



August 11, 2016

## SUPPLIER MANAGEMENT PROCESS

Supplier Trust supports Procurement, Legal and other Business Units (BUs) engaged directly in contract negotiations and the onboarding of third party suppliers. Supplier Trust engages in a tiered security review of the supplier during different stages in the lifecycle of the supplier relationship. Information on supplier security is gathered at the early stages of engagement with a possible supplier, during the contract negotiation process, and annually thereafter. This information gathered is used to determine and execute the security due diligence commensurate with the risk of a particular engagement.

The Supplier Trust process consists of a four phased approach to maintain security throughout the lifecycle of the relationship.

### 1. Engagement

During the engagement process the Supplier Trust team works with Procurement and the Business Unit to triage the security implications of the engagement and gather preliminary information on the security of the potential supplier.

### 2. Onboarding

During the onboarding phase, the Supplier Trust team requests more detailed information regarding the nature of the specific services provided and data classification (if applicable); it then uses the information gathered to determine the appropriate security requirements that should be included in the contract. The Supplier Trust team communicates the security language requirements to the Symantec stakeholders (e.g., Procurement) and requests applicable documentation.

### 3. Monitoring and Compliance

The monitoring process begins once an agreement is executed between the supplier and Symantec. Depending on the nature of services provided, Supplier Trust may collect (1) a SOC 2 Type II report and/or ISO 27001 certificate with corresponding Statement of Applicability (or other security certification), (2) executive summary of a network penetration test, (3) vulnerability scan, (4) evidence of employee basic annual security training, (5) evidence of developer secure code training, and (6) PCI compliance documentation (e.g., Attestation of Compliance). Supplier Trust monitors the supplier to ensure that all the required evidentiary documents are updated at least annually.

### 4. Security Review

Supplier Trust synthesizes the data and metrics received during Onboarding and Monitoring with the goal of identifying suppliers who require a more in-depth review. Supplier Trust conducts this level of due diligence with the aim of achieving higher security. These reviews may include requests for additional documentation, questionnaires and/or onsite reviews. Any and all reviews are done in accordance with the supplier contract terms.

Please note that Symantec's Supplier Trust Process documentation contains proprietary and highly confidential information and we do not, as a business practice, share it. If you require more information regarding Symantec's Supplier Trust Process, please submit your request to [Supplier\\_Trust@symantec.com](mailto:Supplier_Trust@symantec.com).