INFORMATION SECURITY EXHIBIT

PROS maintains a comprehensive, written information security program that contains administrative, technical, and physical safeguards designed to ensure that Customer data remains secure and is handled in compliance with all regulatory requirements applicable to PROS and the Subscription Services. This Information Security Exhibit (this "***Exhibit***") applies to the Subscription Services and all associated PROS processes and systems used to develop, operate and support those Subscription Services.

1. Corporate

A. Information Security Management System

PROS will maintain an Information Security Management System (or "***PROS ISMS***") that defines PROS policies, standards, guidelines, and procedures as part of PROS documented information security program covering the management of information security for the Subscription Services and all related PROS internal operations. PROS ISMS is designed to:

- Establish directives and principles for action regarding information security;
- Document and maintain compliance with statutory, regulatory, and contractual requirements, including SOC1, SOC2, SOX, GDPR, CCPA, CSA STAR, ISO 27001, and ISO 27018; and
- Monitor, evaluate and adjust, as appropriate, considering relevant changes in technology, threats to PROS or to Customer data and security and privacy regulations applicable to PROS.

This Exhibit describes the current policies, standards, guidelines, and procedures under PROS ISMS. PROS may update or enhance the ISMS and this Exhibit in its discretion to reflect ongoing changes in law, regulation, or industry best practice but PROS will not materially diminish the level of security described herein.

Organization. PROS ISMS will maintain a cross-functional Security Council responsible for managing information security risk at PROS and prioritizing security considerations across the organization, including oversight of PROS ISMS.

Risk Management. PROS ISMS will include a risk management program under which PROS will conduct regular risk assessments at the enterprise, Customer and change level intended to anticipate threats to the security of Customer data using qualitative and quantitative measures.

Change Management. PROS ISMS will include a change management program to govern all changes to PROS production Subscription Service systems, applications, and databases, including (i) documentation, testing, and approval of all changes; (ii) security assessments of all changes prior to deployment into production; and (iii) security patching in a timely manner based on risk analysis. In addition, PROS will require all changes to Customer production environments to be documented on an approved change request prior to deployment.

Testing. At least annually, PROS will review and test key controls, systems, and procedures of PROS ISMS to validate that they are properly implemented and effective in addressing identified threats and risks.

Asset Management. PROS ISMS will include an asset management program for all PROS assets. Each asset will first be identified, tagged, and registered by PROS in an asset inventory before it can be used for any business activity related to the Subscription Service. PROS will then classify and label each asset based on relevant criteria, including sensitivity and criticality to the organization.

Business Continuity & Disaster Recovery. PROS ISMS will include a business continuity framework designed to mitigate the risk of single points of failure and provide a resilient environment to support Subscription Service continuity and performance. PROS will administer comprehensive plans for crisis management and communication, supply chain management and individualized department action strategies designed to prevent interruption of critical business functions. PROS will also administer formal disaster recovery plans designed to minimize disruption to critical business operations and Customer systems. PROS will maintain production and disaster recovery environments to support failover procedures and redundancy requirements, as well as proactive protection and detection methods designed to limit damage from disaster events.

Incident Response. PROS ISMS will include a security incident response plan to be followed in the event of any unauthorized exposure, corruption, or loss of Customer data (each a "***Security Incident***"). Such Security Incident response plan will, at a minimum, define personnel roles and responsibilities, as well as procedures related to Security Incident identification, containment, investigation, communication, forensic analysis, recovery and remediation, documentation, and reporting. If PROS verifies that any Customer data is impacted by a confirmed Security Incident, PROS will notify the affected Customer without undue delay to the extent permitted by law.

B. Certifications & Audits

The PROS ISMS policies, procedures and logical controls will be designed to utilize ITIL and COBIT principles, aligned to the ISO 27001 framework, and PROS will maintain an internal audit program and require annual independent third-party assessments for certification purposes. An independent third party will audit the Subscription Services annually for compliance with the following standards (or their successor equivalents):

- SOC 1 Type II;
- SOC 2 Type II;
- ISO 27001;
- ISO 27018; and
- Cloud Security Alliance STAR standard.

In addition, an independent third party will audit any PROS Subscription Service that includes payment processing annually for compliance with PCI DSS. PROS will provide Customer, upon request, with a summary of the then-current audit report or certificate, as applicable.

PROS will also conduct internal audits designed to monitor PROS ISMS compliance on an ongoing basis. PROS will review and modify internal audit controls based on a risk-based approach that takes into account changes in regulations, certification standards, internal audit findings and observations and industry best practices.

C. Personnel

Screening. PROS ISMS will include a pre-screening program for all personnel (employees and contractors that will have access to PROS systems or Customer data), under which PROS will conduct formal background investigations prior to employment or engagement in compliance with applicable local regulations.

Confidentiality & Ethics. PROS will require all PROS employees to (i) sign a confidentiality agreement as a condition of employment, and (ii) annually confirm compliance with all relevant laws, regulations, corporate policies, and industry best practices for ethical corporate interactions by signing the PROS Code of Business Conduct and Ethics. PROS ISMS requires contractors with access to PROS systems or Customer data to be subject to the same confidentiality and ethical obligations as those required of PROS employees.

Training. PROS ISMS will include an annual mandatory security awareness and training program for all PROS personnel designed to promote a culture of security awareness. PROS will provide additional role-based security training to PROS personnel as appropriate. PROS will also train employees who have access to sensitive data in relevant laws and regulations, including GDPR, CCPA and HIPAA. PROS ISMS requires contractors with access to PROS systems or Customer data to complete the same security awareness training and commitment to PROS information security policies as those required for PROS employees.

2. System Controls

A. Access. PROS ISMS will include policies, procedures and logical controls designed to restrict access to PROS networks, PROS systems and all elements of the Subscription Service (including Customer data) on a need-to-know basis and based on the principle of "least privilege." PROS will (i) electronically monitor and manage active access privileges; (ii) verify business justification for access requests; (iii) limit duration of access; and (iv) promptly remove access in the event of a change in job responsibilities, job status or otherwise when access is no longer needed. PROS will secure access points via the use of unique identifiers, password complexity, regularly scheduled password updates and, where PROS deems appropriate, multi-factor authentication (MFA).

B. Intrusion Detection and Prevention. PROS ISMS will include policies, procedures and logical controls designed to limit unauthorized access to and within the PROS network via application layer firewalls and network intrusion prevention. PROS will maintain intrusion-detection or intrusion-prevention systems (IDS/IPS) to monitor network traffic and system operations including:

- PROS environments that host systems processing, transmitting, or storing Customer data;
- Internet facing network segments; and
- Network entry and exit points for third party connections.

PROS will configure and maintain all IDS/IPS devices in accordance with PROS ISMS standards consistent with industry best practices and security vendor recommendations.

C. Malware. PROS ISMS will include layered protection designed to prevent malware across PROS systems, including those supporting Customer environments. PROS will use a combination of client-based threat prevention and trust enforcement (such as trusted change modelling and predictive threat prevention) and network-based threat identification and threat interruption (such as network-embedded antivirus protection and dynamic threat detonation).

D. Monitoring. PROS ISMS will include a comprehensive program of network-wide scanning and monitoring, including the Subscription Service, through a vulnerability assessment tool. PROS will promptly investigate and respond to any reported anomalies. Network monitoring will also extend to performance monitoring and tuning, capacity planning and resource allocation designed to continuously adjust to meet changing regulatory, contractual, and business requirements

E. Logging. PROS ISMS will include a network logging program designed to enable security review and analysis under which all PROS systems (including firewalls, routers, network switches, operating systems, and applications) log information to both their respective system log facility and a centralized log server. PROS will configure monitors of critical systems to alert system administrators to events that could indicate a Security Incident or a failure of security systems to operate as designed. PROS will also regularly review log files for trend analysis and pattern identification.

F. System Hardening. PROS ISMS will include a program for hardening operating systems designed to timely disable unnecessary ports, protocols, and services and to apply security measures to meet baseline security configuration requirements for all infrastructure components, including network and server elements. PROS will evaluate new Subscription Service implementations for compliance with PROS ISMS baseline security configuration requirements, document any deviation(s) from such baseline security configurations requirements and secure appropriate approval before the affected system is deployed into production.

G. Penetration Testing. PROS will engage an independent third-party to conduct penetration testing of PROS systems and products at least annually. PROS will provide the applicable pen testing letter of attestation to Customer upon request.

H. Vulnerability Assessment & Remediation. PROS will retain an independent third party to conduct both internal and external vulnerability scans on a periodic basis. PROS will track all identified vulnerabilities, and then prioritize and address identified vulnerabilities using a risk-based model.

3. Physical Controls

A. Access. PROS ISMS will include policies, procedures and logical controls designed to limit access to PROS facilities (including production data centers) to properly authorized individuals, including through (i) badging, logging and 24/7 monitoring of access to secure areas of the data center; (ii) camera surveillance systems at all entrance points; and (iii) separating data center ingress and egress points from data storage and processing facilities by multiple barriers.

B. Environmental Security. PROS ISMS will include environmental controls to detect and help prevent compromise or destruction of data centers, including (i) fire, heat, and smoke detection; (ii) Uninterruptible Power Supply (UPS) modules and backup generators; and (iii) air temperature and humidity monitoring and control.

4. Data Controls

A. Access. PROS ISMS will include policies, procedures and logical controls designed to: (i) limit access to Customer data to authorized persons, (ii) help protect against Customer data being moved, modified or compromised, and (iii) handle Customer data with the highest level of security and confidentiality.

B. Encryption. PROS ISMS will include policies, procedures and logical controls designed to enforce encryption on all externally accessible systems and communications. PROS will: (i) administer encryption protocols designed to isolate network communication between application host and database host; (ii) provide access to the internet-facing PROS web port (for HTTPS) through network firewalls, (iii) secure volume-based encryption of data-at-rest using keys stored separately from the data; and (iv) secure all end points using encryption, password protection and remote deactivation capability.

C. Segregation. The Subscription Services will operate in a multitenant architecture designed to segregate and restrict Customer Data access based on business needs. PROS ISMS will include policies, procedures and logical controls designed to: (i) logically separate each Customer's data (i.e. separate database schemas) on the Subscription Service from all other Customers' data; (ii) prevent the replication of production data for use in non-production environments without the express permission of the data owner; and (iii) identify, secure, and manage test environments that contain production data with the same level of security as production environments.

D. Transmission. PROS ISMS will include policies, procedures and logical controls designed to prohibit unencrypted connections in to or out of the Subscription Service. PROS will encrypt Subscription Service data transmissions via an AES (or its direct successor standard) by default, and protect Data in motion using TLS1.2 (HTTPS or SFTP) (or its direct successor standard).

E. Geolocation. PROS will utilize data centers in the US, Europe, and Australia. PROS will comply with applicable laws governing cross-border transfers and will put in place cross-border transfer agreements to the extent necessary.

F. Backups. PROS ISMS will include policies, procedures and logical controls designed to (i) back up Customer systems and data on a daily basis to geographically separated, encrypted servers; and (ii) prohibit storage or archival of data on backup tapes or mobile devices.

G. Minimization. PROS ISMS will include policies, procedures and logical controls designed to ensure Customer data is processed only as instructed by Customer.

H. Destruction. PROS ISMS will include standards for secure destruction of data consistent with current industry-standard guidance outlined in NIST Special Publication 800-88, Revision 1 (2014): Guidelines for Media Sanitization (or its direct successor standard). PROS will purge Customer data in compliance with applicable law and the applicable Customer contract.

5. Other Best Practices

A. Coding Standards. PROS ISMS will include policies, procedures and logical controls designed to ensure developers meet industry best standards of quality and use industry best security practices for Systems/Software Development Lifecycle, including a focus on OWASP top 10 vulnerabilities.

B. Supply Chain Management. PROS ISMS will include policies, procedures and logical controls designed to ensure each third-party supplier that (i) acts as a data subprocessor, (ii) stores or processes data that is critical to PROS operations, or (iii) provides contracted staffing for roles with access to PROS systems or Customer data, complies with security standards similar to or more stringent than those set by PROS ISMS.

Last Updated: March 28, 2024