SecureTrust
a Trustwave division

Service Description

Payment Card Industry Data Security Standard

Policy Service

Contents

PCI DSS Policy Service

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Payment Card Industry Data Security Standard (PCI DSS) Policy Service (the "Service") is designed to assist and guide organizations in development of an internal policy in compliance with the PCI DSS as set out by the PCI Security Standards Council (the "Standard").

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:

Qualified Security Assessor (QSA) – A QSA 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.

PCI DSS Policy Template – A template of baseline, PCI DSS policies to assist Client in its development of information security policy to address relevant requirements of the PCI DSS.

PCI DSS Policy Service – Consulting assistance and guidance for modification of the PCI DSS policy template. SecureTrust will provide Client with consulting services to assist Client in the development of an internal policy using the SecureTrust PCI DSS 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. This information will be gathered during calls, and the SecureTrust PCI DSS policy template will serve as the framework of the policy documents. Client staff will provide SecureTrust with the current set of internal procedural steps.

Phase II: Draft Creation

SecureTrust and Client will work together to create a comprehensive set of policies . Documentation will be created in conjunction with Client to reflect the specific environment and procedures of Client's operating environment.

Phase III: Review and Modification

SecureTrust will review draft documentation with Client staff to help ensure security and compliance objectives are addressed. Any necessary additions or modifications will be made to the draft at this time.

Phase IV: Finalization and Implementation

SecureTrust will provide Client 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 communication 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, periodic status and closeout meetings.

CLIENT RESPONSIBILITIES & ACKNOWLEDGEMENTS

- Establish contact and remain available for communication 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 client environment information and configuration requirements.
- Inform SecureTrust of all Client 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.
    - The Service consists of remote consulting activities.
    - The 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 perform the Service in the English language.
    - If the multi-year Service is selected, the Service includes updating the existing policies to include new policies or changes as required by security standards.
    - 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 and procedures, which may include technological changes such as newly deployed systems or devices, system configuration changes, firewall policy changes as well as adjustments to roles, responsibilities and internal processes, and updated compliance requirements.
    - SecureTrust will not offer any legal guidance or counseling.
    - 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.