiCert Acceptable Use Policy; or

j. Industry Standards or DigiCert's CPS require Certificate revocation, or revocation is necessary to protect the rights, confidential information, operations, or reputation of DigiCert or a third party.

19. Sharing of Information.

Customer acknowledges and accepts that if (i) the Certificate or Customer is identified as a source of Suspect Code, (ii) the authority to request the Certificate cannot be verified, or (iii) the Certificate is revoked for reasons other than Customer request (e.g. as a result of private key compromise, discovery of malware, etc.), DigiCert is authorized to share information about Customer, any application or object signed with the Certificate, the Certificate, and the surrounding circumstances with other certification authorities or industry groups, including the CAB Forum.

20. Industry Standards.

Both parties will comply with all Industry Standards and laws that apply to the Certificates; if such an applicable law or Industry Standard changes and that change affects the Certificates or other services provided under the Agreement, then DigiCert may alter the services or amend or terminate the Agreement to the extent necessary to comply with the change.

21. Equipment.

Customer is responsible, at Customer's expense, for (i) all computers, telecommunication equipment, software, access to the Internet, and communications networks (if any) required to use the Certificates and related DigiCert software or services; and (ii) Customer's conduct and its website maintenance, operation, development, and content.

22. Certificate Beneficiaries.

Relying Parties and Application Software Vendors are express third-party beneficiaries of Customer's obligations and representations related to the use or issuance of a Certificate. The Relying Parties and Application Software Vendors are not express third party beneficiaries with respect to any DigiCert software.

23. Intermediate Certificates.

This Section 23 only applies if Customer purchases a dedicated Root Certificate and/or Intermediate Certificate for the issuance of Private Certificates or publicly-trusted Certificates as specified in an Order Form.

a. Creation. Within 60 days after receiving applicable payment pursuant to the Agreement and the information required by DigiCert to create the Root Certificate and/or Intermediate Certificate as described in subsection (b) below, DigiCert will create a Root Certificate and/or an Intermediate Certificate for issuing (i) non-publicly trusted Certificates through the Portal or (ii) publicly-trusted Certificates as specified in an Order Form. A "**Private Certificate**" means a Certificate that is not embedded in any trust store. A "**Root Certificate**" means a self-signed Certificate that is stored in a secure off-line state and used to issue other Certificates. "**Intermediate Certificate**" means a Certificate that is signed by a Private Key corresponding to a Root Certificate and that is used to issue Certificates for use by Customer.

b. Contents. DigiCert and Customer will work together in good-faith to determine the appropriate contents of the Root Certificate and/or Intermediate Certificate. Customer must provide DigiCert with all information required by DigiCert for the creation of the Root Certificate and/or Intermediate Certificate within twelve (12) months of concluding an agreement for the creation of that Root Certificate and/or Intermediate Certificate. If Customer fails to provide all required information within that time frame, Customer will forfeit the right to request the Root Certificate and/or Intermediate Certificate and DigiCert will retain any fees paid for the creation of the Root Certificate and/or Intermediate Certificate. After an Intermediate Certificate is created, Customer may not modify the contents of such Intermediate Certificate but may create as many identical copies of the Intermediate Certificate as needed. Intermediate Certificates have a set ten-year lifecycle, after which they expire without renewal. Customer is responsible for ensuring that all Certificates issued from an Intermediate Certificate expire at least two years prior to the expiration of the Intermediate Certificate. DigiCert has the right to revoke any Certificates issued from the Intermediate Certificates that are still valid within two years of the expiration of the Intermediate Certificate.

c. Ownership. DigiCert retains sole ownership of the Intermediate Certificate but, except as otherwise provided herein, will use the Intermediate Certificate issued in connection with this Agreement solely in accordance with the instructions provided by Customer through the Portal. Customer may generate copies of the Intermediate Certificate and distribute copies of the Intermediate Certificate to its own end users and customers.

d. Hosting. DigiCert will host the Intermediate Certificate's Private Key in DigiCert's secure PKI systems. Customer may not remove or have a third party remove the Intermediate Certificate's Private Key from DigiCert's PKI systems for any reason. DigiCert will provide and host CRL/OCSP services for Customer. DigiCert will continue to provide the CRL/OCSP services after the Agreement's termination until all Certificates issued thereunder expire or are revoked. For an Intermediate Certificate that issues publicly-trusted Certificates, because the Intermediate Certificate issues publicly-trusted Certificates, is hosted in DigiCert's PKI, and is managed by DigiCert's personnel, the Intermediate Certificate will be covered by DigiCert's WebTrust audit. If Industry Standards or the policies of an Application Software Vendor change in a manner that requires a separate audit of the Intermediate Certificate, then DigiCert and Customer will work together in good faith to obtain the required audit.

e. Revocation. DigiCert will have the right to revoke the Intermediate Certificate if: (i) Customer requests revocation in writing to DigiCert, citing a specific violation of industry standards; (ii) DigiCert has reasonable grounds to believe the Intermediate Certificate has been compromised; (iii) Customer materially breaches the Agreement and fails to remedy the breach within 30 days after receiving notice of the breach; (iv) Customer continues to use the Intermediate Certificate after Customer's right to use the Intermediate Certificate terminates, or (v) DigiCert reasonably believes the revocation is required by Industry Standards.

f. Restrictions. Customer will not: (i) create or attempt to create additional intermediate certificates from the Intermediate Certificate; (ii) sell, distribute, rent, lease, license, assign, or otherwise transfer the Intermediate Certificate to any third party; (iii) use an Intermediate Certificate provided by DigiCert after its expiration, its revocation, or the termination of this Agreement; (iv) alter, modify or revise an Intermediate Certificate

provided by DigiCert; or (v) use the Intermediate Certificate if Customer has reason to believe that the Intermediate Certificate's Private Key was compromised.

24. Mark License & Third-Party Terms.

a. DigiCert may make certain of its trademarks and logos (each, a "**Mark**") available for display by Customer to allow Customer to indicate that a particular Certificate issued hereunder has been issued by DigiCert for a particular Customer property. Effective upon issuance of the applicable Certificate, and only for so long as such Certificate remains valid, and Customer is in full compliance with all applicable terms related thereto, DigiCert grants to Customer a limited, revocable license during the validity period of the applicable Certificate to display the applicable Mark (in the form provided by DigiCert to Customer) to accurately and not misleadingly indicate the applicable Certificate on Customer's products, domain names or services. Customer agrees to not modify Marks in any manner (including to not remove or modify and trademark notices that DigiCert may apply to such Marks) or use or display Marks for any inappropriate purpose or in any way that could misrepresent the parties' relationship or diminish or damage DigiCert's reputation or the goodwill associated with any Mark or other DigiCert trademarks or service marks, including using a Mark or Certificate with a website that could be considered associated with crime, fraud, deception, defamation, libel, obscenity, misappropriation or infringement or that is otherwise reasonably objectionable to DigiCert. All goodwill arising in connection with the use of Marks will inure to the benefit of DigiCert and if Customer obtains any right, title or interest in or to any Mark as a result of the use of such Mark, then Customer hereby irrevocably assigns to DigiCert all such right, title and interest therein and thereto.

b. Customer acknowledges and agrees that if Customer's Certificate includes a legal entity identifier ("**LEI**") provided by Ubisecure Oy, then the Ubisecure Oy – RapidLEI Terms of Service available at https://rapidlei.com/documents/global-lei-system-terms/ will apply to Customer's LEI and use of the RapidLEI Legal Entity Identifier Management System or successor service.

c. Customer acknowledges and agrees that Customer's use of DigiCert's post-quantum cryptographic (PQC) toolkit (the "**PQC Toolkit**") will be governed by the following terms, in addition to the terms of any other applicable license agreement: (i) the license granted to Customer in relation to the PQC Toolkit is a non-exclusive, terminable license to be used only in connection with a DigiCert certificate that includes a signature and public key generated by or with the PQC Toolkit or related testing and configuration activities; (ii) Customer acquires no intellectual property or other proprietary rights in the PQC Toolkit or intellectual property related to it; (iii) Customer will not reverse engineer, translate, disassemble, decompile, decrypt or deconstruct the PQC Toolkit; (iv) Customer will cease use of the PQC Toolkit upon termination of the related services from DigiCert; (v) ISARA Corporation will not be liable to Customer for any damages whatsoever; (vi) Customer will import, export and re-use the PQC Toolkit only in accordance with applicable laws of the countries or territories in which the PQC Toolkit is used or imported or from which it is exported or re-exported; (vii) DigiCert makes no warranties, express or implied, related to the PQC Toolkit on behalf of ISARA Corporation; and (viii) Customer will not alter any copyright, trademark or patent notice included in or with the PQC Toolkit or any related materials.

25. Flow-Down Requirements. Customer must not monitor, interfere with, reverse engineer the technical implementation of, or otherwise knowingly compromise the security of any DigiCert system or software, and must impose the same restriction on its appointed manufacturers, if any.

26. Adobe-Required Supplemental Obligations

If Customer is issued Adobe Signing Certificates, Customer agrees to:

a. Adhere to the Adobe Systems Inc. AATL Certificate Policy 2.0 currently available at https://helpx.adobe.com/content/dam/help/en/acrobat/kb/approved-trust-list2/_jcr_content/main-pars/download-section/download-1/aatl_technical_requirements_v2.0.pdf which includes, but is not limited to: (1) only generating and storing Key Sets for Adobe Signing Certificates on a FIPS 140-2 Level 2 device; and (2) upon enrollment of a new account, or at any time a new AATL Certificate enrollment is initiated for a subscriber, providing accurate and true information to DigiCert which requires (A) an account administrator to carry out strong identity proofing based on a face to face meeting with DigiCert or on a procedure that provides an equivalent assurance (e.g. by means of a secure video communication), (B) an account administrator to carry out strong identity proofing based on a face to face meeting with its subscribers (i.e. end-users), and store the recording locally to support audits, until DigiCert provides an online mechanism for

administrator to upload attestations and recordings; and (C) the identity proofing process, regardless of an administrator or a subscriber, must include recording of the subscriber showing themselves and a valid government ID (e.g. driving license, passport, national ID card, etc.) displaying a matching photo of the subscriber; and

b. the terms of the applicable CPS.

27. **Additional Restrictions for Code Signing Certificates**. Customer must not use a code signing Certificate: (i) to distribute Suspect Code; or (ii) in a manner that exposes or exports the Private Key related to the Certificate outside of the corresponding hardware security module. .

    For all OV code signing Certificates issued on or after June 1, 2023, including any renewed or reissued Certificates, all Private Keys must be stored on hardware certified as FIPS 140 Level 2, Common Criteria EAL 4+, or equivalent. For all OV code signing Certificates issued before June 1, 2023, including any renewed or reissued Certificates, all Private Keys must be stored on hardware tokens.

28. **Additional Restrictions for non-public TLS/SSL Certificates**. TLS/SSL Certificates that are chained to a Private Root Certificate must be used only with intranet domains and may not be assigned to devices that are publicly accessible from the Internet. DigiCert reserves the right to monitor publicly-facing Internet servers and/or devices to ensure that private TLS/SSL Certificates comply with this clause. If DigiCert discovers any use of private TLS/SSL Certificate(s) not in compliance with this clause, then DigiCert will immediately notify Customer of non-compliance. Customer must, within twenty-four (24) hours, either (i) immediately move the private TLS/SSL Certificate to an intranet domain; or (ii) remove and revoke the private TLS/SSL Certificate from Customer's servers. If the Customer does not revoke or remove the non-compliant Certificate, then DigiCert may revoke the Certificate.

29. **Additional Terms for X9 Certificates**. "**X9 Certificate**" means a Certificate issued by DigiCert or its affiliates within the public key infrastructure governed by the Accredited Standards Committee X9, Inc. When purchasing and using X9 Certificates, Customer will do so in accordance with the DigiCert X9 PKI Certificate Terms of Use ("**X9 Certificates Terms of Use**") available at https://www.digicert.com/legal-repository/, as updated from time to time. If there is a conflict between these Certificate Terms of Use and the X9 Certificate Terms of Use, the X9 Certificate Terms of Use control. Customer will not use X9 Certificates for publicly-trusted TLS/SSL, publicly-trusted S/MIME, or any other purpose outside the X9 trust framework, and DigiCert may revoke any X9 Certificate used outside those constraints.

30. **Electronic Communication/Notification Tools.** When using email or other electronic communication or notification tools ("**Notification Tools**") provided by DigiCert to send a communication or notice ("**Communication**") you agree that (1) the content of any such Communication will be strictly limited to communication or notice about DigiCert products or services; (2) you will follow applicable law (including applicable electronic communications law and data privacy/data protection law) in the jurisdictions of recipients of the Communication; (3) you are solely responsible for the contents of any Communication you send using the Notification Tools; and (4) you will indemnify, defend and hold harmless DigiCert against third-party claims, government regulatory action or fines, and all liabilities, damages and costs, including reasonable attorney fees arising from your use of the Notification Tools or the contents of any Communication you send using the Notification Tools.

31. **Survival and Termination.** The Certificate Terms of Use survive the termination of the Agreement until all Certificates issued expire or are revoked.