SecureTrust
a Trustwave division

Service Description

Data Privacy Policy Service

Contents

Data Privacy Policy Service

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Data Privacy Policy Service ("Service") is designed to assist and guide the Client in the development of policies to adhere with privacy regulatory requirements or data privacy management programs specified in the applicable Order Form or SOW ("Privacy Requirements").

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 and Risk Services (GCRS)

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 Policy Template – A template of baseline policies to assist Client in its development of an internal policy to address relevant Privacy Requirements.

Data Privacy Policy Consulting – A Security Consultant assists and guides Client in review and examination of Privacy Requirements . SecureTrust will provide Client with consulting to assist and guide Client in the customization of an internal policy using the SecureTrust Data Privacy Policy Template.

DELIVERY AND IMPLEMENTATION

Project Initiation

The SecureTrust GCRS team facilitates delivery of the Service which includes scheduling and conducting the remote kickoff meeting 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.

Phase I: Information Gathering

SecureTrust's Security Consultant will gather information in order to gain an understanding of Client's operating environment, business processes, and data privacy management program. This information will be gathered during collaborative remote sessions, and the template will serve as the framework of the policy documents.

Phase II: Draft Creation

SecureTrust will work with Client to customize a set of policies to address Privacy Requirements. Policy documentation will be modified in conjunction with Client to reflect the specific data privacy management program.

Phase III: Draft Review and Modification

SecureTrust and Client will review draft documentation to address Requirements. Any necessary modifications will be made to the draft policy documentation at this time.

Phase IV: Draft Finalization and Implementation

SecureTrust will provide Client with the final policy documentation in an editable format as a deliverable to be adopted, implemented, and maintained by Client.

SecureTrust will conduct a closeout meeting with Client.

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, deliverables and resource requirements.
- Schedule and conduct kickoff, periodic status and closeout 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 milestone dates, key steps, estimates for duration, deliverables and resource requirements.
- Accurately provide all necessary information including key stakeholders, applicable environment information and configuration requirements.

- Inform SecureTrust of all environment maintenance activity and changes that may impact 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 the 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.
        - Privacy Officer and Data Protection Officer
    - The Service consists of remote consulting activities.
    - The project start and end dates will be determined during the kickoff call.
    - SecureTrust may request information about Client's systems and processes as required to describe the Client data privacy management programs. Client agrees to provide all such information in a timely manner.
    - 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 Data Privacy Policy Service.
    - If a multi-year term is selected, the Service includes updating the existing policies to include new policies or changes as required by Privacy Requirements.
    - Subsequent years will utilize the same methodology and Client shall identify any changes within the environment. These changes may require the adjustment of existing policies, which may include technological changes such as newly deployed systems or devices, system configuration changes, as well as adjustments to roles, responsibilities and internal processes or updated Privacy Requirements.
    - SecureTrust will not offer any legal guidance or counseling. The provision of the Service does not guarantee compliance with Privacy 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.