Proof SM

ORGANIZATION DIGITAL CERTIFICATE SUPPLEMENT

This Organization Digital Certificate Supplement is attached to and incorporated into the Proof General Terms ("**General Terms**"). Capitalized terms not otherwise defined have the meanings given in the General Terms, the Proof Glossary, or the Order Form.

1. **Applicability**. This Organization Digital Certificate Supplement applies to a User in an entity capacity ("**Organization**"), if Proof provides the Organization with a Digital Certificate. "**Organization**" means the legal entity, including a corporation, limited liability company, partnership, association, trust, governmental body, or other organization, identified in the Application as the subject of, and on whose behalf a User requests, accepts, and uses, an Organization Digital Certificate. References to obligations, representations, acknowledgments, or actions of the Organization in this Organization Digital Certificate Supplement include the authorized representative who accepts this Organization Digital Certificate Supplement and submits the Application on the Organization's behalf.

2. **General**. Proof will use commercially reasonable efforts to verify the information provided by Organization when requesting a Digital Certificate (an "**Application**"). If Proof accepts Organization's Application, Proof will provide the Digital Certificate to Organization subject to the terms, conditions, and restrictions stated in the Agreement. Proof has no obligation to provide the Digital Certificate to Organization. Proof will tell Organization the length of time that the Digital Certificate is valid. At the end of that validity period, Organization must submit a new Application for a Digital Certificate.

3. **Verification**. The Organization authorizes Proof to verify the identity of the Organization, the beneficial owners of the Organization, as well as other agents or representatives of the Organization as Proof may reasonably determine necessary for issuance of the Organization Digital Certificate. Proof may consult public or private databases or other sources for the purpose of verifying submitted information. The Organization represents and warrants that any responses provided to Proof by the Organization as part of the verification shall be complete and accurate when given. The Organization authorizes Proof to collect, store, and use, in accordance with the Organization Digital Certificate Supplement, any information collected or generated during the application, verification, and issuance process.

4. **Issuance**. If verification of the Organization is completed to Proof's satisfaction, Proof will issue and deliver the Organization Digital Certificate to the Organization using any reasonable means of delivery. Proof may change which root or intermediate certificate is used to issue Organization Digital Certificates at any time and without notice to the Organization. The Organization will abide by all applicable laws, regulations and industry standards when applying for and using the Organization Digital Certificate. If Proof is unable to confirm the Organization's identity and authorization, Proof may refuse to approve the Organization's application or refuse to issue an Organization Digital Certificate to the Organization without any liability to any person or entity.

5. **Defective Organization Digital Certificate**. The Organization's sole remedy for a defect in an Organization Digital Certificate ("**Defect**") is to require Proof to use commercially reasonable efforts to cure the defect after receiving notice of such Defect from the Organization. Proof is not obligated to correct a Defect if (i) the Organization misused, damaged, or modified the Organization Digital Certificate, (ii) the Organization did not promptly report the Defect to Proof, or (iii) the Organization has breached any provision of the Agreement.

6. **Obligations and Restrictions on Use**.

6.1 Protection of Private Key. Organization must protect the Private Key included in a Digital Certificate. A "**Private Key**" means part of a key pair, along with the corresponding public key, that is kept secret. Organization must take all reasonable measures to protect Organization's account, Private Key, and any associated activation data or device (such as a password, pass phrase, or token) from unauthorized use and disclosure.

6.2 Organization's Obligations. As a condition of issuance and use of a Digital Certificate, Organization acknowledges and agrees that Organization must:

(a) provide accurate and complete information as part of the Application;

(b) request revocation of the Digital Certificate, if information provided by Organization changes or if Organization discovers or suspects that Organization's Private Key was misused or compromised;

(c) promptly notify Proof if Organization becomes aware of any misuse of an Organization Digital Certificate;

(d) fully cooperate with Proof by providing information, assistance, and cooperation as a result of any compromise of the Digital Certificate or the Private Key;

(e) not use the Digital Certificate for any purpose other than the purpose(s) designated by Proof;

(f) use the Digital Certificate in accordance with all applicable laws and regulations; and

(g) obtain and maintain any authorization or license necessary to order, use, or distribute an Organization Digital Certificate.

7. Representations and Warranties. Organization represents and warrants that Organization: (a) provided true and correct information in the Application and there is no additional information necessary to make the information submitted materially accurate and complete; (b) has the full legal right and authority to obtain an Organization Digital Certificate; (c) has protected and secured the Private Key; (d) has full legal rights to use the Organization Digital Certificate; and (e) the individual accepting the Organization Digital Certificate Supplement is acting as an authorized representative of the Organization. Subject to the provisions of this Organization Digital Certificate Supplement and Organization's fulfilment of its duties and obligations under the same, Proof warrants that the Organization Digital Certificate shall be issued and managed in accordance with the applicable terms of the Proof Certificate Policy available at www.proof.com/legal/certificate-policy, the CPS, and this Organization Digital Certificate Supplement.

8. Revocation.

8.1 Revocation. Proof, in its sole discretion, may revoke a Digital Certificate if Proof discovers or reasonably suspects that the Digital Certificate or any element of the Digital Certificate: (a) has been compromised; (b) is being used in connection with any illegal activities, such as phishing attacks or fraud; (c) is being used in connection with activities that violate industry norms for acceptable network use, such as hate speech, defamation, intellectual property infringement, non-consensual sex acts or child pornography, network abuse, bulk correspondence (spam), etc.; (d) the continued use of the Digital Certificate presents a risk to the security or integrity of the public key infrastructure ("**PKI**") or presents any other risk to its business, its reputation, Relying Parties, or other users; (e) Organization is engaged in conduct that is illegal or would be grounds for revocation of the Digital Certificate under this Organization Digital Certificate Supplement; or (f) other grounds stated in documents maintained by Relying Parties. Revocation of the Digital Certificate may also be backdated to protect Internet users and the PKI. "**Relying Parties**" include any and all entities that rely upon the information contained within the Digital Certificate.

8.2 Other. In addition, a Digital Certificate may be revoked, if Proof ceases doing business or is no longer allowed to issue Digital Certificates and no other certificate provider is willing to provide revocation support.

8.3 Expired and Revoked Organization Digital Certificates. Organization may not use any revoked or expired Digital Certificate. Organization may not use any Private Key associated with Organization's revoked or expired Digital Certificate(s) except to decrypt previously encrypted data associated with Organization's Private Key.

9. Indemnification. Organization will indemnify, defend, and hold Proof, its affiliates and their officers, directors, employees, agents and representatives harmless from and against any and all costs, damages, liabilities or expenses (including reasonable attorneys' fees) arising from any third-party claims resulting from (a) Organization's misrepresentation of, or omission, of any material fact in the Application or otherwise submitted to Proof for purposes of the Digital Certificate, regardless of whether such misrepresentation or omission was

intentional or unintentional; (b) the compromise or unauthorized use or disclosure of a Digital Certificate or a Private Key; and (c) Organization's misuse of a Digital Certificate or Private Key. Organization's obligations under this Section 9 are conditioned on Proof: (x) giving prompt notice of the claim to Organization, (y) granting sole control of the defense or settlement of the claim to Organization, and (z) providing reasonable cooperation to Organization at Organization's request and expense. Proof may participate in the claim's defense at its sole cost and expense. Organization will not enter into any settlement that adversely affects Proof's interests without prior written approval, not to be unreasonably withheld. Organization is not responsible for any settlement it does not approve in writing.

* * * *