InnovaSafe is now SOC2 Type II Compliant - Security Principal

What does that mean?

To achieve compliance, the following areas of InnovaSafe's policies and practices were reviewed:

- **Infrastructure**: The physical and hardware components of its system.
- **Software**: The programs and operating software of its systems.
- **People**: The personnel involved in the operation and use of its systems.
- **Procedures**: The automated and manual procedures involved in the operation of its systems.
- **Data**: The information used and supported by its systems.

What is it?

The Service Organization Control (SOC)2 Type II audit demonstrates that an independent accounting and auditing firm has reviewed and examined an organization's control objectives and activities, and tested those controls to ensure that they are operating effectively. SOC2 is based on Policies, Communications, Procedures and Monitoring. The specific Trust Service Principle explained below must be met in order to successfully achieve compliance.

- **Security:** InnovaSafe's system has controls in place to protect against unauthorized access (both physical and logical).

The security principal requires service organizations to have in place highly formalized and documented policies, procedures, and processes. More specifically, it means having documentation stating the policies, and then actually having personnel undertaking the stated procedures. Ultimately, this mandates that service organizations put in place a large number of information security and operational policies, procedures, and other supporting documentation. There are two types of SOC 2 reports: Type I and Type II.

The Type II report is issued to organizations that have audited controls in place and the effectiveness of the controls have been audited over a specified period of time. The Type I report is preliminary to the Type II report and is based on the ability to test and

report on design. Type I reports are issued to organizations that have audited controls in place, but have not yet audited the effectiveness of the controls over a period of time.

Why is it important and why does it matter?

Type II Certification consists of a thorough examination by a third party firm of an organization's internal control policies and practices over a specified period of time. The period of time is typically six (6) months to one year. This independent review ensures that the organization meets the stringent requirements set forth by the AICPA and CICA. When trusting InnovaSafe with highly sensitive and confidential information, such as intellectual property, source code, client data and documents obtaining a SOC2 Type II compliance certification is crucial.

How does it impact systems?

Systems developed by a SOC 2 certified organization must be developed and implemented following audited processes and controls. This helps ensure that systems, applications and code are developed, reviewed, tested, and released following the the AICPA Trust Services Principles. The result is a service and application that have been developed under audited processes and controls to help ensure the highest level of trust and security.

How does it impact our Clients?

By working with a SOC 2 certified vendor like InnovaSafe, our clients can rest assured knowing that their data is kept secure through the implementation of standardized controls as defined in the AICPA Trust Service Principles framework (as mentioned above).

InnovaSafe provides technology escrow solutions and acts as a trusted neutral/independent third party. InnovaSafe receives and stores all types of intellectual property for various requirements. Because InnovaSafe is a SOC 2 certified organization, with audited controls and processes in place, our clients can be sure that our services and application perform and operate as described.

Services and applications developed and provided by organizations that are not SOC 2 Type II certified do not have the same level of assurance.

For more information please email us at requestinfo@innovasafe.com