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 is a professional services engagement. SecureTrust's Data Privacy Policy Service is designed to assist and guide organizations in development of policies to adhere with privacy regulations or data privacy management programs.

BASE SERVICE FEATURES

SecureTrust's Data Privacy Policy Service includes the following standard features:

SecureTrust© Portal

The SecureTrust Portal consists of, among other features, a Compliance Manager application which manage the engagement process and collects and securely stores 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 – An information security consultant is the primary resource for the fulfilment of the Data Privacy Policy Service.

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

Data Privacy Policy Template – A template of baseline policies to assist Client in its development of a data privacy policy to address relevant requirements.

Data Privacy Policy Consulting – Consulting assistance and guidance for modification of the Data Privacy Policy Template. SecureTrust will provide consulting services to assist and guide Client in the customization of policy using the SecureTrust Data Privacy Policy Template.

DELIVERY AND IMPLEMENTATION

Project Initiation

The SecureTrust GCRS team is assigned to facilitate delivery of the Data Privacy Policy 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.

Project Initiation phase activities include:

- Introduction to the Compliance Manager application for data sharing.

Outputs of Project Initiation phase includes:

- Agreement on the high-level project plan.
- Regular project status meetings with key stakeholders.

Phase I: Data 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 relevant to privacy regulations or data privacy management programs. Documentation will be modified in conjunction with Client to reflect the specific data privacy management program.

Phase III: Review and Modification

SecureTrust will review draft documentation with Client staff to address privacy regulations or data privacy management programs. Any necessary modifications will be made to the draft at this time.

Phase IV: Delivery of Documentation for Client Adoption

SecureTrust will provide 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 and maintain contact with 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

- Establish and maintain contact with 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 activity and changes that may impact the Data Privacy Policy 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 consulting 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 brokers, controllers or processors.
        - Privacy Officer and Data Protection Officer
    - The engagement 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 engagement.
    - SecureTrust will perform the service in the English language.
    - SecureTrust will not provide remediation services as a part of the Data Privacy Policy Service.
    - If the multi-year service is selected, the service includes updating the existing policies to include new policies or changes as required by privacy regulation or data privacy management programs.
    - 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 regulation requirements.
    - SecureTrust will not offer any legal guidance or counseling. The provision of the Data Privacy Policy Service does not guarantee compliance with data privacy regulation. 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.