SOC 2 Readiness

SOC 2 is an auditing procedure that ensures your service providers securely manage your data to protect the interests of your organizations and the privacy of its clients.

Address: 7311 W 132nd Street, Suite 305
Overland Park, KS 66213

1 Hartfield Blvd, Suite 300
East Windsor, CT 06088

A8 Ively Road, Farnborough
Hampshire, GU14 0LX UK

Phone: +1 800-940-4699
+44 800-358-4915

E-mail: info@foresite.com

Website: www.foresite.com

FIVE TRUST PRINCIPALS OF SOC 2

Security

Refers to protection of system resources against unauthorized access. Access controls help prevent potential system abuse, theft or unauthorized removal of data, misuse of software, and improper alteration or disclosure of information. IT security tools such as network and Web Application Firewalls (WAFs), two factor authentication and intrusion detection are useful in preventing security breaches that can lead to unauthorized access of systems and data.

Availability

Refers to the accessibility of the system, products or services as stipulated by a contract or Service Level Agreement (SLA). As such, the minimum acceptable performance level for system availability is set by both parties. This principle does not address system functionality and usability, but does involve security-related criteria that may affect availability. Monitoring network performance and availability, site failover and security incident handling are critical in this context.

Processing Integrity

The processing integrity principle addresses whether or not a system achieves its purpose (i.e., delivers the right data at the right price at the right time). Accordingly, data processing must be complete, valid, accurate, timely and authorized. However, processing integrity does not necessarily imply data integrity. If data contains errors prior to being input into the system, detecting them is not usually the responsibility of the processing entity. Monitoring of data processing, coupled with quality assurance procedures, can help ensure processing integrity.

Confidentiality

Data is considered confidential if its access and disclosure is restricted to a specified set of persons or organizations. Examples may include data intended only for company personnel, as well as business plans, intellectual property, internal price lists and other types of sensitive financial information. Encryption is an important control for protecting confidentiality during transmission. Network and application firewalls, together with rigorous access controls, can be used to safeguard information being processed or stored on computer systems.

Privacy

This principle addresses the system's collection, use, retention, disclosure and disposal of personal information in conformity with an organization's privacy notice, as well as with criteria set forth in the AICPA's Generally Accepted Privacy Principles (GAPP). Personal Identifiable Information (PII) refers to details that can distinguish an individual (e.g., name, address, Social Security number). Some personal data related to health, race, sexuality and religion is also considered sensitive and generally requires an extra level of protection. Controls must be put in place to protect all PII from unauthorized access.