PROOF SECURITY STATEMENT

Proof offers a proprietary cloud technology Platform and related Services that allow Users to facilitate and participate in Remote Online Notarizations, eSign Services, Proof Services, and other transactions. Capitalized terms not otherwise defined have the meanings given in Proof General Terms ("**General Terms**") or the Proof Glossary.

1. General Provisions.

This Security Statement ("**Security Statement**") applies to all Users participating in any Transaction or otherwise accessing the Platform in any capacity, other than Subscribers who have signed a separate written agreement with Proof that expressly supersedes this Security Statement.

2. Information Security and Security Incidents.

2.1 Security. Proof has implemented and will maintain appropriate technical, physical and organizational measures in compliance with applicable law intended to protect User Data against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction.

2.2 Payment Card Information. Proof does not collect or process payment card information for payment purposes. Payment card payments are managed by third party service providers that are subject to Payment Card Industry Data Security Standards ("**PCI DSS**").

2.3 Information Security Policies. Proof follows a written information security policy for each of the Services designed to comply with applicable law.

2.4 Organization of Information Security.

(a) *Security Ownership*. Proof has appointed and maintains one or more senior officials responsible for coordinating and monitoring the security rules and procedures.

(b) *Risk Management Program*. Proof performs a risk assessment (1) annually, (2) in conjunction with significant changes to the Services, and (3) before offering new Services or processing new kinds of data.

(c) *Retention*. Proof retains its security-related policies, procedures, and related reviews and assessments documents pursuant to its record retention schedule, subject to applicable record retention laws.

2.5 Asset Management.

(a) *Asset Inventory*. Proof maintains an inventory of all media on which User Data is stored. Access to the inventories of such media is restricted to Proof personnel authorized in writing to have such access.

(b) *Asset Handling*. Proof classifies User Data in accordance with Proof's current policies and procedures and applies appropriate controls to protect it. Proof imposes restrictions on printing User Data and has procedures for disposing of printed materials that contain User Data. Proof avoids storing User Data on portable devices unless it is necessary. When necessary, Proof authorizes such storage and instructs personnel on proper security measures prior to storing User Data on portable devices.

2.6 Human Resources Security; Security Training. Proof takes reasonable steps designed to ensure the compliance of its personnel with security procedures relevant to the Services, including by informing its personnel about relevant security procedures. Proof also informs its personnel of possible consequences of breaching the security rules and procedures. Proof does not use User Data to train its personnel.

2.7 Physical Security, Resiliency, and Data Handling.

(a) *Physical Access to Facilities*. Proof and its third-party service providers limit access to facilities where information systems that process User Data are located to authorized individuals.

(b) *Physical Access to Components*. Proof or its vendors maintain records of the incoming and outgoing media containing User Data, including the kind of media, the authorized sender/recipients, date and time, the number of media, and the types of User Data they contain.

(c) *Resiliency*. Proof uses third-party service providers that offer protections intended to prevent or limit service interruptions.

(d) *Data Deletion*. Proof uses reasonable processes to delete User Data when it is no longer needed pursuant to the terms of the Agreement.

(e) *Data Location*. Proof uses a third-party's cloud service (in its United States-based cloud "region") for processing, storing or accessing User Data. For Subscribers, Proof will notify the Subscriber in advance if it uses a cloud region in a location outside of the United States.

(f) *Protection from Disruptions*. Proof or its vendors use a variety of systems designed to protect against loss of data due to power supply failure or line interference.

(g) *Component Disposal*. Proof or its vendors use processes to delete User Data when it is no longer needed pursuant to the terms of the Agreement.

2.8 Communications and Operations Management.

(a) *Malicious Software*. Proof uses anti-malware controls to avoid malicious software gaining unauthorized access to User Data, including malicious software originating from public networks.

(b) *Event Logging*. Proof logs access and use of information systems containing User Data, registering the access ID, time, authorization granted or denied, and relevant activity.

2.9 Access Control.

(a) *Operational Policy*. Proof maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to User Data.

(b) *Access Policy*. Proof maintains a policy and supporting procedures that identify, by roles, those having access to User Data.

(c) *Access Authorization*. Proof maintains and updates records of roles authorized to access Proof systems that contain User Data, including roles that may grant, alter or cancel authorized access to data and resources.

(d) *Least Privilege*. Proof restricts access to User Data to only those individuals who require such access to perform their role. Proof only permits technical support personnel to have access to User Data if necessary.

(e) *Integrity and Confidentiality*. Proof instructs Proof personnel to disable administrative sessions when they leave their workstations. Proof stores passwords using cryptographic techniques designed to protect them from disclosure.

(f) *Authentication*. Proof uses processes to identify and authenticate users who attempt to access information systems. Where authentication mechanisms are based on passwords, Proof requires that the passwords are composed and maintained based on current best practices. Proof does not reactivate deactivated or expired credentials without proper authorization. Proof monitors and locks accounts (where appropriate) that have repeated failed attempts to gain access to the information system. Proof maintains procedures to deactivate passwords that have been corrupted or inadvertently disclosed.

2.10 Network Design. Proof implements and maintains controls designed to avoid individuals assuming access rights they have not been assigned to gain access to User Data they are not authorized to access.

2.11 Encryption. Proof encrypts, or enables Subscribers to encrypt, User Data that is transmitted over public networks. This feature may not be available to all Users.

2.12 Data Backup Plan. The Services are designed for high availability and to be resilient in the event of failure. On an ongoing basis, but in no case less frequently than once a week (unless no User Data has been updated during that period), Proof maintains multiple copies of User Data from which User Data can be recovered. Proof has specific procedures in place governing access to backups of User Data. Proof logs data restoration efforts, including the person responsible, the description of the restored User Data and where applicable, the person responsible and which User Data (if any) had to be input manually in the data recovery process. Proof's redundant storage and its procedures for recovering data are designed to reconstruct User Data in its original or last-replicated state from before the time it was lost or destroyed.

2.13 Security Incidents.

(a) *Incident Response Plan*. Proof maintains a cyber-incident breach response plan in accordance with Proof's information security policy ("**Incident Response Plan**") and implements the procedures required under such plan on the occurrence of a Security Incident.

(b) *Security Incident Notification*. If Proof becomes aware of a Security Incident, Proof, after initial investigation, without unreasonable delay: (1) notifies Subscriber of the Security Incident; (2) investigates the Security Incident and, after completing its investigation, provide Subscriber with information about the Security Incident; (3) uses reasonable efforts to mitigate the effects and to minimize any damage resulting from the Security Incident and, after doing so, informs Subscriber of the steps taken; and (4) once determined, informs Subscriber of any modifications Proof makes to its security procedures that are intended to prevent similar security incidents occurring in the future.

(c) *Information Security Incident Management*.

(i) *Incident Response Process*. Proof maintains a record of Security Incidents with a description of the Security Incident, the time period, the consequences of the incident, the name of the reporting person, to whom the Security Incident was reported, and the procedure for recovering any affected data. Proof shall track, Security Incidents, including what data has been disclosed and to whom, or what data has been lost, damaged, destroyed or altered (as the case may be), and at what time.

(ii) *Service Monitoring*. Following a Security Incident, Proof security personnel review relevant service-related logs to propose remediation efforts, if necessary.

* * * * *