SecureTrust
a Trustwave division

Service Description

Data Privacy Consulting

Contents

Data Privacy Consulting

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Data Privacy Consulting (the "Service") is designed to assist and guide organizations in review and examination of compliance solutions, policy, procedures, processes, technology and documentation for compliance, data protection, and privacy management programs.

Capitalized terms used in this service description but not defined herein have the meaning given to them in the Trustwave Master Services Agreement found at https://www.trustwave.com/en-us/legal-documents/contract-documents/ or a similar agreement signed between SecureTrust and Client.

BASE SERVICE FEATURES

The Service includes the following standard features:

SecureTrust Portal

The SecureTrust Portal features consist of, among others, a Compliance Manager application to manage the engagement process as well as collect and securely store evidence, documentation, and final deliverables.

Global Compliance & Risk Services

The Global Compliance and Risk Services (GCRS) team consists of, among others, the following key personnel and functions:

Security Consultant – A Security Consultant is the primary resource for the fulfilment of the Service, responsible for scheduling and conducting consulting activities.

Managing Consultant (MC) – An MC provides guidance, project oversight, and report quality assurance to the Security Consultant and serves as Client's secondary point of contact for escalations and queries.

Data Privacy Consulting – A SecureTrust Security Consultant assists and guides Client in review and examination of compliance solutions, policy, processes and documentation. The Security Consultant provides Client with guidance and recommendations for compliance solutions, policies, procedures and technologies to support Client efforts and business priorities.

DELIVERY AND IMPLEMENTATION

Project Initiation

The SecureTrust GCRS team facilitates delivery of the Service, which includes scheduling and conducting the remote kickoff meeting. The kickoff meeting will be used to define and agree to a high-level project plan consisting of milestone dates, key steps, estimates for duration, deliverables, resource requirements and escalation procedures.

Data Privacy Consulting Engagement

SecureTrust's Security Consultant and Client will review and examine Client's compliance, data protection and privacy management programs. Activities may include, but are not limited to the following:

- Help Client understand compliance and data protection requirements;
  Prepare and coach Client;
- Review and provide guidance for the design and implementation of compliance and data protection controls;
- Advise Client of identified compliance or data protection gaps;
- Identify and prioritize remediation actions to achieve and maintain compliance and security; and
- Provide recommendations for remediation of compliance and data protection issues.

SecureTrust will conduct a closeout meeting with Client, if desired.

SECURETRUST RESPONSIBILITIES

- Establish contact and remain available for communications from Client.
- Establish communication and escalation plans.
- Create a Client account in the SecureTrust Portal.
- Define high-level project plan consisting of milestone dates, key steps, estimates for duration and resource requirements.
- Schedule and conduct kickoff and consulting meetings.

CLIENT RESPONSIBILITIES & ACKNOWLEDGEMENTS

- Establish contact and remain available for communications from SecureTrust.
- Establish communication and escalation plans.
- Agree to high-level project plan consisting of key steps, estimates for duration, deliverables and resource requirements.
- Accurately provide all necessary information including key stakeholders, applicable Client environment information and configuration requirements.
- Inform SecureTrust of all Client environment maintenance activity and changes that may impact delivery of the Service.
- Accurately respond to requests from SecureTrust teams when establishing contact and collecting information.
- Provide complete and accurate details of the relevant environment and other business operations information.
- Make available resources capable of participating in Service activities.
- Participate in and understand materials explained during calls, meetings, interviews, discussions, facilities inspection and controls analysis.
- Client acknowledges:
    - All security and feature updates for SecureTrust Portal software will be included in major version release upgrades.
    - Personnel from the following departments are generally involved:
        - Operations, Security Governance, Information Technology, Enterprise Risk Management, Legal and Compliance, Procurement, Internal Audit, Human Resources, Facilities, Complaints, and Finance.
        - Third party Data Controllers or Processors are involved.
    - The Service consists of remote consulting.

- SecureTrust may request evidence from Client's systems and processes as required to prove compliance with specific requirements. Client agrees to provide all such evidence in a timely manner.
- The Service project start and end dates will be determined during the kickoff call.
- SecureTrust is not responsible for defining systems in scope or whether information provided by Client is accurate.
- SecureTrust retains the right to reject or accept Client comments based on the facts and circumstances of the service.
- SecureTrust will not provide remediation services as a part of the Service.
- SecureTrust will not offer any legal guidance or counseling. The provision of the Service does not guarantee compliance with data privacy regulatory requirements. Client is responsible for making all management decisions with regard to its data privacy policies.
- The quality and accuracy of the Service is dependent on Client's provision of accurate information and access to Client systems and resources to SecureTrust.