Symantec™ Incident Response Retainer Services

Service Description

June 3, 2015

Service Overview

This Service Description, with any attachments included by reference, is part of any agreement which incorporates this Service Description by reference (collectively, the "Agreement"), for the Services described in this Service Description and are provided by Symantec. This Service Description shall apply to Services purchased by Customer on or after June 3, 2015. For Services purchased by Customer prior to June 3, 2015, the Service Description dated April 6, 2015 shall apply, a copy of which is available at http://go.symantec.com/proserveterms or upon request to Symantec.

Symantec™ Incident Response Retainer Services allow Customer to maintain access to critical capabilities needed to effectively respond to a security incident. Incident Response Retainer Services comprise one of the following services, depending on the offering purchased by Customer as indicated in the Subscription Instrument: (a) Incident Response Retainer Service - Standard ("**IRRS - Standard**"); (b) Incident Response Retainer Service - Enterprise ("**IRRS - Enterprise**"); (c) Incident Response Retainer Service - Advanced Enterprise ("**IRRS - Advanced Enterprise**"); or (d) any one of various add-on options ("**Add-On Option**"), (each a "**Service**" or collectively, "**Services**"), as further described in this Service Description. **All Services are available in the English language only.**

Table of Contents

Technical/Business Functionality and Capabilities

Service Features.

The following table illustrates the Service features associated with each Service.

SERVICE FEATURE	INCIDENT RESPONSE RETAINER SERVICES			SERVICE FEATURE DESCRIPTION
	IRRS - STANDARD	IRRS - ENTERPRISE	IRRS - ADVANCED ENTERPRISE	
INCIDENT RESPONSE ASSISTANCE	X	X	X	Customer will have access to a regional 24x7 phone number to request incident response assistance ("**Initial Call**"); a member of Symantec's Incident Response delivery team, will then return Customer's Initial Call according to the Service Level Agreement detailed below to further discuss the possible security incident.
SERVICE MANAGEMENT	X	X	X	Customer will be assigned a Symantec Service Manager. Symantec's Service Manager is assigned based on market segment or location, and Customer security maturity so that when Customer contacts Symantec to request assistance, information about other attacks affecting a specific vertical or locale can be leveraged to assist Customer with the assessment of the scope and severity of a security incident and receive customized recommendations.
INCIDENT RESPONSE READINESS SERVICE	1 per annual period of the Term (not to exceed 1 Service Period per annual period)	1 per annual period of the Term (not to exceed 1 Service Period per annual period)	1 per annual period of the Term (not to exceed 1 Service Period per annual period)	Symantec will assess Customer's ability to detect and respond to security incidents by leveraging questionnaires and conducting an onsite workshop to understand Customer's current definition of roles and responsibilities during a security incident. The Incident Response Readiness Service will not only provide Symantec with critical insights needed to help deliver an Incident Investigation based on Customer's unique environment, but also enable Symantec to provide recommendations which may assist in improving its response times and effectiveness during an Incident Investigation. Following the commencement of Services, Symantec's Incident Response delivery team will organize an initial call with Customer ("**Kick-Off Call**"). During the Kick-Off Call, Symantec's Incident Response delivery team and the Customer will setup a mutually acceptable time for the Incident Response Readiness Service to be provided by Symantec. If a time cannot be determined during that call, the Customer may contact the Incident Response Project Manager at a later date. Customer is strongly advised to setup the Incident Response Readiness Service as soon as possible in order to aid Symantec in delivering a quicker, more effective Incident Investigation, should one be required. During the first thirty (30) days of the annual period of the Term of the applicable Service, Customer may exchange the provision of the Incident Response Readiness Service for one (1) Service Period of any of the Alternate Readiness Services or for one (1) Service Period of Incident Investigation.

SERVICE FEATURE	INCIDENT RESPONSE RETAINER SERVICES			SERVICE FEATURE DESCRIPTION
	IRRS - STANDARD	IRRS - ENTERPRISE	IRRS - ADVANCED ENTERPRISE	
EMERGING THREAT REPORTS	X	X	X	Symantec will periodically provide Customer with Emerging Threat Reports published by Symantec via email on emerging threats that may impact Customer's security posture. Emerging Threat Reports may contain the following: • Executive Summary • Technical Threat Details, Attack Vector • Detection Capabilities and Indicators • Mitigation Strategy and Recommendations • References to additional resources for more information
INCIDENT INVESTIGATION	Not Included	Includes 6 Service Periods per annual period of the Term	Includes 12 Service Periods per annual period of the Term	Customer shall contact Symantec to request an Incident Investigation. Based on the nature and type of security incident, Symantec and Customer will mutually agree on an appropriate number and type of responders and Service Period(s) required. Symantec will then provide Customer with a corresponding WAF describing these decisions, and Customer must sign and return the WAF to Symantec ("**Incident Investigation Registration**"). Incident Investigation Registration is the date of receipt by Symantec of the signed WAF. Following Incident Investigation Registration, Symantec will make arrangements to fly onsite or coordinate remote efforts to conduct an Incident Investigation in accordance with the Service Level Agreement below. Further details of what Symantec may perform during an Incident Investigation are provided below. Customer acknowledges and agrees that an Incident Investigation will use at least one (1) Service Period. In the event Symantec completes the Incident Investigation earlier than the natural expiration of the applicable Service Period(s), no credit or refund will be due to Customer for any unused portion. If Customer determines more time is needed than originally requested, Customer may request additional Service Period(s). Following Customer's request, Symantec will then provide Customer with a corresponding WAF, which Customer must sign and return to Symantec. For the avoidance of doubt, the applicable additional Service Period(s) requested by Customer will first be deducted from Customer's available Service Period(s); or if Customer has no Service Period(s) available, Customer may purchase the additional Service Period(s) required by Customer.

SERVICE FEATURE	INCIDENT RESPONSE RETAINER SERVICES			SERVICE FEATURE DESCRIPTION
	IRRS - STANDARD	IRRS - ENTERPRISE	IRRS - ADVANCED ENTERPRISE	
REMOTE INVESTIGATION	X	X	X	Symantec may perform certain remote investigations ("**Remote Investigation**") on Customer data, including, without limitation, hardware, software, images, memory, network, logs ("**Customer Data**"). Customer acknowledges and agrees that any such Remote Investigation performed by Symantec shall be subject to the following: (a) Remote Investigation of Customer Data shall be scheduled by Customer via the Incident Response delivery team; (b) Customer shall, at its sole cost and expense, be solely responsible for the delivery of Customer Data (on a medium to be mutually agreed with Symantec) to Symantec and the return of such Customer Data to Customer following conclusion of Remote Investigation; (c) Customer Data shall be delivered to Symantec at a location mutually agreed between Customer and the Incident Response delivery team, in a tamper-evident container (where applicable). Where applicable, Customer shall provide Symantec with the applicable delivery tracking number and shall ensure that Symantec's physical acknowledgement of receipt is required upon delivery ("**Symantec Receipt**"); (d) all Remote Investigation performed by Symantec shall be during Normal Business Hours only; (e) Symantec shall have no responsibility whatsoever with respect such Customer Data, including, without limitation, to any Customer Data that may remain within any Customer hardware (whether accessible, readable or not).
SERVICE LEVEL AGREEMENT	Within 3 hours	Within 3 hours	Within 3 hours	**Initial Call SLA**. Symantec's Incident Response delivery team shall return Customer's Initial Call within the applicable timeframe following receipt of Customer's Initial Call by Symantec. In the event Customer's Initial Call is not returned within the applicable timeframe, Symantec agrees to credit Customer's account with one (1) Service Credit.
	Within 12 Normal Business Hours	Within 12 Normal Business Hours	Within 12 Normal Business Hours	**Remote Investigation SLA**. Symantec will commence a Remote Investigation within the applicable timeframe following Symantec Receipt. In the event Symantec does not commence a Remote Investigation within the applicable timeframe, Symantec agrees to credit Customer's account with one (1) Service Credit.
	Not Included	Within 48 hours of Incident Investigation Registration	Within 24 hours of Incident Investigation Registration	**Incident Investigation SLA.** Symantec will have an Incident Investigation responder "in transit" to Customer's location for an Incident Investigation within the applicable timeframe following Incident Investigation Registration. The term "in transit" means the Incident Investigation responder will have commenced travel to Customer's location. In the event that the Incident Investigation responder is not "in transit" within the applicable timeframe, Symantec agrees to credit Customer's account with one (1) Service Credit for each Normal Work Day delay.

SERVICE FEATURE	INCIDENT RESPONSE RETAINER SERVICES			SERVICE FEATURE DESCRIPTION
	IRRS - STANDARD	IRRS - ENTERPRISE	IRRS - ADVANCED ENTERPRISE	
ADD-ON OPTIONS	X	X	X	If Symantec determines that an additional Incident Investigation (not already included in IRRS – Enterprise or IRRS – Advanced Enterprise) and/or additional Incident Investigation responder(s) are recommended during an Incident Investigation ("**Add-On Option(s)**"), Customer may choose to purchase such Add-on Option(s) from Symantec or via its nominated channel partner. Customer acknowledges and agrees that Add-On Option(s) are provided on a commercially reasonable efforts basis only. Accordingly, the Service Level Agreement does not apply to any Add-On Option(s).
ALTERNATE READINESS SERVICES	Not Included	X	X	During an annual period of the Term of the applicable Service, Customer may exchange Service Period(s) for any of the following Alternate Readiness Services (each as further described below): • Incident Response Plan Assessment • Incident Response Plan Development • Incident Response Tabletop Exercises • Incident Response Training • Advanced Threat Hunting Delivery of an Alternate Readiness Service is subject to Customer having appropriate Service Period(s) available and Symantec resource availability. Alternate Readiness Services must be scheduled by Customer via the Symantec's Incident Response delivery team at least thirty (30) days in advance. Symantec will provide Customer with a corresponding WAF describing the Alternate Readiness Service, and Customer must sign and return the WAF to Symantec. The total number of Service Period(s) required for each Alternate Readiness Service will vary as scoped by Symantec, but will require a minimum of at least one (1) Service Period. The Service Level Agreement shall not apply to any Alternate Readiness Service.

Incident Investigation

Subject always to the nature of Customer's security incident, logistics with respect to Symantec's delivery of the Services, and the number of Service Period(s) available and requested by Customer, Symantec may perform certain of the activities described below, as coordinated with Customer's Project Manager, solely to the extent Symantec can reasonably complete such activities based on the Service Period(s) requested by Customer:

Information Gathering and Project Coordination:

- Working with Customer to identify required Customer Incident response team resources including, without limitation, a Customer Project Manager.
- Reviewing Customer's networking diagrams to determine the design of the existing network infrastructure.

- Conducting onsite interviews with Customer's representatives and designated Customer personnel responsible for:
  - Managing servers, clients, and remote systems to determine connectivity and management processes;
  - Internet gateway security to determine availability of solutions to provide information security protection, monitoring and mitigation;
  - Email security to determine availability of solutions to provide information security protection, monitoring and mitigation managing the endpoint security solutions to identify monitoring capabilities.
- Establishing procedures for documentation of actions taken and the handling of findings.
- Scheduling the necessary resources and establishing meeting cadence in coordination with Customer's Project Manager.

Detection, Data Collection and Analysis:

Conducting an assessment of Customer's compromised information systems assets which may include the following tasks:

- Monitor hostile activity.
- Network packet capture and analysis.
- Log collection & analysis.
- Live system artifact collection.
- Physical system memory analysis.
- Disk analysis.
- Malware sample collection and advanced analysis.
- Cross-reference collected findings and indicators of compromise with Symantec analysts and with the Symantec Global Intelligence Network (GIN) to potentially identify links to campaigns and adversaries.
- Identify data extraction techniques.
- Other analysis as deemed necessary by Symantec.

Containment:

Review and analyze compromised information systems assets and provide a written analysis of the threat and short-term containment plan recommendations to assist with the following:

- Monitor and/or stop hostile activity.
- Isolate affected resources.
- Guide Customer through execution of the recommended containment plan.

Eradication and Recovery:

Review and analyze compromised information systems assets and provide a written strategy and recommendations for threat eradication and recovery.

Written Report and Presentation:

Upon completion of this engagement Symantec will deliver a set of documents containing the following types of components:

- **Executive Summary**
  - Background
  - Initial findings
  - Initial Attack Narrative
  - Scope of Compromise
  - Malicious Code
  - Involved High Profile Systems
  - Containment Strategy
  - Summary of Recommendations

- **Conclusions**
- **Detailed Findings**
  - Technical Findings
  - Attack Timeline
  - Attack Taxonomy
  - Identified Vectors
  - Analysis of Identified Threats
- **Recommendations**
  - Incident Specific Remediation/Mitigation steps
  - General Recommendations
- **List of tools used in Analysis**
- **Lists of Systems Analyzed**

Upon request, Symantec may also provide a presentation summarizing the contents of the written report outlined above, intended to be adaptable for Customer's use in briefing Customer's board of directors or senior executive staff.

Travel and Expenses ("T&E")

The Annual Subscription Charge does not include any travel and expenses ("**T&E**") that may be required to deliver Services. Travel and expenses up to Five Thousand U.S. Dollars ($5,000.00) (or the local currency equivalent for non-U.S. expenditures) per resource per Service Period, or Ten Thousand U.S. Dollars ($10,000) if intercontinental travels are involved shall be reimbursed to Symantec. Any T&E that Symantec incurs above the applicable amount must be pre-approved by Customer in writing. All T&E will be invoiced by Symantec at actual cost in accordance with Symantec's standard business practices.

Add-on Options

As the size and scope of a security incident can vary, Customer can purchase additional responders to help assist Customer to manage the additional capacity of work required during an Incident Investigation. Each quantity of an Add-On Option purchased entitles Customer to one specific corresponding additional responder for the Incident Investigation during one (1) Service Period and will be reflected in the applicable WAF.

Additional Responders	Description
Investigator	An Investigator assists in the identification of targets for evidence collection, the collection of evidence, and analysis of what was collected to provide critical insights into an attack narrative.
Lead Investigator	A Lead Investigator has a minimum of 8 years of practical experience performing incident response work, leading investigations, and communicating and collaborating with C-level executives to align investigation outcomes to business goals.
Specialist	A Specialist can add a particular skillset to an Incident Investigation. Symantec has responders available who specialize in a variety of Symantec and 3rd party technologies used to help contain a security incident. A Specialist maintains core competencies in specialized areas such as malware outbreak assistance, web application and mobile device penetration testing, and incident response planning that can add specialized expertise to assist in the incident response lifecycle.

Additional Responders	Description
Symantec Project Manager	A Symantec Project Manager coordinates all areas of the Incident Investigation project delivery process to assist Customer in finding and eradicating threats in Customer's environment. A Project Manager will support Customer with security operations knowledge that can be critical in managing a large scale Incident Investigation.
Senior Leader	A Senior Leader collaborates with CISO and CIO level Customer stakeholders to build and deliver an effective communication plan and messaging platform Customer may use with their senior executive staff and board of directors.

Alternate Readiness Services

Incident Response Plan Assessment

An incident response plan assessment comprises in-depth assessment of Customer's information security incident response plan. Symantec will work with Customer to determine current and future needs and examine how the incident response plan currently operates from a strategic, operational and tactical viewpoint. This approach allows Symantec to provide a holistic review of Customer's incident response plan. Dependencies between Customer's incident response team, other internal teams and third parties will also be reviewed to determine the effectiveness and efficiency of these arrangements. An incident response plan assessment is performed using a series of questionnaires, workshops and interviews, typically over a three or four week period, and a three or four day onsite review. Symantec will provide an assessment snapshot with recommended actions presented at the end of the onsite visit.

Incident Response Plan Development

An incident response plan helps minimize the impact of security incidents and shortens the timeframe between incident identification and incident resolution. Accordingly, an incident response plan should foster a continuous improvement process that leverages lessons learned from past incidents to improve overall security effectiveness. An incident response plan documents the processes and procedures, roles and responsibilities of various stakeholders, and communications flows and notifications procedures that are critical in timely recovery from security incidents. Symantec will leverage its experience in responding to incidents throughout the globe combined with industry best practices to produce an Incident Response Plan tailored to Customer's organizational needs and unique requirements.

Incident Response Tabletop Exercises

Symantec will use a table top exercise (TTX) to test and refine Customer's existing incident response plan or process. The TTX is performed in a conference room where Customer's key stakeholders talk through the incident response plan or process and their response to a particular incident without the need to actually deploy Customer equipment or resources. During the TTX gaps and weaknesses in the incident response plan or process may be identified. After the TTX, a debriefing will occur to review findings and create a plan for improving the incident response process.

Incident Response Training

Symantec will provide incident response training to assist Customer in the initial identification and containment of security incidents. Training may be tailored to specific Customer requests, internal team composition and specific security incident response handling requirements. Training topics may include security awareness, current security trends, data handling, volatile data collection, or other relevant areas.

Advanced Threat Hunting

Symantec will search Customer's network to attempt to uncover the presence of compromises and threat activity previously unidentified in Customer's environment ("**Advanced Threat Hunting**"). Symantec uses proprietary hunting methodology and technologies to search networks and identify the presence of possible threats ranging from undetected malware to full advanced persistent threat activity. Advanced Threat Hunting uses Symantec's vast intelligence resources that include indicators from the Symantec Global Intelligence Network, and research from Symantec analysts. Symantec will provide Customer with a better understanding of any potential exposure that may have been uncovered during the exercise and provide recommendations for containment and eradication.

Customer Responsibilities

Customer acknowledges and agrees that Symantec can only perform the applicable Service if Customer provides required information or performs required actions as set forth in the Agreement or as reasonably requested by Symantec. Accordingly, and without limitation, if Customer does not meet the following responsibilities, Symantec's performance of the applicable Service may be delayed, impaired or prevented, as noted below:

- **Project Manager**. Customer will nominate a "Project Manager" to assist Symantec in coordinating Customer resources in a timely manner and to act as the focal point for resolution of Service related issues. Customer's Project Manager shall also have the necessary technical and business knowledge and authority to make decisions concerning the Service. In addition, Customer shall assign an appropriate number of suitable skilled personnel to assist and cooperate with Symantec consistent with the Service described in this Service Description. Customer will further provide escalation/contact information for required resources. Customer must identify and provide the names for Customer's incident response resources.

- **Facilities**. Customer will provide Symantec with all necessary cooperation, information and support that may reasonably be required by Symantec for the performance of the Service including, without limitation, arranging and/or obtaining appropriate travel documentation (including work permits, visas, etc.), access to suitably configured computers, unrestricted network physical connectivity, technical support resources for installing network monitoring hardware, software products and applicable passwords, at such times as Symantec requests. In addition, Customer will provide Symantec personnel with access to all buildings, phone systems, internet access, server rooms, and workstations, and will provide all necessary passes for access to such areas if work is required by Customer outside of a Normal Business Hours. Customer will also provide access to a suitable conference room facility for meetings, interviews, and facilitated sessions during any on-site components of the engagement and provide technical support resources for installing network monitoring hardware, where applicable.

- **Information**. Customer will ensure that Symantec has access to the following at all times: (i) materials and resources related to Customer's business and technical environment; (ii) software design documentation, current design diagrams, and other information required to deliver the Service; (iii) access to all operating systems and network and computing environments necessary to complete the Service. Where applicable, such access shall include various user accounts for relevant applications, as needed, to perform for example, a penetration assessment, including, a list of relevant IP addresses, URLs and user authentication.

Service-Specific Terms

Service Conditions

- Anything not specifically described in this Service Description is out of scope and is not included in the Service.
- All Services expire if not used and delivered during the Term (including without limitation any applicable Incident Investigations) and no credit or refund will be due Customer for any expired or unused Services.
- Customer authorizes Symantec to perform any offsite analysis of Customer data necessary for the Service. Accordingly, Customer acknowledges and agrees that Symantec may be required to connect its computers and equipment directly to Customer's computer network. Customer explicitly consents to Symantec connecting its computers and equipment directly to Customer's computer network and Customer assumes all risk and liability in this regard and Symantec shall have no liability in this regard whatsoever.
- Except for Customer's 24/7 access to request assistance (as described in the Service features), all Services will be performed during Normal Business Hours. However, it is understood that an Incident Investigation is provided on an urgent basis, and that flexibility may be requested and accommodated, subject to local labor laws and the free choice of the individual resources delivering the Incident Investigation.
- **Exclusions.** The following services ("**Litigation Support Services**") are explicitly excluded from the Services:
    - Depositions, fact witness testimony, expert witness testimony, affidavits, declarations, expert reports;
    - Responding to discovery requests, subpoenas;
    - eDiscovery services;
    - Other forms of litigation support or participation in any legal proceeding relating to the subject matter of the engagement (including those involving a governmental entity).

  Litigation Support Services. Although the parties acknowledge that the Services may be sought by Customer at the direction of Customer's legal counsel, it is neither Symantec's nor Customer's intention for Symantec to perform Litigation Support Services. If, however, Symantec is later compelled to perform any Litigation Support Services, Customer and Symantec agree the following would apply to those Litigation Support Services regardless of whether such Litigation Support Services are sought directly by Customer or by a third party, and notwithstanding any conflict with other terms:

    - The then-current hourly rate would apply for all Symantec personnel who perform Litigation Support Services. Litigation Support Services are provided on a time and materials basis, since the actual time required to complete Litigation Support Services may vary.
    - The parties will work in good faith to document the terms in this "Litigation Support Services" section as well as any additional necessary terms and conditions in a separate agreement at such time as the need for Litigation Services should occur.
    - This "Litigation Support Services" Section will survive termination or expiration of the Agreement.

  Privilege. If Customer has listed General Counsel contact information in the Required Contact Information Form or has otherwise entered into a separate agreement confirming that the engagement is being conducted at the request of, and at the direction of, Customer's legal counsel, Symantec will work with all reasonable requests from Customer's legal counsel to preserve any attorney-client, attorney work product, or other applicable privileges. Symantec will treat all findings, reports and documentation it provides to Customer as part of the Services as Confidential Information.

  Indemnification. Customer will fully indemnify and reimburse Symantec for all losses, damages, liabilities, expenses, costs, and fees (including reasonable attorney's fees) and for Symantec personnel time (at the hourly rate listed above for Litigation Support Services) incurred in connection with any allegation, claim, demand, subpoena, or legal proceeding (including those involving a governmental entity) arising from any incident for which Customer has engaged Symantec to provide the Services, regardless of fault.

- Customer acknowledges and agrees that in the course of delivering the Services, Symantec may become aware of issues such as data breaches, network intrusions, or the presence of malware, and that such issues may give rise to regulatory reporting obligations which Customer is subject to in one of more territories in which Customer operates. Accordingly, Customer shall remain solely responsible for all such reporting requirements and Symantec shall have no liability in this regard whatsoever.
- Customer acknowledges, understands and agrees that Symantec does not guarantee or otherwise warrant that the Service, or Symantec's recommendations and plans made by Symantec as a result of that Service, will result in the identification, detection, containment, eradication of, or recovery from all of Customer's system threats, vulnerabilities, malware, malicious software, or other malicious threats. Customer agrees not to represent to anyone that Symantec has provided such a guarantee or warranty.
- Symantec reserves the right to assign any suitable skilled resource(s) available to provide Services. Symantec is not obligated to provide a specific Symantec resource or third-party resource.
- Access Rights: Customer acknowledges, understands and agrees that an unauthorized intrusion into wireless access points may be prohibited by applicable local law. By agreeing to this Agreement, Customer is: (i) explicitly confirming to Symantec that it has obtained all applicable consents and authority for Symantec to deliver the Service; and (ii) giving Symantec explicit permission to perform the Service and to access and process any and all data related to the Service, including without limitation, consent to analyze network traffic in real time to detect evidence of known malicious communication patterns and traffic containing unrecognized malicious code (malware), connect to Customer's computer network, archive and retain all network traffic captured as part of Services (including to store any malware and metadata supplied by Customer, or anyone else working with or for Customer), and (iii) representing that such access and processing by Symantec does not violate any applicable law or any obligation Customer owes to a third party; and (iv) accepting sole responsibility and liability with respect to engagement of such Service. Accordingly, Customer warrants and represents that it is the owner or licensee of any network, systems, IP addresses software, appliances, code, templates, tools, policies, records, working papers, data and/or computers upon which Symantec performs the Service ("Customer Systems"), and that Customer is authorized to instruct Symantec to perform the Service on such Customer Systems. Customer shall fully indemnify and hold harmless Symantec for any claims by any third parties with respect to the Service.
- Applicable law or regulation(s) of the country in which Services, including without limitation an Incident Investigation, will be performed may limit or alter the scope of the Services.

Service Level Agreement

- A Service Credit shall equal 2.5% of the Annual Subscription Charge for the applicable Service. Service Credit(s) granted hereunder will first be applied toward Customer's next invoice due for the applicable Service, or if no additional invoice is due for the applicable Service, as a payment. Notwithstanding anything to the contrary in the Agreement, in no event shall Symantec be required to credit Customer more than 7.5% of the Annual Subscription Charge payable by Customer for the affected Service in any calendar month and Symantec's maximum cumulative liability to issue Service Credits for an annual period shall not exceed the Annual Subscription Charge. Symantec's sole and exclusive obligation and Customer's sole and exclusive remedy for this Service Level Agreement shall be limited to the issuance of Service Credits.
- If Customer believes it is entitled to a remedy in accordance with the Service Level Agreement, Customer must submit a Service Credit Request within ten (10) business days of the end of the calendar month in which the suspected Service Level Agreement non-compliance occurred.
- All Service Credit Requests will be subject to verification by Symantec.
- Symantec shall not be responsible for its inability to perform Services (including meeting the Service Level Agreement): (i) due to a Force Majeure Event; (ii) during any period of suspension of Service by Symantec in accordance with the terms of the Agreement; (iii) where Customer is in breach of the Agreement (including without limitation if Customer has any overdue invoices); or (iv) Symantec resources are required to obtain visas prior to performing work in Customer's country.

- The remedies set out in the Service Level Agreement shall be Customer's sole and exclusive remedy in contract, tort (including without limitation negligence) or otherwise, with respect to the Service Level Agreement.

Definitions

Capitalized terms used in this Service Description shall have the meaning given below. Any capitalized terms not defined in this Service Description shall have the same meaning as in the Subscription Instrument.

"Annual Subscription Charge" means the annual charge Customer has paid for the Service that Customer has subscribed to in the Subscription Instrument.

"Normal Work Day" means a day that comprises the Normal Business Hours.

"**Normal Business Hours**" means the normal working hours, typically between 8.00 a.m. and 5.30 p.m. local time, exclusive of any applicable statutory rest periods, weekends and public holidays, as observed in the country in which Services are performed.

"**Service Credit**" means the amount of money that will be refunded to Customer or credited to Customer's next invoice after submission of a Service Credit Request and validation by Symantec that a Service Credit is due to Customer.

"Service Credit Request" means the notification which Customer must submit to Symantec by email to Customer's Service Manager.

"**Service Period**" means one Symantec resource working a period of consecutive five (5) Normal Work Days.

"**Subscription Instrument**" means one or more of the following applicable documents which further defines Customer's rights and obligation related to the Service: a Symantec certificate or a similar document issued by Symantec, or a written agreement between Customer and Symantec, that accompanies, precedes or follows the Service.

"**WAF**" or "**Work Authorization Form**" means the form Symantec provides to Customer wherein Customer authorizes and acknowledges the location, contact information, T&E, Add-On Option(s), Alternate Readiness Service(s), and/or Service Period(s) for Incident Investigation(s).

END OF SERVICE DESCRIPTION