SecureTrust
a Trustwave division

Service Description

National Institute of Standards and Technology

Privacy Framework Consulting

Contents

National Institute of Standards and Technology (NIST) Privacy Framework Consulting

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Privacy Framework Consulting (the "**Service**") is designed assist and guide Client in understanding and adopting the National Institute of Standards and Technology (NIST) Privacy Framework.

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 Client's primary resource during the Service and is responsible for conducting the assessment, evaluating compliance, and producing the report.

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.

NIST Privacy Framework Consulting – The Security Consultant will consult with Client on the adoption of the NIST Privacy Framework.

DELIVERY AND IMPLEMENTATION

Project Initiation

The SecureTrust GCRS team will initiate the Service by scheduling and conducting a remote kickoff meeting to define and agree to a high-level project plan consisting of key steps, estimates for duration, deliverables, resource requirements, and escalation procedures.

The Project Initiation phase includes:

- Introduction to the SecureTrust Compliance Manager application for data sharing
- Setting out a high-level project plan
- Regular project status meetings with key stakeholders

NIST Privacy Consulting

SecureTrust will provide assistance and guidance to Client's privacy personnel on how to use the NIST Privacy Framework in the context of certain privacy laws, regulations, or business requirements. The Security Consultant will work with Client's privacy personnel to implement the NIST Privacy Framework.

Key activities may include:

- Identify Client privacy stakeholders or business owners responsible for the privacy program or adoption of the NIST Privacy Framework
- Review the critical components of the NIST Privacy Framework with Client's privacy personnel in the context of the laws, regulations, or business requirements to which Client is subject
- Review existing data protection strategies
- Engage with key management personnel to understand Client's strategy, objective, scope, and risk appetite with regard to NIST Privacy Framework adoption
- Discussion between Client and SecureTrust on Client's privacy business goals and strategic direction
- Review the key aspects of the NIST Privacy Framework (core, functions, profiles, etc.)
- Assist Client with use and adoption of NIST Privacy Framework and data protection strategies for processing, storing, transmitting, and sharing data

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 and escalation procedures.
- Schedule and conduct kickoff, periodic status, and closeout meetings.
- Interview appropriate organization personnel and collect information from such personnel.

CLIENT RESPONSIBILITIES

- 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, resource requirements and escalation procedures.
- 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 personnel 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:
    - The following personnel will typically need to be involved:
        - Personnel from Client's departments of 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 or Data Protection Officer.
    - The Service may consist of remote and onsite activities.
    - The 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 will perform the Service in the English Language.
    - SecureTrust will not create or modify Client documentation as part of the Service.
    - SecureTrust will not provide remediation services as 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 or any other 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.