PROS Cloud Security Exhibit

Information Security Program

PROS maintains administrative, technical, and physical controls as part of a documented and certified information security program under ISO 27001 and SOC2 Type 2 or similar established industry standard. PROS regularly reviews controls to assess compliance with applicable law and sufficiency in light of the (a) size and nature of PROS business; (b) resources available to PROS; (c) nature of the information that PROS stores; and (d) need for security, confidentiality and privacy for such information.

PROS information security program is governed by PROS Security Council under the leadership of the Information Security Department, which is responsible for overseeing and enforcing security training; physical and environmental security controls; systems access controls; security incident procedures; contingency planning and business continuity; audit controls; data integrity protections; systems testing and monitoring; and procedures for secure data destruction. PROS information security program includes:

Security Training and Software Coding Standards

PROS employees and contractors participate in annual security awareness training and agree to comply with published security policies. PROS regularly conducts mandatory secure development training for all developers. In addition, PROS has adopted secure coding standards, developed in accordance with the OWASP Top 10 and SANS guidelines, which define the security principles, standards, guidelines, and best practices for secure code development.

Physical and Environmental Security Controls

PROS limits access to PROS facilities to authorized and badged individuals. PROS policies require that visitors are registered, recorded, and accompanied at all times. Access to PROS datacenters is further restricted to individuals with a legitimate business need and appropriate approval(s). PROS requires that all access rights be assigned based on the “least privilege” principle and removed when no longer necessary. PROS physical security controls include, but are not limited to logging and monitoring unauthorized access attempts to datacenters; and video surveillance systems at critical datacenter entry points.

PROS maintains environmental controls established to detect and prevent destruction of its datacenters, including, but not limited to:

- Fire suppression systems;

- Air temperature and humidity monitoring and control systems for computing equipment; and
- Uninterruptible power supply modules and backup generators.

Systems Access Controls

PROS limits access to PROS information systems to named and authorized individuals with a legitimate business need and appropriate approval(s). PROS requires a two factor (also known as, two step) authentication safeguard for all privileged administration of customer systems. PROS default configuration limits individual customer access to specific customer approved network IP addresses and PROS recommends to its customers that they use the same default limitations.

Security Incident Procedures

PROS security incident response plan includes procedures to be followed in the event of a security breach of applications or systems that access, process, store, communicate, or transmit customer data. PROS incident response plan includes the following procedures:

- Respond. Assemble internal incident response team;
- Validate. Qualify existence of security event;
- Scope. Assess impact;
- Contain. Limit impact and potential damage and preserve evidence;
- Report. Determine if regulatory or contractual reporting requirements exist based on the nature of the incident and perform appropriate notifications;
- Recover. Restore normal service and analyze incident for potential legal action; and
- Improve. Perform root cause analysis, determine lessons learned and implement strategic remediation.

PROS provides appropriate communications to affected customers in the event of a security incident compromising such customer's data.

Contingency Planning and Business Continuity

PROS maintains policies and procedures for responding to emergency situations (e.g., fire, vandalism, system failure, and natural disaster) that could damage or otherwise compromise customer data. Such procedures include, but are not limited to:

- Periodically backing up production file systems and databases;
- Employing a formal business continuity and disaster recovery plan, including:
- Periodic disaster recovery testing for SaaS services;

- Contingency plans for each key business function, including customer support, operations, and administrative functions, to continue critical business and service activities through certain emergency situations; and
- Crisis communication plans to provide appropriate communications to affected parties.
- Maintaining a formal process to evaluate PROS contingency planning and business continuity policies.

Audit Controls

PROS maintains hardware, software, and procedural mechanisms to record and examine activity in information systems that contain or use electronic information, including appropriate logs and reports concerning these security requirements.

Data Integrity

PROS maintains policies and procedures to ensure the confidentiality, integrity, and availability of customer data. Specifically, customer data in the PROS cloud is firewalled on a secured network; safeguarded by industry standard SSL/TLS encryption in transit; and fortified using industry standard network intrusion detection and/or network intrusion prevention systems.

PROS utilizes malware detection systems, which include mathematical threat prediction models intended to help prevent the execution of predicted, novel, or targeted malicious threats. PROS runs static attribute detection analysis on individual computers.

Testing and Monitoring

PROS regularly tests key controls, systems, and procedures of its information security program to validate that they are properly implemented and effective in addressing the threats and risks identified. Internal audits are conducted on an ongoing basis and independent third party audits are conducted annually and more frequently as needed, based on the results of periodic risk assessments and continuous monitoring of the threat landscape.

PROS monitors its systems, logs, and events, including by:

-Reviewing changes affecting systems handling authentication, authorization, and auditing; -Reviewing privileged access to PROS production systems; and -Engaging third parties to perform network vulnerability assessments and penetration testing on a regular basis.

Secure Destruction

Other than in exceptional circumstances, PROS purges all customer data upon verification that the relevant contract has been validly terminated and the relevant customer data is no longer required. PROS standards for secure destruction of data are based upon guidance from NIST Special

Publication 800-88, Revision 1 (2014): Guidelines for Media Sanitization or similar industry standards established in the future.

Shared Responsibility

Customer trust and confidence are critical to PROS and its customers' continued success. Both providers and consumers of SaaS services must understand that security is a shared responsibility. As a SaaS provider, PROS is responsible for secure delivery of PROS SaaS services, which include the underlying infrastructure required to deliver such services. As a SaaS consumer, customer is responsible for data provided to PROS and non-PROS services that are integrated with PROS services.