MASTER LICENSE AGREEMENT

Customer Company Name:	**General Services Administration**								
Address:	Contact Name: Email: Address: *(All fields are required)* Country:								
Symantec Agreement Number: *(To be filled in by Symantec)*							O	T	H
Effective Date: *(To be filled in by Symantec upon signature)*									

This Master License Agreement ("Agreement") is entered into by and between **Symantec Corporation,** a Delaware corporation**,** and Customer (identified above) as of the Effective Date defined above. This Agreement consists of these terms and conditions ("Master Terms") and any Addenda executed under these Master Terms. This Agreement applies to the Symantec software products available for purchase through the applicable GSA Schedule 70 contract from an authorized Symantec reseller, and any mention in the Agreement of "Professional Services" or other services available for additional fees does not add such services to the reseller's GSA Schedule contract.

Customer and Symantec agree as follows:

1 Definitions. All capitalized terms may be used in the singular or in the plural, as the context requires.

1.1 "Addendum" to this Agreement means any addendum, including its exhibits or attachments, executed between the parties from time to time, which references this Agreement and supplements or modifies these Master Terms.

1.2 "Business Critical Services" means Symantec's commercially-available Business Critical Services offerings, subject to the additional terms and conditions of the Business Critical Services Addenda in Attachment 4.

1.3 "Certificate" means the machine-generated certificate sent to Customer by Symantec to confirm a purchase of the applicable Licensed Software and/or Maintenance/Support and/or (at Symantec's discretion) certain Services.

1.4 "Customer" means the end user licensee named below.

1.5 "Documentation" means the user manuals and release notes accompanying the Licensed Software.

1.6 "Effective Date" of this Agreement means the relevant date assigned by Symantec upon acceptance of this Agreement.

1.7 "EULA" means Symantec's end user license agreement accompanying the Licensed Software. The only portion of the EULA that shall apply to the Licensed Software is the Section 17 (Additional Terms and Conditions) of each EULA. Such EULAs may be reviewed at any time at http://www.symantec.com/about/profile/policies/eulas. For the avoidance of doubt, if an Ordering Activity places its order for Licensed Software, then such Ordering Activity is deemed to have reviewed and approved Section 17 of the applicable EULA.

1. 8 "Licensed Software" means the Symantec software products in object code form, that are commercially available on Symantec's applicable in-country price list in effect at the time of Customer's order, and any software updates provided under Maintenance/Support.

1.9 "Maintenance/Support" means the commercially-available Symantec maintenance/technical support services ordered by Customer for the Licensed Software, provided pursuant to Symantec's then-current maintenance/support policies and processes.

1.10 "**Managed Security Services**" means Symantec's commercially-available managed security services offerings, subject to the additional terms and conditions of the Managed Security Addenda in Attachment 5.

1.11 "MSRP" means Symantec's then-current in-country suggested list price in effect at the time of Customer's order.

1.12 "Ordering Activity" means a government entity authorized to purchase under the applicable General Services Administration federal supply schedule at the time an order is placed.

1.13 "Professional Services" means Symantec's commercially-available professional services offerings, subject to the additional terms and conditions of the Professional Services Terms Addendum in Attachment 2.

1.14 "Services" means collectively, Professional Services, Business Critical Services and Managed Security Services.

1.15 "Subscription Software" means Licensed Software licensed on a non-perpetual (term-limited) basis, as set forth in the applicable Addendum or Certificate.

1. 16 "Symantec" means the licensor entity named above.

1. 17 "Territory" means the geographic area in which Customer is authorized to purchase, install and use the Licensed Software. For purposes of this Agreement, Customer's Territory is: the United States or any U.S. Government installation sites world-wide.

1.18 "Use Level" means the license unit of measurement or model, including operating system or machine tier limitation, if applicable, by which Symantec measures, prices and sells the right to use a given Licensed Software product, in effect at the time an order is placed, as indicated in the applicable Addendum, Certificate or EULA, in that order of precedence.

2. License Grant.

2.1 Except with respect to the limited assignability of Licensed Software as set forth in Section 2.2 below, and notwithstanding any license rights to the contrary in Section 8, Utilization Limitations of the applicable GSA Schedule Contract, Symantec grants Customer, a non-exclusive, non-transferable license in the Territory to use (and to allow Customer's Ordering Activities to use) the Licensed Software in accordance with the Documentation, solely in support of Customer's and Ordering Activities internal business operations, in the quantities and at the Use Levels purchased from Symantec. The term of each Licensed Software license granted under this Agreement shall be perpetual, except for Subscription Software, for which Customer purchases a term-limited license as set forth in an applicable Addendum or Certificate. For archival purposes, Customer may make a single uninstalled copy of the Licensed Software and Documentation. All copies made pursuant to this section shall be complete copies, and shall include all copyright, trademark, and other notices in the original. Customer may not otherwise copy the Licensed Software or Documentation without Symantec's prior written consent.

Customer or Ordering Activities may allow consultant(s) or outsourcer(s) to use Customer's Licensed Software licenses to deliver dedicated services to Customer or to an Ordering Activity , so long as such use is consistent with Customer's own permitted scope of use, and is compliant with the terms of this Agreement. Customer and Ordering Activity agree that each is responsible for such third party access and use of the Licensed Software, to the same extent as if such consultant(s), outsourcer(s) or were Customer's employees.

If Customer purchases a Licensed Software license designated by Symantec for home use ("Home Use"), where available, then Customer may allow Customer's or an Ordering Activity's employee or dedicated consultant to use one copy of such Licensed Software on his or her personal home computer, provided such equipment is not owned or provided by Customer or an Ordering Activity, and provided such individual also has a computer licensed for such product at Customer's or the Ordering Activity's offices, but only for so long as such individual remains Customer's or the Ordering Activity's employee or dedicated consultant. The number of Home Use copies made and used cannot exceed the number of Home Use licenses purchased.

Symantec retains all title, copyright and other proprietary rights in the Licensed Software and Documentation, and in all copies, improvements, enhancements, modifications and derivative works thereof, including without limitation all patent, copyright, trade secret and trademark rights. Customer's rights to use the Licensed Software and Documentation shall be limited to those expressly granted in this Agreement and the applicable Addendum. All rights not expressly granted to Customer are retained by Symantec.

Non-Software Products. For any non-software products purchased by Customer under this Agreement, the terms and conditions for such products shall be as set forth in the applicable Certificates. For the avoidance of doubt, if an Ordering Activity places its order for non-software products, then such Ordering Activity is deemed to have reviewed and approved the applicable Certificate. The Dell Hardware/Appliance EULA is attached hereto as Attachment 3.

2.2 Customer may, based on its prime contract with a specific U.S. Government agency, assign Licensed Software licenses to such U. S. Government agency during the term of this Agreement. Customer must complete a License Assignment Request form in the form required by Symantec and otherwise comply with Symantec's then-current License Assignment Policy. Such assignment shall be at no additional cost to the U.S. Government, except for subsequent renewal of Maintenance/Support services, which the subject U.S. Government agency may or may not elect to procure. If Customer has obtained Maintenance/Support services in support of the Licensed Software, then Customer shall assign the remainder of any associated Maintenance/Support services to the U.S. Government agency to which Customer assigns the Licensed Software. Any U.S. Government agency to which Customer assigns Licensed Software and Maintenance/Support services under this Section must agree in writing to be bound by the terms and conditions of this Agreement. Certain purchasing Addenda may limit Customer's right to assign licenses purchased under and during the term of such Addenda.

3. License Restrictions. Customer shall not, without Symantec's prior written consent, conduct, cause or permit the: (a) use, copying, modification, rental, lease, sublease, sublicense, or transfer of the Licensed Software or Documentation, except as expressly provided in this Agreement; (b) creation of any derivative works based on the Licensed Software or Documentation; (c) reverse engineering, disassembly, or decompiling of the Licensed Software (except that Customer may decompile the Licensed Software for the purposes of interoperability only to the extent permitted by and subject to strict compliance under applicable law); (d) use of the Licensed Software or Documentation in connection with a service bureau or like activity whereby Customer, without purchasing a service bureau license from Symantec, operates or uses the Licensed Software or Documentation for the benefit of a third party; or (e) use of the Licensed Software or Documentation by any party other than Customer. In addition, Customer shall only use the number and type of Licensed Software licenses for which it has purchased an appropriate quantity and Use Level.

4. Orders. Customer may acquire copies of the Licensed Software, Maintenance/Support, Professional Services, Business Critical Services and/or Managed Security Services by submitting a Purchase Order to Symantec or to a Symantec Authorized Reseller.

5. Delivery.

5.1 **Delivery – Direct Orders to Symantec**. Customer elects to receive all Licensed Software via electronic download where available, and via tangible format where electronic download is not available. Customer acknowledges that Symantec may deliver upgrades and patches to Licensed Software under Maintenance/Support using tangible media as part of mass mailings. The terms of any physical delivery shall be F.O.B. destination.

5.2 **Delivery – Orders to Symantec Authorized Reseller**, Symantec shall not be responsible for delivery under terms other than those stated in Section 5.1, notwithstanding that Customer and a Symantec Authorized Reseller may negotiate other delivery terms.

6. Maintenance/Support. Customer may purchase Maintenance/Support for the applicable Licensed Software. Maintenance/Support is provided and performed subject to Symantec's then-current policies and processes. Symantec may amend its Enterprise Technical Support Policy from time to time in its sole discretion; provided, however, that for a period of five (5) years from the Effective Date of this Agreement, Symantec agrees that any such changes shall not significantly degrade the material elements of the Maintenance/Support plan offering provided to Customer. Substantive revisions of such Maintenance/Support policies or processes shall apply to Customer only when Maintenance/Support is renewed. Current Maintenance/Support terms and conditions are available at http://www.symantec.com/business/support/support_policies.jsp.

7. Services.
(a) **Professional Services**. Customer may purchase Services, which are provided and performed pursuant to the Professional Services Terms Addendum in Attachment 1 and any applicable statement(s) of work.

(b) **Business Critical Services**. Customer may purchase such Business Critical Services, which are provided and performed pursuant to Attachment 3.

(c) Managed Security Services. Customer may purchase such Managed Security Services, which are provided and performed pursuant to Attachment 4.

8. Payment Terms; Taxes
8.1 **Payment**.
8.1.1 **Payment Terms – Direct Orders to Symantec**. Customer shall pay all invoices according to the terms of the applicable GSA Schedule Contract.

8.1.2 **Payment Terms – Orders to Symantec Authorized Reseller**. For orders placed with a Symantec Authorized Reseller, payment shall be in accordance with the terms and conditions negotiated between the Symantec Authorized Reseller and the Customer.

8.2 **Taxes**.
Taxes will not apply to charges for products or services directly paid for by the Federal Government, if such exemption is allowed by the tax jurisdiction in which the products or services are delivered.

9. Warranties.

9.1 Media. If Symantec provides Customer tangible media for Licensed Software, Symantec warrants that the magnetic media upon which the Licensed Software is recorded will not be defective under normal use, for a period of ninety (90) days from delivery. Symantec will replace any defective media returned to it within the warranty period at no charge to Customer.

9.2 Licensed Software**.** Symantec warrants that the Licensed Software, as delivered by Symantec and when used in accordance with the Documentation, will substantially conform to the Documentation for a period of ninety (90) days from delivery. If the Licensed Software does not comply with this warranty and such non-compliance is reported by Customer to Symantec within the ninety (90) day warranty period, Symantec will do one of the following, selected at Symantec's reasonable discretion: either (a) repair the Licensed Software, (b) replace the Licensed Software with software of substantially the same functionality, (c) terminate the license and refund the relevant license fees paid for such non-compliant Licensed Software, or (d) in the case of software updates provided under Maintenance/Support, refund the relevant Maintenance/Support fees. The above warranties specifically exclude defects resulting from accident, abuse, unauthorized repair, modifications or enhancements, or misapplication.

9.3 Maintenance/Support and Business Critical Services**.** Symantec warrants, for a period of thirty (30) days from the date of performance of Maintenance/Support, that such Maintenance/Support will be performed in a manner consistent with generally accepted industry standards. For Maintenance/Support not performed as warranted in this provision, and provided Customer has reported such non-conformance to Symantec within thirty (30) days of performance of such non-conforming Maintenance/Support, Symantec will, in its reasonable discretion either correct any nonconforming Maintenance/Support or refund the relevant fees paid for the nonconforming Maintenance/Support.

9.4 Professional Services and Managed Security Services.

(a) Professional Services. Symantec will provide the Professional Services described in the Statement of Work ("SOW") in a good and workmanlike manner and in accordance with generally accepted industry standards.

(b) Managed Security Services. Unless otherwise specified in the Managed Security Services Certificates attached hereto, the Managed Security Service(s) will be performed in a good and workmanlike manner and in accordance with: (a) generally accepted industry standards; and (b) the service level warranties indicated in the applicable Managed Security Service(s) Certificates.

9.5 Disclaimer of Warranties; Exclusive Remedies. THE WARRANTIES SET FORTH IN THIS SECTION 9 ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, CONCERNING THE LICENSED SOFTWARE AND RELATED MAINTENANCE/SUPPORT. THE REMEDIES SET FORTH ABOVE IN THIS SECTION 9 ARE CUSTOMER'S EXCLUSIVE REMEDY AND SYMANTEC'S SOLE LIABILITY WITH RESPECT TO THE APPLICABLE EXPRESS WARRANTIES SET FORTH ABOVE. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW SYMANTEC EXPRESSLY DISCLAIMS ALL OTHER WARRANTIES, INCLUDING ANY IMPLIED WARRANTIES OF SATISFACTORY QUALITY, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND STATUTORY OR OTHER WARRANTIES OF NON-INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS WITH RESPECT TO THIS AGREEMENT AND ITEMS OR ACTIVITIES CONTEMPLATED HEREUNDER. SYMANTEC DOES NOT WARRANT THAT THE LICENSED SOFTWARE SHALL MEET CUSTOMER'S REQUIREMENTS OR THAT USE OF THE LICENSED SOFTWARE SHALL BE UNINTERRUPTED OR ERROR FREE.

10. Intellectual Property Claims.

10.1 Symantec shall defend, indemnify and hold Customer harmless from any claim asserting that the Licensed Software infringes any intellectual property right of a third party, and shall pay any and all damages finally awarded against the Customer by a court of final appeal, or agreed to in settlement by Symantec and attributable to such claim. Symantec's obligations under this provision are subject to Customer's doing the following: notifying Symantec of the claim in writing, as soon as Customer learns of it; providing Symantec all reasonable assistance and information to enable Symantec to perform its duties under this Section. Notwithstanding the foregoing, Customer, through the Attorney General, acting by and through the attorneys of the US Department of Justice, may participate at Customer's expense in the defense of any such claim. Customer has the right to approve any settlement that affirmatively places on Customer an obligation that has a material adverse effect on Customer other than the obligations to cease using the affected Licensed Software or to pay sums indemnified hereunder. Such approval will not be unreasonably withheld.

10.2 If the Licensed Software is found to infringe, or if Symantec determines in its sole opinion that it is likely to be found to infringe, then Symantec shall either (a) obtain for Customer the right to continue to use the Licensed Software; or (b) modify the Licensed Software so as to make such Licensed Software non-infringing, or replace it with a non-infringing equivalent substantially comparable in functionality in which case Customer shall stop using any infringing version of the Licensed Software, or (if Symantec determines in its sole opinion that (a) and/or (b) are not commercially reasonable), (c) terminate Customer's rights and Symantec**'**s obligations under this Agreement with respect to such Licensed Software, and refund to Customer the license fee paid for the relevant Licensed Software, and provide a pro-rated refund of any unused, prepaid Maintenance/Support fees paid by Customer for the applicable Licensed Software.

10.3 Notwithstanding the above, Symantec will have no liability for any infringement claim to the extent that it is based upon: (a) modification of the Software other than by Symantec; (b) combination, use, or operation of the Licensed Software with products not specifically authorized by Symantec to be combined with the Software as indicated in the Documentation; (c) use of the Licensed Software other than in accordance with the Documentation and this Agreement; or (d) Customer's continued use of infringing Licensed Software after Symantec, for no additional charge, supplies or offers to supply modified or replacement non-infringing Licensed Software as contemplated under 10.2(b) above.

THIS SECTION 10 STATES CUSTOMER'S SOLE AND EXCLUSIVE REMEDY AND SYMANTEC'S SOLE AND EXCLUSIVE LIABILITY REGARDING INFRINGEMENT OR MISAPPROPRIATION OF ANY INTELLECTUAL PROPERTY RIGHTS OF A THIRD PARTY.

11. LIMITATION OF LIABILITY. EXCEPT AS LIMITED BY APPLICABLE LAW, THE FOLLOWING SHALL APPLY NOTWITHSTANDING THE FAILURE OF THE ESSENTIAL PURPOSE OF ANY LIMITED REMEDY AND REGARDLESS OF THE LEGAL BASIS FOR A CLAIM: IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER PARTY OR TO ANY PERSON FOR (i) ANY COSTS OF PROCUREMENT OF SUBSTITUTE OR REPLACEMENT GOODS AND SERVICES, LOSS OF PROFITS, LOSS OF USE, LOSS OF OR CORRUPTION TO DATA, BUSINESS INTERRUPTION, LOSS OF PRODUCTION, LOSS OF REVENUES, LOSS OF CONTRACTS, LOSS OF GOODWILL, OR ANTICIPATED SAVINGS OR WASTED MANAGEMENT AND STAFF TIME; OR (ii) ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL OR INDIRECT DAMAGES WHETHER ARISING DIRECTLY OR INDIRECTLY OUT OF THIS AGREEMENT.

THE FOREGOING SHALL APPLY EVEN IF (SUCH PARTY, ITS RESELLERS, SUPPLIERS OR ITS AGENTS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. EXCEPT FOR LIABILTY

ARISING FROM SYMANTEC'S OBLIGATIONS UNDER SECTION 10 (INTELLECTUAL PROPERTY CLAIMS), OR LIABILITY ARISING FROM BREACH OF SECTION 12 (CONFIDENTIALITY) OR FROM CUSTOMER'S BREACH OF ITS PERMITTED SCOPE OF AUTHORIZED USE UNDER THIS AGREEMENT, AND REGARDLESS OF THE LEGAL BASIS FOR THE CLAIM, EACH PARTY'S MAXIMUM LIABILITY UNDER THIS AGREEMENT SHALL NOT EXCEED THE FEES PAID OR OWED FOR THE LICENSED SOFTWARE, MAINTENANCE/SUPPORT SERVICES OR HARDWARE GIVING RISE TO THE CLAIM. NOTHING IN THIS AGREEMENT SHALL EXCLUDE OR LIMIT A PARTY'S LIABILITY FOR ANY LIABILITY WHICH CANNOT BE EXCLUDED OR LIMITED BY LAW. This Section 11, "Limitation of Liability", shall not impair the U.S. Government's right to recover for fraud or crimes arising out of or related to this Contract under any federal fraud statute, including the False Claims Act, 31 U.S.C. §§ 3729-3733. Furthermore, this clause shall not impair nor prejudice the U.S. Government's right to EXPRESS remedies provided in the applicable Schedule Contract (i.e. clause 552.238-72 – Price Reductions, clause 52.212-4(h) – Patent Indemnification, Liability for Injury or Damage (Section 3 of the Price List), and GSAR 552.215-72 – Price Adjustment – Failure to Provide Accurate Information).

12. Confidentiality.

12.1 "Confidential Information" means the non-public information that is exchanged between the parties, provided that such information is: (a) identified as confidential at the time of disclosure by the disclosing party ("Discloser"), or (b) disclosed under circumstances that would indicate to a reasonable person that the information ought to be treated as confidential by the party receiving such information ("Recipient"). A Recipient may use the Confidential Information that it receives from the other party solely for the purpose of performing activities contemplated under this Agreement ("Purpose"). For a period of five (5) years following the applicable date of disclosure of any Confidential Information, a Recipient shall hold the Confidential Information in confidence and not disclose the Confidential Information to any third party. A Recipient shall protect the Confidential Information by using the same degree of care, but no less than a reasonable degree of care, to prevent the unauthorized use, dissemination or publication of the Confidential Information as the Recipient uses to protect its own confidential information of a like nature. The Recipient may disclose the Confidential Information to agents and independent contractors with a need to know in order to fulfill the Purpose who have signed a nondisclosure agreement at least as protective of the Discloser's rights as this Agreement.

12.2 This provision imposes no obligation upon a Recipient with respect to Confidential Information which: (a) is or becomes public knowledge through no fault of the Recipient; (b) was in the Recipient's possession before receipt from the Discloser and was not subject to a duty of confidentiality; (c) is rightfully received by the Recipient without any duty of confidentiality; (d) is disclosed generally to a third party by the Discloser without a duty of confidentiality on the third party; or (e) is independently developed by the Recipient without use of the Confidential Information. The Recipient may disclose the Discloser's Confidential Information as required by law or court order provided: (i) the Recipient promptly notifies the Discloser in writing of the requirement for disclosure; and (ii) discloses only as much of the Confidential Information as is required. The Recipient's obligations with respect to the Confidential Information hereunder will survive any termination of the Agreement. Upon request from the Discloser or upon termination of the Agreement the Recipient shall return to the Discloser all Confidential Information and all copies, notes, summaries or extracts thereof or certify destruction of the same, except information that qualifies as a "Government Record" under the Federal Records Act (44 USC 3301).

12.3 Each party will retain all right, title and interest to such party's Confidential Information. Neither party to this Agreement acquires any patent, copyright or other intellectual property rights or any other rights or licenses under this Agreement except the limited right to use for fulfillment of the Purpose, as set forth in section 12.1 above. Nothing in this provision shall be construed to preclude either party from developing, using, marketing, licensing, and/or selling any product or service that is developed without use of the Confidential Information.

13. Verification. Except where prohibited by applicable federal law or security regulations, Customer or Ordering Activity as appropriate, agrees to keep accurate business records relating to its use and deployment of the Licensed Software. Upon thirty (30) days prior written notice, Customer agrees to provide Symantec written reports related to Customer's use of the Licensed Software to verify Customer's compliance with its obligations under this Agreement. Such report shall include, at a minimum, the product name (including any options, agents and extensions), version number, quantity of each product, and the operating system/platform, hardware model, Host ID and street address location of the Designated Computer on each such copy is installed. In the event that Customer fails to provide reports acceptable to Symantec; once annually, Symantec may verify Customer's compliance with this Agreement by reviewing (upon five (5) business days' prior written notice) Customer's use and deployment of the Licensed Software. Either Symantec or an independent public accounting firm reasonably acceptable to both parties shall perform the audit during Customer's regular business hours with minimal disruption to Customer's ongoing business operations and adherence to any security measures the Customer deems appropriate, including any requirements under Federal security regulations that may require personnel clearances prior to accessing sensitive information or facilities. Any nondisclosure agreement Customer may require the independent public accounting firm to execute shall not prevent disclosure of the audit results to Symantec. All audits shall be subject to Customer's reasonable safety and security policies and procedures. In the event unauthorized deployments of Symantec products are disclosed by the audit, Symantec will submit a claim to the contracting officer of the Customer or relevant Ordering Activity.

14. Term and Termination.

14.1 Term**.** Unless terminated as set forth in the applicable GSA Schedule Contract, these Master Terms shall continue indefinitely, and each Addendum shall continue for the term set forth in such Addendum.

14.2 Termination**.**

The provisions of this Agreement regarding confidentiality, restrictions on use of intellectual property, limitations on liability and disclaimers of warranties and damages, audit, and Customer's payment obligations accrued prior to termination, shall survive any termination. The license grants for Licensed Software and terms regarding Maintenance/Support purchased prior to termination shall survive such termination.

15. General

15.1 Governing Law; Severability; Waiver. This Agreement shall be governed by and construed in accordance with the laws of the United States. Such application of law excludes any provisions of the United Nations Convention on Contracts for the International Sale of Goods, including any amendments thereto, and without regard to principles of conflicts of law. If any provision of this Agreement is found partly or wholly illegal or unenforceable, such provision shall be enforced to the maximum extent permissible, and the legality and enforceability of the other provisions of this Agreement shall remain in full force and effect. A waiver of any breach or default under this Agreement shall not constitute a waiver of any other right for subsequent breach or default.

15.2 Assignment**.** Except with respect to the Licensed Software as set forth in Section 2.2 above, and subject to FAR 42.12 (Novation and Change of Name Agreements and its successor regulations), neither party may assign this Agreement, in whole or in part and whether by operation of contract, law or otherwise, without the other party's prior written consent. Such consent shall not be unreasonably withheld or delayed. For purposes

of this provision, a change of control shall constitute an assignment. Notwithstanding the foregoing, either party may, upon written notice to the non-assigning party, (i) assign this Agreement to a successor in interest to all or substantially all of its assets, whether by sale, merger, or otherwise, (ii) assign this Agreement to a parent company; or (iii) assign this Agreement to a wholly-owned subsidiary. All terms and conditions of the Agreement shall be binding upon any assignee hereunder; assignee's acceptance of these terms shall be evidenced by its performance hereunder.

15.3 Export. Customer acknowledges that the Licensed Software and related technical data and services (collectively "Controlled Technology") may be subject to the import and export laws of the United States, specifically the U.S. Export Administration Regulations (EAR), and the laws of any country where Controlled Technology is imported or re-exported. Customer agrees to comply with all relevant laws and will not to export or re-export any Controlled Technology in contravention to U.S. law, nor to any prohibited country, entity, or person for which an export license or other governmental approval is required. All Controlled Technology is prohibited for export or re-export to Cuba, North Korea, Iran, Syria and Sudan and to any country subject to relevant trade sanctions. Customer hereby agrees that it will not export, re-export or sell any Controlled Technology for use in connection with chemical, biological, or nuclear weapons, or missiles, drones or space launch vehicles capable of delivering such weapons.

15.4 Government Rights. The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR Part 12 and its successor regulations, and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, “Rights in Commercial Computer Software or Commercial Computer Software Documentation”, as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the Government shall be solely in accordance with the terms of this Agreement.

15.5 Entire Agreement**.** Any subsequent modifications to this Agreement shall be made in writing and must be duly signed by authorized representatives of both parties or they shall be void and of no effect. Unless an Ordering Activity and Symantec negotiate alternative terms, this Agreement prevails.

15**.**6 Force Majeure. Each party shall be excused from performance (other than payment obligations) for any period during which, and to the extent that, it is prevented from performing any obligation or service, in whole or in part, due to unforeseen circumstances or to causes beyond such party's reasonable control, including but not limited to acts of God, war, terrorism, riot, embargoes, acts of civil or military authorities, fire, floods, accidents, strikes, regulatory requirements or shortages of transportation, facilities, fuel, energy, labor or materials.

15.7 Notices. All notices required to be sent hereunder shall be in writing addressed to the relevant Contracting Officer or to Symantec’s corporate headquarters, with a simultaneous cc: to the attention of Symantec’s Legal Department/General Counsel. Notices shall be effective upon receipt, and shall be deemed to have been received as follows: (a) if personally delivered by courier, when delivered; (b) if mailed by first class mail, on the fifth business day after deposit in the mail with the proper address; or (c) if by certified mail, return receipt requested, on the date received.

15.8 Signatures. Facsimile signatures and signed facsimile copies of this Agreement, its Addenda, attachments and exhibits shall legally bind the parties to the same extent as originals. This Agreement with its accompanying Addendum/Addenda may be executed in multiple counterparts all of which taken together shall constitute one single agreement between the parties. The signatories hereto represent that they are duly authorized to sign this Agreement on behalf of their respective companies.

15.9 Subcontractors. Symantec may assign the Service(s) (Maintenance/Support, Business Critical Services or Managed Security Services) or any part thereof, and may additionally subcontract the Agreement and / or Service(s), provided that it remains responsible for any subcontractors performing on its behalf.

Attachment 1 – Professional Services Addendum

Attachment 2 – Hardware Warranty Agreement (Symantec 8160/8360/8380)

Attachment 3 – Business Critical Services

Attachment 4 – Managed Security Services

ATTACHMENT 1

PROFESSIONAL SERVICES TERMS ADDENDUM

ATTACHMENT 1

PROFESSIONAL SERVICES TERMS ADDENDUM

1. Statements of Work (a) During the Term (as defined in Section 2 below) Symantec and Customer (including Ordering Activity) may agree upon a written statement of work, quote/order form, or certificate under this Addendum (**"SOW"**), that may include descriptions of services to be performed by Symantec ("**Professional Services**") and deliverables **("Deliverables")** to be provided by Symantec, fees, duration and renewal of the Professional Services, and other responsibilities undertaken by Customer and/or Symantec. Certain Professional Services may require software, hardware and associated documentation to be separately provided by Symantec as part of the Service ("**Service Components**"). This Addendum will control in the event of any conflict with a SOW, unless otherwise specified in the SOW. However, the SOW may contain terms and conditions specific to the applicable Professional Services ordered which terms will have no effect on other SOWs.

2. Term; Termination. "**Term**" means the applicable effective period of this Addendum and/or of Professional Services under a Purchase Order or SOW. The Term of this Addendum will begin on the Effective Date and continue until termination. The Term for any Professional Services provided under this Addendum, which may include an initial set-up period, will be as set forth in the applicable Purchase Order or SOW and may be extended by mutual agreement of the parties. . This Addendum and/or a SOW may be terminated in accordance with the terms of the applicable GSA Schedule contract.

3. The Purchase Order issued by the Ordering Activity shall include any additional terms and conditions negotiated between Symantec and the Ordering Activity regarding payment for Professional Services fees, travel and living expenses incurred in the course of performance and reseller fees.

4. Rights in Deliverables.

(a) Ownership Rights. Subject to Symantec's rights in Symantec Information and Symantec Derivative Work as each are defined below, all Deliverables created specifically for and provided to Customer by Symantec under an SOW will, upon final payment, become the property of Customer for Customer's internal business purposes. Any inventions, designs, intellectual property or other derivative works of Symantec Information, will vest in and be the exclusive property of Symantec ("**Symantec Derivative Work**"). Any inventions, designs, intellectual property or other derivative works of Customer Information (as defined below) will vest in and be the exclusive property of Customer ("**Customer Derivative Work**").

(b) Pre-Existing Work. Any pre-existing proprietary or Confidential Information of Symantec or its licensors used to perform the Professional Services, or included in any Deliverable, including, but not limited to Service Components, software, appliances, methodologies, code, templates, tools, policies, records, working papers, know-how, data or other intellectual property, written or otherwise, including Derivative Works will remain the exclusive property of Symantec and its licensors (collectively, "**Symantec Information**"). Any Customer pre-existing information, including but not limited to any Customer proprietary and Confidential Information provided to Symantec by Customer will remain the exclusive property of Customer or its licensors ("**Customer Information**"). For the purposes of this Addendum, Symantec Information and Customer Information will be deemed Confidential Information.

(c) Retention. Customer acknowledges that Symantec provides similar services to other customers and that nothing in this Addendum or a SOW will be construed to prevent Symantec from carrying on such business. Customer acknowledges that Symantec may at its sole discretion develop, use, market, distribute and license substantially similar Deliverables. Notwithstanding the preceding sentence, Symantec agrees that it will not market or distribute any Deliverables that include the Confidential Information of Customer.

(d) License Grant. In consideration of Customer's payment of applicable Fees, Symantec grants Customer a limited, non-exclusive, non-transferable license, to access and use, in accordance with the SOW and solely for Customer's internal business purposes: (i) Symantec Information, to the extent such information is necessary to utilize the Professional Services or incorporated into any Deliverable; and (ii) Service Components in the format provided by Symantec, for use on systems under Customer's control, solely in connection with the Professional Services for which such Service Components are provided.

(e) License Restrictions. Customer will not act to infringe the intellectual property rights of Symantec or its licensors, including Symantec Information. Other than as expressly permitted under this Addendum or applicable law, Customer will not copy, sublicense, sell, rent, lease or otherwise distribute Symantec Information, or permit either direct or indirect use of Symantec Information by any third party. Customer will not modify, reverse engineer, disassemble, decompile, or create derivative works of Symantec Information, or otherwise attempt to build a competitive product or service using Symantec Information. Notwithstanding the foregoing, the license grant set forth above may be further limited as set forth in any applicable SOW.

(f) In the event that Customer, based on its prime contract with the U.S. Government, requires that data from analysis tasks performed under a SOW be transferable to a specific U.S. Government agency, then Customer shall identify the prime contract number and the U.S. Government Agency in that SOW. Symantec will allow the transfer request to the specified U.S. Government Agency under the prime contract number identified in the SOW. The rights in technical data transferred to the U.S. Government under the prime contract number identified in a SOW are set forth in Section (g) below. This provision will only apply to an Ordering Activity if the parties so state in an applicable SOW with such Ordering Activity.

(g) Government Rights. The data resulting from analysis tasks performed under an applicable SOW are deemed to be Commercial Items as defined in FAR Part 12 and its successor regulations, subject to restricted rights as defined in DFARS 252.227-7015, "Technical Data – Commercial Items", and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of such data by the U.S. Government agency identified in the applicable SOW shall be solely in accordance with the terms of this Agreement.

5. Intellectual Property Indemnification.

a) To the extent the Addendum includes provisions providing an express intellectual property indemnity for Licensed Software, such provision(s) are supplemented to add the Deliverables to the scope of the parties' obligations under such indemnification provisions, to the same extent as for such Licensed Software. Where Customer's use of the Deliverables is terminated pursuant to such provisions, the Deliverables shall be returned to Symantec and Symantec's sole liability, in addition to its indemnification obligations herein, shall be to refund to Customer the fees paid to Symantec for the relevant Services or portion thereof.

b) In the event that any willful misconduct or grossly negligent act or omission of a Party or its employees during the performance of Professional Services on Customer's premises causes or results in the (i) loss, damage to or destruction of physical property of the other Party or third parties, and/or (ii) death or injury to any person, then such Party will indemnify, defend and hold the Party harmless from and against any and all resulting claims, damages, liabilities, costs and expenses (including reasonable attorney's fees), subject to the Limitation of Liability of the Master Agreement, as supplemented below.

6. Non-Solicitation. During the Term of any applicable SOW, and for a period of one (1) year thereafter, neither Party will actively solicit for hire, nor knowingly allow its employees to solicit for hire, any employee of either Party associated with the performance of Professional Services under the applicable SOW without the prior written consent of the other Party. This provision will in no way restrict the right of either Party to solicit generally in the

media for required personnel, and will not restrict employees, contractors, or representatives of either Party from pursuing on their own initiative employment opportunities from or with the other Party. In the event a Party violates this provision, the Parties may mutually agree to liquidated damages.

7. Data Privacy. For the purpose of providing Professional Services pursuant to this Addendum, Symantec will require Customer to supply certain personal information e.g. business contact names, business telephone numbers, business e-mail addresses. Customer acknowledges that Symantec is a global organization, and such personal information may be accessible on a global basis by Symantec affiliates or Symantec partners and subcontractors, including in countries that may have less protective data protection laws than the country in which Customer is located. By providing such personal information, Customer consents to Symantec using, transferring and processing this information on a global basis for the use described above. For any question regarding the use of personal information, Customer may contact Symantec Corporation - Privacy Lead, 350 Ellis Street, PO Box 7011, Mountain View, CA 94043, U.S.A. Telephone 650-527-8000 Email: privacy@symantec.com.

8. Miscellaneous. (a) While on Customer's premises, Symantec will ensure that its personnel follow all reasonable instructions, as such are provided to Symantec prior to the performance of the Professional Services. **(b)** Symantec is an independent contractor and will not be deemed an employee or agent of Customer. **(c)** Symantec has the right to subcontract the performance of the Professional Services to third parties, provided that Symantec remains responsible for the contractual obligations according to this Addendum and any SOW.

Attachment 2
Hardware Appliance Warranty

Attachment 2
Hardware Appliance Warranty

1. **HARDWARE/SOFTWARE.** The hardware ("Hardware") that accompanies this Warranty Agreement is to be used only with the Licensed Software. "Licensed Software" means the Symantec software product, in object code form, that is pre-loaded, pre-installed, or included as a media kit accompanying the Hardware, including any documentation provided with such software. You may not use the Licensed Software unless You have purchased a separate license for such Licensed Software. Your use of the Licensed Software shall comply with the terms and conditions of the Master License Agreement that has been accepted as part of the applicable GSA Schedule contract and the License Instrument applicable for such Licensed Software. "License Instrument" means one or more of the following applicable documents which further defines Your license rights to the Licensed Software: a Symantec license certificate or a similar license document issued by Symantec, or a written agreement between You and Symantec, that accompanies, precedes or follows the Master License Agreement for the Licensed Software.

2. **OWNERSHIP.** The Licensed Software is the proprietary property of Symantec or its licensors and is protected by copyright law. Symantec and its licensors retain any and all rights, title and interest in and to the Licensed Software, including in all copies, improvements, enhancements, modifications and derivative works of the Licensed Software. Your rights to use the Licensed Software shall be limited to those expressly granted in this Warranty Agreement. All rights not expressly granted to You are retained by Symantec and/or its licensors.

3. **GEOGRAPHIC USE LOCATION.** Prior to using the Hardware, You must register a service tag for such Hardware in the location You intend to use the Hardware ("Geographic Use Location"). In the event You wish to change Your Geographic Use Location, You must re-register the Hardware using the tag transfer process located at http://www.symantec.com/business/support/contact_techsupp_static.jsp. Any change to the Geographic Use Location and/or any service request which requires Symantec to obtain additional information and/or validate information to acknowledge and approve warranty service entitlements may result in a delay in providing such warranty service entitlements.

4. **LIMITED WARRANTY.** Symantec warrants that the Hardware shall be free from defects in material and workmanship under normal authorized use and service and will substantially conform to the written documentation accompanying the Hardware for the applicable Warranty Period (defined in this Section 4) and as specified at the time of original purchase and in the packing slip documentation accompanying Your Hardware. The standard warranty period is three (3) years from the date of original purchase of the Hardware ("Standard Warranty Period"). However, if at time of original purchase You acquired extended warranty, as indicated in the packing slip documentation accompanying Your Hardware, the Hardware shall be warranted for a period of up to five (5) years from the date of original purchase ("Extended Warranty Period"). "Standard Warranty Period" and "Extended Warranty Period" shall collectively be referred to as "Warranty Period". Upon confirmation of a defect or failure of a Hardware, or component thereof, to perform as warranted in this Section 4, and depending on the then-current Geographic Use Location of the Hardware, Your sole and exclusive remedy for defective Hardware, or component thereof, if notified within the Warranty Period, shall be for Symantec, at its sole option and discretion, to:

(i) repair or replace the defective Hardware, or component thereof, with either a new or refurbished replacement Hardware, or component thereof, as applicable;

(ii) provide onsite repair services for any defective Hardware, or component thereof; or

(iii) repair or replace any defective Hardware returned to Symantec through Symantec's Returned Merchandise Authorization Services process for Hardware.

All defective Hardware, or component thereof, which has been replaced, shall become the property of Symantec. All defective Hardware, or component thereof, which has been repaired shall remain Your property. **EXCEPT FOR THE SPECIFIC WARRANTIES OR REMEDIES SET FORTH UNDER THE APPLICABLE GSA SCHEDULE, THE FOREGOING IS YOUR SOLE AND EXCLUSIVE REMEDY, AND SYMANTEC'S SOLE AND EXCLUSIVE LIABILITY FOR SYMANTEC'S BREACH OF THIS LIMTED WARRANTY.**

5. **LIMITED HARDWARE WARRANTY SUPPORT SERVICES.** During the Warranty Period, warranty support services will be provided in accordance with (i) the service procedures identified by Symantec in Section 7, below, and (ii) the then-current Symantec Enterprise Technical Support Policy in accordance with Section 6 (Maintenance/Support) of the Agreement

The Geographic Use Location of the Hardware will determine whether You are entitled to either warranty service consisting of (a) Next Business Day Service, (b) Same Day Service or (c) Return Merchandize Authorization Services as detailed below in this Section 5. Upon discovery of any failure of the Hardware, or component thereof, during the Warranty Period, the following options are available to You.

A. **Next Business Day Service**. You may initiate a request for next business day onsite repair services if You have purchased such services as part of Your warranty support. A service technician will, in most cases, be dispatched to arrive at Your location for onsite repair services on the next business day; Monday through Friday 8:00 AM to 6:00 PM local time, excluding regularly observed holidays. If the service technician is dispatched for onsite repair services after 5:00 PM local time, the service technician may take additional business day(s) to arrive at Your Geographic Use Location.

B. **Same Day Service**. If You have purchased the optional same day service upgrade, then for an additional fee and if offered in the then current Geographic Use Location, You may initiate a request for same day onsite services. A service technician will, in most cases, be dispatched to arrive at Your location for onsite service within the same day after dispatch, twenty-four (24) hours a day, seven (7) days a week (including holidays), provided the service location is between one hundred twenty-five (125) miles from the nearest parts stocking location.

C. **Return Merchandise Authorization Process**. In the event Symantec does not have Next Business Day Service, or Same Day Service available in Your then current Geographic Use Location or, if, Symantec determines in its sole discretion that Next Business Day**,** or Same Day Service may not be appropriate You are required to contact Symantec within ten (10) days after such failure and seek a return material authorization ("RMA") number. Symantec will promptly issue the requested RMA as long as Symantec determines that You meet the conditions for warranty service. The allegedly defective Hardware, or component thereof, shall be returned to Symantec, securely and properly packaged, freight and insurance prepaid, with the RMA number prominently displayed on the exterior of the shipment packaging and with the Hardware. Symantec will have no obligation to accept any Hardware which is returned without an RMA number. Symantec reserves the right, in its sole option, to repair or replace defective Hardware, or component thereof. With respect to a return of defective Hardware, or component thereof, Symantec and Customer or Ordering Activity will negotiate mutually agreeable transportation or other direct costs. With respect to a return

of functional Hardware, or return of Hardware ordered in error by Customer, Customer will pay any transportation costs. Any credits are subject to Symantec's then-current RMA (Return Materials Authorization) policies/process.

6. **SERVICE PARTS INSTALLATION.** Regardless of the service response level purchased, some component parts are specifically designed for easy removal and replacement by You: such parts are designated as Customer Self Replaceable ("**CSR**"). If during the troubleshooting and diagnosis, the Symantec technical support analyst determines that the repair can be accomplished with a CSR designated part, Symantec will ship the CSR designated part directly to You. CSR parts fall into two categories:

(A) **Optional CSR parts.** Optional CSR parts are designed for simple installation by You; however, depending on the type of service that was purchased with the Supported Product, Symantec may provide an onsite technician to replace the parts.

(B) **Mandatory CSR parts.** Mandatory CSR parts are designed for simple installation by You and Symantec does not provide installation labor services to install Mandatory CSR parts. If You request that Symantec and/or the Symantec Authorized Reseller replace these parts, You will be charged a fee for this service.

7. **HARDWARE WARRANTY SERVICE PREQUISITES. IN ORDER TO EXERCISE ANY OF THE WARRANTY RIGHTS CONTAINED IN THIS WARRANTY AGREEMENT, YOU MUST COMPLY WITH THE FOLLOWING PROCEDURES:**

(A) have available an original sales receipt or bill of sale demonstrating proof of purchase with Your warranty claim;

(B) separately procure and maintain during the entire Warranty Period, an active maintenance contract for the Licensed Software, as designated by Symantec and corresponding support ("Software Support and Maintenance");

(C) identify for Symantec the then current Geographic Use Location for the Hardware, in accordance with Symantec's requirements.

(D) Prepare for the Call. You must have the following information and materials ready when You call the technician: Your system's invoice and serial numbers; the then current Geographic Use Location service tag number for the Hardware; model and model numbers; the current version of the operating environment You are using; and the brand names and models of any peripheral devices (such as a mouse and/or keyboard) You are using.

(E) Call For Assistance. For warranty service and support call the support telephone numbers provided upon purchase of Your Software Support and Maintenance.

(F) Explain Your Problem to the Technician. Now You are ready to describe the problem You are having with Hardware. Let the technician know what error message You are getting and when it occurs; what You were doing when the error occurred; and what steps You may have already taken to solve the problem.

(G) Cooperate with the Technician. Experience shows that most system problems and errors can be corrected over the phone as a result of close cooperation between the user and the technician. Listen carefully to the technician and follow the technician's directions.

(H) Software/Data Backup. If the technician is unable to resolve the problem over the phone and determines that onsite support services as identified in Section 5, above, is necessary, the following standard procedure applies:

Software/Data Backup. You understand and agree that Symantec and its licensors are not responsible for any loss of software or data. You should back up the software and data on the hard disk drive of Your Hardware and on any other storage device(s) in the Hardware.

8. **HARDWARE WARRANTY SERVICE RESTRICTIONS/EXCLUSIONS.** The warranties contained in this Warranty Agreement will not apply to any Hardware which:

a) has been altered, supplemented, upgraded or modified in any way not authorized by Symantec;
b) has been repaired except by Symantec or its designee;

Additionally, the warranties contained in this Warranty Agreement do not apply to repair or replacement caused or necessitated by: (i) events occurring after risk of loss passes to You such as loss or damage during shipment; (ii) acts of God including without limitation natural acts such as fire, flood, wind earthquake, lightning, or similar disaster; (iii) improper use, environment, installation or electrical supply, improper maintenance, or any other misuse, abuse or mishandling (such as, but not limited to, use of incorrect line voltages, use of incorrect fuses, use of incompatible, defective, or inferior devices, supplies, or accessories, improper or insufficient ventilation, or failure to follow operating instructions) by anyone other than Symantec (or its representatives); (iv) governmental actions or inactions; (v) strikes or work stoppages; (vi) Your failure to follow applicable use or operations instructions or manuals; (vii) Your failure to implement, or to allow Symantec or its designee to implement, any corrections or modifications to the Hardware made available to You by Symantec; (viii) the moving of the Hardware from one Geographic Use Location to another or from one entity to another or (ix) such other events outside Symantec's reasonable control.

9. **WARRANTY DISCLAIMERS. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, AND EXCEPT TO THE EXTENT THIS WARRANTY DISCLAIMER CONFLICTS WITH ANY WARRANTIES EXPRESSLY STATED IN THE APPLICABLE GSA SCHEDULE, THE WARRANTIES SET FORTH IN SECTION 4 ARE YOUR EXCLUSIVE WARRANTIES AND ARE IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. SYMANTEC MAKES NO WARRANTIES OR REPRESENTATIONS THAT THE HARDWARE WILL MEET YOUR REQUIREMENTS OR THAT OPERATION OR USE OF THE HARDWARE WILL BE UNINTERRUPTED OR ERROR-FREE. YOU MAY HAVE OTHER WARRANTY RIGHTS, WHICH MAY VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.**

10. GENERAL

10.1. **COMPLIANCE WITH APPLICABLE LAW.** You are solely responsible for Your compliance with, and You agree to comply with, all applicable laws, rules, and regulations in connection with Your use of the Hardware.

10.2. **INTERNATIONAL COMMERCE TERMS (INCOTERMS):** Delivery of all items shall be in accordance with the Agreement.

Attachment 3
Business Critical Services

- **BUSINESS CRITICAL ADVANCED ACCESS**
- **BUSINESS CRITICAL NATIONAL PACKAGE**
- **BUSINESS CRITICAL SERVICES DATACENTER PACKAGE**
- **BUSINESS CRITICAL SERVICES REMOTE PRODUCT SPECIALIST**
- **BUSINESS CRITICAL SERVICES – CLEARED SUPPORT/VERIFIED SUPPORT**
- **Symantec DeepSight Early Warning Services Certificate - Silver, Gold, and Platinum Services**
- **Symantec DeepSight Early Warning Services Certificate - DeepSight Early Warning Services Starter Pack, DeepSight Early Warning Services Advanced Pack, DeepSight Early Warning Services Add-on to MSS and DeepSight DataFeeds Early Warning Services User Add-on Services**

Attachment 3
Business Critical Services

Where the terms of the following Business Critical Services Certificates issued separately to the Customer conflict with the terms of the Attachment 3 Certificates, the terms of the following Certificates shall control for each respective Business Critical Services support offering:

Business Critical Advanced Access

- **BCS-AA Offering:** Commencing on the issue date set forth on the face of this Certificate, Symantec will provide to Licensee BCS-AA for the Product Family/Families (as defined below) listed on the face of this Certificate, under the terms and conditions listed below, until the end date set forth on the face of the Certificate.

- **Product Family:** The following URL **www.symantec.com/techsupp/enterprise/bcs/bcsadvanced.html** lists, by Product Family, the underlying Symantec software products ("Software") eligible for coverage under BCS-AA. Licensee acknowledges that BCS-AA only applies to Software under the specific Product Family for which Licensee has purchased BCS-AA and that the list of Software may be revised and updated by Symantec from time to time without notice to Licensee. If additional Symantec software is added to the list of Software after the issue date set forth on the face of the Certificate, for the Product Family covered under this Certificate, no additional BCS-AA fee shall apply for BCS-AA coverage of such additional Software.

- **BCS-AA Services:** BCS-AA for each Product Family purchased by Licensee consists of the following services. Such services will be provided during each annual term for applicable Eligible Software: (i) priority call queuing; (ii) direct access to a Senior Symantec Technical Services Engineers for Severity 1 and Severity 2 Cases; (iii) access to the Business Critical Services website.; and (iv) unlimited number of Designated Contacts per Product Family. Delivery of BCS-AA services is in English.

- **Renewal Term; Fees for Renewal Term**. Unless otherwise terminated, Licensee's annual subscription for BCS-AA may be renewed for additional periods of twelve (12) months each (each, a "Renewal Term"), subject to general availability of BCS-AA on the applicable GSA price list and subject to Licensee's satisfaction of all requirements set forth in this Certificate. If Licensee purchases the Renewal Term through a Symantec authorized reseller, then the amount of fees for Licensee's Renewal Term and payment terms will be those fees and terms that are separately arranged between Licensee and such distributor/reseller.

II. **Prerequisites for BCS-AA:**

- **Required Maintenance/Support.** Licensee may only subscribe to receive BCS–AA (as defined in Section I above) during such time as Licensee has and maintains a valid support agreement for Essential Support for the Software. Designated Contacts shall be established in accordance with any then current Symantec policies. Additionally, Licensee is required to maintain consistency across all Software within a Product Family and may not exclude any individual Software product within a Software Family for coverage under this Certificate.

- **Payment**. Licensee's right to receive BCS-AA is subject to payment of applicable annual fees for both all required Essential Support and such BCS-AA. If Licensee's failure to pay the BCS-AA fees constitutes a material breach of the contract, then Symantec shall have the right to suspend or terminate the provision of BCS-AA for the Eligible Software. If Licensee's failure to pay for required Essential Support constitutes a material breach of the contract, then Symantec shall also have the right to suspend or terminate the provision of Essential Support for such unsupported Eligible Software, and in which case Symantec may also suspend or terminate BCS-AA for that Eligible Software. A material breach shall be deemed to occur if the Licensee fails to pay the contractually specified BCS-AA fees and/or Essential Support fees without justification for a period of sixty (60) days or more from the date when payment was due. If Licensee has a site license then Licensee is required to maintain Essential Support for all Software covered under a site license. The requirements in this Certificate to maintain and pay for Essential Support for the Eligible Software are separate from and do not change Licensee's obligation to maintain and pay for Essential Support for Software under any other agreement between Symantec and Licensee.

III. **Terms and Conditions:**

- **Limitations.** Notwithstanding anything to the contrary herein, Licensee shall have no right to sell, resell, outsource, or otherwise transfer the benefits of BCS-AA to any third party under any circumstances. Licensee shall not assign, delegate, or subcontract any of its rights or obligations under this Certificate absent Symantec's written consent, except to the extent expressly permitted under the License Agreement.

- **Termination**. Symantec may terminate Licensee's BCS-AA under this Certificate for Licensee's non-payment pursuant to Section II of this Certificate. Licensee's BCS-AA under this Certificate will also automatically terminate upon any termination of the License Agreement or any termination of required Essential Support pursuant to Section II of this Certificate. No refund will be due for any termination of BCS-AA under this Certificate. **Acknowledgement of Use of Personal Data**. Licensee recognizes that Symantec will require Licensee to supply certain personal data (such as business contact names, business telephone numbers, business e-mail addresses), in order for Symantec to provide BCS-AA and to keep Licensee apprised of support and product updates. Licensee acknowledges that Symantec is a global organization, and such personal data may be accessible on a global basis to enable Symantec to provide BCS-AA. By providing such personal data, Licensee consents to Symantec using, transferring and processing this personal data on a global basis for the purposes described **above.**

BUSINESS CRITICAL NATIONAL PACKAGE

I. **BCS-National Package:** Commencing on the issue date set forth on the face of this Certificate, Symantec will provide to Licensee BCS Services for the Eligible Software listed on the face of this Certificate installed in production environments in the national area designated by Licensee to Symantec in writing (each, a "Supported Datacenter"), for the period set forth on the face of this Certificate ("Term").

- **BCS Services.** BCS Services consist of the following services: (1) six (6) On-Site Visits per annual BCS term (an "On-Site Visit" means the provision of Symantec Maintenance/Support for a specific Severity 1 or Severity 2 Case that is performed on-site for Licensee's production environments at any Supported Datacenter; unused On-Site Visits cannot be carried over from one annual BCS term to another); (2) unlimited Designated Contacts; (3) priority call queuing; (4) direct access to senior Symantec Technical Services Engineers for Severity 1 and Severity 2 Cases; (5) Network Link Assessments performed once per quarter at Licensee's request (Network Link Assessments consist of diagnostics designed to measure end-to-end network performance of up to 200 nodes and seven servers on Licensee-selected network(s)); (6) Support Account Management (Licensee will be assigned a named Business Critical Account Manager (BCAM) whose function is to serve as Licensee's primary account contact for Licensee's Business Critical Services relationship); (7) Quarterly On-Site Case History and Account Reviews (a quarterly account review provided by the BCAM to Licensee that will be scheduled at a mutually convenient time and will take place at an HQ Datacenter designated by Licensee to Symantec in writing); and (8) if BCS Services are purchased for Licensed Security Software, Licensee will receive one seat of the Symantec DeepSight™ Threat Management System.
- **Eligible Software.** Eligible Software is the Symantec software eligible for coverage under Business Critical Services that are listed by type of product at the following URL: http://www.symantec.com/techsupp/enterprise/bcs/bcsdngspl.html. The list of Eligible Software may be revised and updated by Symantec from time to time without notice to Licensee. If, following the Issue Date of this Certificate, the list of Eligible Software is modified to add additional software of the same type(s) of product(s) as those for which the Licensee has paid current BCS fees, then this Certificate, including the prerequisites for BCS Services, shall automatically include such additional Eligible Software at a Supported Datacenter without the payment of additional BCS fees.
- **Renewal Term; Fees for Renewal Term**. Unless otherwise terminated, Licensee's annual subscription for BCS Services may be renewed for additional periods of twelve (12) months each (each, a "Renewal Term"), subject to general availability of BCS Services on the applicable GSA price list and subject to Licensee's satisfaction of all requirements set forth in this Certificate. In the event the Ordering Activity wishes to renew such BCS Services, the BCS fees charged to such Ordering Activity or to a Symantec authorized distributor/reseller, as applicable, for each twelve (12) month period of any Renewal Term, shall be the BCS fees for the immediately preceding twelve (12) month period ("Base BCS Fee") plus an increase not to exceed more than three percent (3%) over the Base BCS Fee. If Licensee purchases the Renewal Term through a Symantec authorized distributor/reseller, then the amount of fees for Licensee's Renewal Term and payment terms will be those fees and terms that are separately arranged between Licensee and such distributor/reseller.

II. **Prerequisites for BCS Services:**

- **Required License Agreement and Maintenance/Support.** Licensee must hold a valid license agreement ("License Agreement") for the underlying Eligible Software and have a current support agreement for Essential Support for the Eligible Software.
- **Payment**. Licensee's right to receive BCS Services is subject to payment of applicable annual fees for (i) all required Essential Support and (ii) such BCS Services. If Licensee's failure to pay the BCS fees constitutes a material breach of the contract, then Symantec shall have the right to suspend or terminate the provision of BCS for the Eligible Software. If Licensee's failure to pay for required Essential Support constitutes a material breach of the contract, then Symantec shall also have the right to suspend or terminate the provision of Essential Support for such unsupported Eligible Software, and in which case Symantec may also suspend or terminate BCS for that Eligible Software. A material breach shall be deemed to occur if the Licensee fails to pay the contractually specified BCS fees or Essential Support fees without justification for a period of sixty (60) days or more from the date when payment was due. If Licensee has a site license then Licensee is required to maintain Essential Support for all Software covered under a site license.

III. **Terms and Conditions:**

- **Limitations.** Licensee shall have no right to sell, resell, outsource, or otherwise transfer the benefits of BCS Services to any third party under any circumstances. Licensee shall not assign, delegate, subcontract any of its rights or obligations under this Certificate absent Symantec's written consent, except to the extent expressly permitted under the License Agreement.
- **DeepSight™ Terms and Conditions**. As a condition of purchase, Licensee understands and agrees that for Security Software Licensee shall receive the DeepSight™ Threat Management System in accordance with the DeepSight™ Alert Services and TMS Certificate terms and conditions ("DeepSight Certificate"). Licensee's purchase of Essential Support shall satisfy all requirements for technical support and maintenance set forth in the DeepSight Certificate. Licensee may contact its BCAM for DeepSight™ Threat Management System technical support issues. In the event of a conflict between this Certificate and the DeepSight Certificate, this Certificate shall control. The Deepsight Certificate is attached hereto.
- **Termination**. Licensee's BCS Services may be terminated (i) by Symantec for Licensee's non-payment of applicable fees in accordance with Section II of this Certificate; or (ii) automatically upon any termination of the License Agreement or any termination of required Essential Support in accordance with Section II of this Certificate. No refund will be due for any termination of BCS Services.
- **Acknowledgement of Use of Personal Data**. Licensee recognizes that Symantec will require Licensee to supply certain personal data (such as business contact names, business telephone numbers, business e-mail addresses), in order for Symantec to provide BCS Services and to keep Licensee apprised of support and product updates. Licensee acknowledges that Symantec is a global organization, and such personal data may be accessible on a global basis to enable Symantec to provide BCS Services. By providing such personal data, Licensee consents to Symantec using, transferring and processing this personal data on a global basis for the purposes described above.

BUSINESS CRITICAL SERVICES DATACENTER PACKAGE

BCS-DataCenter Package: Commencing on the issue date set forth on the face of this Certificate, Symantec will provide to Licensee BCS Services for the Eligible Software listed on the face of this Certificate installed in production environments at one (1) single Licensee location designated by Licensee to Symantec in writing ("Supported Datacenter"), for the period set forth on the face of the Certificate ("Term").

- **BCS Services.** BCS Services consist of the following services: (1) two (2) On-Site Visits per annual BCS term (an "On-Site Visit" means the provision of Symantec Maintenance/Support for a specific Severity 1 Case that is performed on-site for Licensee's production environments at the Supported Datacenter; unused On-Site Visits cannot be carried over from one annual BCS term to another); (2) unlimited Designated Contacts; (3) priority call queuing; (4) direct access to senior Symantec Technical Services Engineers for Severity 1 Cases; (5) Support Account Management (Licensee will be assigned a named Business Critical Account Manager (BCAM) whose function is to serve as Licensee's primary account contact for Licensee's Business Critical Services relationship); (6) Semiannual On-Site Case History and Account Reviews (a semiannual account review provided by the BCAM to Customer that will be scheduled at a mutually convenient time and will take place at Customer's Supported Datacenter); and (7) if BCS Services are purchased for Licensed Security Software, Licensee will receive one seat of the Symantec DeepSight™ Threat Management System.

- **Eligible Software.** Eligible Software is the Symantec software eligible for coverage under Business Critical Services that are listed by type of product at the following URL: http://www.symantec.com/techsupp/enterprise/bcs/bcsdngspl.html. The list of Eligible Software may be revised and updated by Symantec from time to time without notice to Licensee. If, following the Issue Date of this Certificate, the list of Eligible Software is modified to add additional software of the same type(s) of product(s) as those for which the Licensee has paid current BCS fees, then this Certificate, including the prerequisites for BCS Services, shall automatically include such additional Eligible Software at a Supported Datacenter without the payment of additional BCS fees.
- **Renewal Term; Fees for Renewal Term**. Unless otherwise terminated, Licensee's annual subscription for BCS Services may be renewed for additional periods of twelve (12) months each (each, a "Renewal Term"), subject to general availability of BCS Services on the applicable GSA price list and subject to Licensee's satisfaction of all requirements set forth in this Certificate. In the event the Ordering Activity wishes to renew such BCS Services, the BCS fees charged to such Ordering Activity or to a Symantec authorized distributor/reseller, as applicable, for each twelve (12) month period of any Renewal Term, shall be the BCS fees for the immediately preceding twelve (12) month period ("Base BCS Fee") plus an increase not to exceed more than three percent (3%) over the Base BCS Fee. If Licensee purchases the Renewal Term through a Symantec authorized distributor/reseller, then the amount of fees for Licensee's Renewal Term and payment terms will be those fees and terms that are separately arranged between Licensee and such distributor/reseller.

II. **Prerequisites for BCS Services:**

- **Required License Agreement and Maintenance/Support.** Licensee must hold a valid license agreement ("License Agreement") for the underlying Eligible Software and have a current support agreement for Essential Support for the Eligible Software.

- **Payment**. Licensee's right to receive BCS Services is subject to payment of applicable annual fees for (i) all required Essential Support and (ii) such BCS Services. . If Licensee's failure to pay the BCS fees constitutes a material breach of the contract, then Symantec shall have the right to suspend or terminate the provision of BCS for the Eligible Software. If Licensee's failure to pay for required Essential Support constitutes a material breach of the contract, then Symantec shall also have the right to suspend or terminate the provision of Essential Support for such unsupported Eligible Software, and in which case Symantec may also suspend or terminate BCS for that Eligible Software. A material breach shall be deemed to occur if the Licensee fails to pay the contractually specified BCS fees and/or Essential Support fees without justification for a period of sixty (60) days or more from the date payment was due. If Licensee has a site license then Licensee is required to maintain Essential Support for all Software covered under a site license.

III. **Terms and Conditions:**

- **Limitations.** Licensee shall have no right to sell, resell, outsource, or otherwise transfer the benefits of BCS Services to any third party under any circumstances. Licensee shall not assign, delegate, subcontract any of its rights or obligations under this Certificate absent Symantec's written consent, except to the extent expressly permitted under the License Agreement.

- **DeepSight™ Terms and Conditions**. As a condition of purchase, Licensee understands and agrees that for Security Software Licensee shall receive the DeepSight™ Threat Management System in accordance with the DeepSight™ Alert Services and TMS Certificate terms and conditions ("DeepSight Certificate"). Licensee's purchase of Essential Support shall satisfy all requirements for technical support and maintenance set forth in the DeepSight Certificate. Licensee may contact its BCAM for DeepSight™ Threat Management System technical support issues. In the event of a conflict between this Certificate and the DeepSight Certificate, this Certificate shall control. The Deepsight Certificate is attached hereto.

- **Termination**. Licensee's BCS Services may be terminated (i) by Symantec for Licensee's non-payment of applicable fees in accordance with Section II of this Certificate ; or (ii) automatically upon any termination of the License Agreement or any termination of required Essential Support in accordance with Section II of this Certificate. No refund will be due for any termination of BCS Services

- **Acknowledgement of Use of Personal Data**. Licensee recognizes that Symantec will require Licensee to supply certain personal data (such as business contact names, business telephone numbers, business e-mail addresses), in order for Symantec to provide BCS Services and to keep Licensee apprised of support and product updates. Licensee acknowledges that Symantec is a global organization, and such personal data may be accessible on a global basis to enable Symantec to provide BCS Services. By providing such personal data, Licensee consents to Symantec using, transferring and processing this personal data on a global basis for the purposes described above.

BUSINESS CRITICAL SERVICES REMOTE PRODUCT SPECIALIST

I. **BCS-RPS Offering**

Commencing on the issue date set forth on the face of this Certificate, Symantec will provide to Licensee BCS-RPS for the Product Family/Families (as defined below) listed on the face of this Certificate, under the terms and conditions listed below, until the end date set forth on the face of the Certificate.

- **Product Family**: The following URL www.symantec.com/techsupp/enterprise/bcs/bcsrpsspl.html lists, by Product Family, the Software eligible for coverage under BCS-RPS. Licensee acknowledges that BCS-RPS only apply to Software under the specific Product Family for which Licensee has purchased BCS-RPS and that the list of Software may be revised and updated by Symantec from time to time without notice to Licensee. If additional Symantec software is added to the list of Software after the issue date set forth on the face of the Certificate, no additional BCS-RPS fee shall apply for BCS-RPS coverage of such additional Software provided that Licensee has purchased BCS-RPS for the relevant Product Family.
- **BCS-RPS Services**: BCS-RPS for each Product Family purchased by Licensee consists of the following services. Such services will be provided during each annual term for applicable Software: (i) six (6) Designated Contacts per Product Family; (ii) Priority Call Queuing; (iii) Access to a Shared or Dedicated Remote Product Specialist, as such terms are defined at www.symantec.com/business/support/bcs/bcsdesc.html during regional business hours. All calls will be directed to an advanced team outside of regional business hours or in the event the Remote Product Specialist is not available; and (iv) DeepSight™ Alert Services. If BCS-RPS is purchased for a Product Family consisting of Symantec security products, Licensee will receive one seat of Symantec DeepSight™ Alert Services and one add-on Delivery Method.
- **Renewal Term; Fees for Renewal Term**. Unless otherwise terminated, Licensee's annual subscription for BCS-RPS may be renewed for additional periods of twelve (12) months each (each, a "Renewal Term"), subject to general availability of BCS-RPS on the applicable GSA price list and subject to Licensee's payment of the applicable BCS-RPS fees as well as payment of the annual fees for required Essential Support. If Licensee purchases the Renewal Term through a Symantec authorized reseller, then the amount of fees for Licensee's Renewal Term and payment terms will be those fees and terms that are separately arranged between Licensee and such reseller.

II. **Prerequisites for BCS-RPS:**

- **Required Maintenance/Support**. Licensee may only subscribe to receive BCS–RPS (as defined in Section I above) during such time as Licensee has and maintains a valid support agreement for Essential Support for the Software. BCS-RPS is only applicable to Software installed in production environments.
- **Payment**. Licensee's right to receive BCS-RPS is subject to payment of applicable annual fees for both all required Essential Support and such BCS-RPS. If Licensee's failure to pay the BCS fees constitutes a material breach of the contract, then Symantec shall have the right to suspend or terminate the provision of BCS-RPS for the Eligible Software. If Licensee's failure to pay for required Essential Support constitutes a material breach of the contract, then Symantec shall also have the right to suspend or terminate the provision of Essential Support for such unsupported Eligible Software, and in which case Symantec may also suspend or terminate BCS-RPS for that Eligible Software. A material breach shall be deemed to occur if the Licensee fails to pay the contractually specified BCS fees and/or Essential Support fees without justification for a period of sixty (60) days or more from the date payment was due. If Licensee has a site license then Licensee is required to maintain Essential Support for all Software covered under a site license. The requirements in this Certificate to maintain and pay for Essential Support for the Software are separate from and do not change Licensee's obligation to maintain and pay for Essential Support for Software under any other agreement between Symantec and Licensee.

III. **Terms and Conditions:**

- **DeepSight™ Terms and Conditions**. As a condition of purchase, Licensee understands and agrees that Licensee shall receive the DeepSight™ Alert Services in accordance with the DeepSight™ Alert Services and TMS Certificate terms and conditions ("DeepSight Certificate"). Licensee's purchase of Required Maintenance/Support (as defined below) shall satisfy all requirements for technical support and maintenance set forth in the DeepSight Certificate. Licensee may contact its Remote Product Specialist for DeepSight™ Alert Services technical support issues. In the event of a conflict between this Certificate and the DeepSight Certificate, this Certificate shall control. The Deepsight Certificate is attached hereto.
- **Designated Contacts**: Any Designated Contact may call Symantec for assistance; provided that Designated Contacts can only request BCS-RPS for Software. Designated Contacts shall have a thorough understanding of the Software for which they are the named contact(s). Symantec reserves the right to request replacement of any Designated Contact if Symantec reasonably deems that such Designated Contact lacks the necessary technical and product knowledge to assist Symantec with the timely resolution of a Licensee problem. Licensee will use its best efforts to designate a replacement Designated Contact with appropriate technical and product knowledge as soon as is reasonably practicable. Licensee recognizes that the lack of suitably-qualified Designated Contacts may affect Symantec's ability to provide the BCS-RPS hereunder.
- **Limitations**. Notwithstanding anything to the contrary herein, Licensee shall have no right to sell, resell, outsource, or otherwise transfer the benefits of BCS-RPS to any third party under any circumstances. Licensee shall not assign, delegate, subcontract any of its rights or obligations under this Certificate absent Symantec's written consent, except to the extent expressly permitted under the License Agreement.
- **Termination**. Symantec may terminate Licensee's BCS-RPS under this Certificate for Licensee's non-payment pursuant to Section II of this Certificate. Licensee's BCS-RPS under this Certificate will also automatically terminate upon any termination of the License Agreement or any termination of required Essential Support in accordance with Section II. Except as otherwise provided herein, no refund will be due for any termination of BCS-RPS under this Certificate.

- **Acknowledgement of Use of Personal Data**. Licensee recognizes that Symantec will require Licensee to supply certain personal data (such as business contact names, business telephone numbers, business e-mail addresses), in order for Symantec to provide BCS-RPS and to keep Licensee apprised of support and product updates. Licensee acknowledges that Symantec is a global organization, and such personal data may be accessible on a global basis to enable Symantec to provide BCS-RPS. By providing such personal data, Licensee consents to Symantec using, transferring and processing this personal data on a global basis for the purposes described above.

Symantec Business Critical Services – Cleared Support Services
Verified Support

I. **CSS-VS Services:** Commencing on the issue date set forth on the face of this Certificate, Symantec will provide to Licensee CSS-VS Services for the Supported Products (as defined below), listed on the face of this Certificate, for the period set forth on the face of this Certificate ("Term").

- **CSS-VS Services.** CSS-VS Services shall mean: (i) support services consisting of initial verification of Licensee' entitlement and subsequent remote diagnostic and troubleshooting performed only by United States citizens in the fifty (50) states of the United States and (ii) performed at up to a total of three (3) Supported Data Centers as designated in writing by Licensee to Symantec.
- **Supported Products.** The following URL http://www.symantec.com/techsupp/enterprise/bcs/bcsclearedss.html lists, the Supported Products, for which CSS-VS Services are provided under this Certificate, subject to purchase by Licensee of Essential Support for each Product Title designated by Licensee to be covered hereunder. Licensee acknowledges that the list of Supported Products may be revised and updated by Symantec from time to time without notice to Licensee.
- **Renewal Term; Fees for Renewal Term.** Unless otherwise terminated, upon request, Licensee's annual subscription for CSS-VS Services may be renewed for additional periods of twelve (12) months each (each, a "Renewal Term"), subject to general availability of CSS-VS Services on the applicable GSA price list and subject to Licensee's satisfaction of all requirements set forth in this Certificate. In the event the Ordering Activity wishes to renew such CSS-VS Services, the CSS-VS fees charged to such Ordering Activity or to a Symantec authorized distributor/reseller, as applicable, for each twelve (12) month period of any Renewal Term, shall be the BCS fees for the immediately preceding twelve (12) month period ("Base CSS-VS Services Fee") plus an increase not to exceed more than three percent (3%) over the Base CSS-VS Services Fee. If Licensee purchases the Renewal Term through a Symantec authorized distributor/reseller, then the amount of fees for Licensee's Renewal Term and payment terms will be those fees and terms that are separately arranged between Licensee and such distributor/reseller.

II. Prerequisites for CSS-VS Services:

- **Required License Agreement and Maintenance/Support.** Licensee must hold a valid license agreement ("License Agreement") for the underlying Software Product Title and have a current support agreement for Essential Support for each Software Product Title. Designated Contacts for CSS-VS Services shall be those same Designated Contacts established in connection with Essential Support for each Product Title designated by Licensee for coverage hereunder.
- **Payment.** Licensee's right to receive CSS-VS Services is subject to payment of applicable annual fees for (i) all required Essential Support and (ii) CSS-VS Services. If Licensee's failure to pay the BCS fees constitutes a material breach of the contract, then Symantec shall have the right to suspend or terminate the provision of CSS-VS for the Supported Products. If Licensee's failure to pay for required Essential Support constitutes a material breach of the contract, then Symantec shall also have the right to suspend or terminate the provision of Essential Support for such unsupported Product Titles, and in which case Symantec may also suspend or terminate CSS-VS for such Suport Products. A material breach shall be deemed to occur if the Licensee fails to pay the contractually specified BCS fees and/or Essential Support fees without justification for a period of sixty (60) days or more from the date payment was due.

III. Terms and Conditions:

- **Limitations.** Licensee shall have no right to sell, resell, outsource, or otherwise transfer the benefits of CSS-VS Services to any third party under any circumstances. Licensee shall not assign, delegate, or subcontract any of its rights or obligations under this Certificate absent Symantec's written consent, except to the extent expressly permitted under the License Agreement.
- **Termination.** Licensee's CSS-VS Services may be terminated (i) by Symantec for Licensee's non-payment of applicable fees in accordance with Section II; or (ii) automatically upon any termination of the License Agreement or any termination of required Essential Support in accordance with Section II. No refund will be due for any termination of CSS-VS Services.
- **Acknowledgement of Use of Personal Data.** Licensee recognizes that Symantec will require Licensee to supply certain personal data (such as business contact names, business telephone numbers, business e-mail addresses), in order for Symantec to provide CSS-VS Services and to keep Licensee apprised of support and product updates. Licensee acknowledges that Symantec is a global organization, and such personal data may be accessible on a global basis to enable Symantec to provide CSS-VS Services. If and by providing such personal data, Licensee consents to Symantec using, transferring and processing this personal data on a global basis for the purposes described above.

Symantec DeepSight Early Warning Services Certificate
Silver, Gold, and Platinum Services

1. DEFINITIONS. "**Administrative Users**"**:** means employees or third party contractors designated to use and access the Services (as further described in Section 3 below), as are identified upon Registration or thereafter via the DeepSight Website. Administrative Users may additionally designate Designated Users via the DeepSight Website and contact Support (as such term is defined in Section 5 below). In the event of a conflict, those Administrative Users identified via the DeepSight Website will control over Administrative Users identified at the time of Registration. Administrative Users may be modified to reflect personnel changes, provided that the total number of Administrative Users does not exceed five (5) Administrative Users per Services entitlement purchased. "**Alert Information**"**:** means the alert messages, data and/or information that Symantec provides or makes available to Authorized Users pursuant to the Services. "**Authorized Users**": means both Administrative Users and Designated Users. "**DeepSight Website**"**:** means Symantec's password-protected Early Warning Services TMS website, currently located at TMS.symatnec.com, including any Symantec subsites accessible via the DeepSight Website, and all content accessible on such sites. **Delivery Medium(s)**"**:** means the manner by which, and / or location where, Symantec will send the Alert Information. Each Authorized User may designate one of the following Delivery Medium(s) during Registration through the DeepSight Website for each of the Services purchased: email address(es), and/or RSS, and/or short message service (SMS) device number(s) that belong to Authorized Users, as specified through the DeepSight Website. Authorized Users of the Gold Services and Platinum Services may designate the XML Delivery Location option. "**Designated Users**"**:** means employees or third party contractors (excluding Administrative Users) designated by Administrative Users to access and use the Services, provided such number of Designated Users does not exceed the cumulative number of persons employed by or contracted to perform on Licensee's behalf or on behalf of Ordering Activity (as applicable). Designated Users do not have authorization to designate, add, change, or remove other Designated Users, or to access Support. "**Reports**"**:** means the reports that Symantec provides or makes available with the Services. Administrative Users of the Gold Services and Platinum Services may select and receive custom Reports, as may be available through the DeepSight Website. "**Symantec Material(s)**"**:** means the materials provided in connection with the Services, including but not limited to the Alert Information, Reports, but not including any third party websites, or content thereon, that may be reached from any link contained in any such materials.

2. REGISTRATION; SERVICES. Licensee or Ordering Activity (as applicable) must first register the serial number(s) printed on the initial page of this Certificate in the Symantec licensing portal located at https://licensing.symantec.com and designate the Administrative User(s) associated with the Services ("**Registration**"). Symantec will use commercially reasonable efforts to provide the Services in accordance with the terms and conditions set forth herein. Each of the Services will commence upon the earlier of: (i) the issue date set forth on the front of this Certificate; or (ii) the date(s) the Service(s) are registered, and will continue through the end date(s) ("**End Date**") set forth on the front of the Certificate ("**Service Period**"). Any delay in Registration may delay the start date of Services, and Symantec will not be liable for any such delay arising out of any failure to register the Services. Services will expire upon the expiration of the Service Period, even if Licensee or Ordering Activity (as applicable) do not complete Registration during the Service Period. Platinum Services include access to a Remote Expert Analyst **("REA")**, whom Administrative Users may contact for (a) incident research, (b) assistance with reporting content and context, and for (c) guidance on threat remediation. Access to the REA is limited to no more than fifteen (15) hours per calendar month, and availability of REAs are between the hours of 9am-5pm USA Eastern Time (UTC−05:00). REAs are located in the USA and are limited to assisting with no more than one (1) request for assistance with the REA at any one time; additional requests for assistance will not be addressed until the final resolution of the prior request.

3. LICENSE GRANT. Symantec grants to Licensee and/or Ordering Activity (as applicable) the following non-exclusive, non-transferable, limited license rights, which may be exercised solely for the internal business operations of Licensee and/or Ordering Activity (as applicable). Licensee warrants and represents that the quantity of Services purchased , as identified on the front of this Certificate, reflects the total number of Nodes owned or used by Licensee and / or Ordering Activity (as applicable) at the time of purchase, regardless of whether each such Node directly interacts with the Services ("**Node Count**"). Each "**Node**" is a virtual or physical unique network address, such as an Internet protocol Address. If, during the Service Period, Licensee and / or Ordering Activity's (as the case may be) applicable Node Count increases by more than five percent (5%) over the Node Count associated with the Services purchased, then Licensee or Ordering Activity agree to promptly, but no later than thirty (30) days following the increase in Node Count, purchase additional Services entitlements to become compliant with such expanded Node Count. In addition to the audit rights set forth below, Symantec may, at its discretion, but no more than once every twelve (12) months, request Licensee or Ordering Activity to validate (as applicable) the Node Count to Symantec in writing. Authorized Users may use the Symantec Materials and may access the DeepSight Website; Authorized Users may distribute content from the Symantec Materials within its internal organization for internal use only, provided that the number of recipients does not exceed the number of Authorized Users associated with the level of Services purchased (as identified on the front of this Certificate), and subject to the confidentiality terms contained herein. Licensee or Ordering Activity will ensure that use of the Symantec Materials by Authorized Users (including third party contractors) is in accordance with this Certificate.

4. TECHNICAL SUPPORT. Symantec will provide Maintenance/Support Services in accordance with Section 6 of the Agreement.

5. PRIVACY AND DATA PROTECTION. For the purpose of providing Services pursuant to this Certificate, Symantec will require Licensee or Ordering Activity to supply certain personal information (such as business contact names, business telephone numbers, business e-mail addresses). Licensee and/or Ordering Activity acknowledge that Symantec is a global organization, and such personal information may be accessible on a global basis by Symantec affiliates, by Symantec partners and subcontractors, including in countries that may have less protective data protection laws than the country in which Licensee and/or Ordering Activity are located. By providing such personal information, Licensee and/or Ordering Activity consent to Symantec using, transferring and processing this information on a global basis for the use described above. For any question regarding the use of personal information, Licensee or Ordering Activity may contact Symantec Corporation - Privacy Lead, 350 Ellis Street, PO Box 7011, Mountain View, CA 94043, U.S.A. Telephone 650-527-8000 Email: privacy@symantec.com.

6. MISCELLANEOUS. Symantec reserves the right to make changes to the Services, including but not limited to the content and/or format of the Symantec Materials, without notification. However, if, in Symantec's reasonable discretion such modifications would materially degrade the Symantec Materials or the Services, then Symantec agrees to use commercially reasonable efforts to provide Licensee and / or Ordering Activity (as applicable) thirty (30) days' advance notice of such changes. Licensee and/or Ordering Activity are solely responsible for acquiring and maintaining the Internet or telecommunications services and devices required for Administrative Users to receive, access and/or use the Services and / or Symantec Materials. Symantec will not be liable for any downtime of the DeepSight Website, or subsites due to reasonable scheduled maintenance, maintenance for critical issues or forces beyond the reasonable control of Symantec.

Symantec DeepSight Early Warning Services Certificate
DeepSight Early Warning Services Starter Pack, DeepSight Early Warning Services Advanced Pack, DeepSight Early Warning Services Add-on to MSS and DeepSight DataFeeds Early Warning Services User Add-on Services

1. DEFINITIONS. "**Administrative User(s)**"**:** means the permitted number of employees or third party contractors designated to use and access the Services (as further described in Section 3 below), as are identified upon Registration or thereafter, via the DeepSight Website. Administrative User(s) identified via the DeepSight Website will control over Administrative User(s) identified at the time of Registration. Administrative User(s) may be modified to reflect personnel changes, provided that the total number does not exceed the permitted number of Administrative User(s) permitted for the Service purchased (as further described in Section 3 below). "**Alert Information**"**:** means the alert messages, data and/or information that Symantec provides or makes available to Administrative User(s). **"Alert Website"** means Symantec's password-protected alerts website currently located at alerts.symantec.com, including any Symantec subsites accessible via the Alert Website, and all content accessible on such sites. **"DeepSight Website":** means either the Alert Website or the TMS Website, as applicable to the Service purchased. "**Delivery Medium(s)**"**:** means the manner by which, and / or location where, Symantec will send the Alert Information. Either of the following Delivery Medium(s) may be identified during Registration through the DeepSight Website applicable to the Service purchased for each permitted Administrative User(s): email address(es) or RSS. "**Reports**"**:** means the reports that Symantec provides or makes available with each Service purchased. "**Symantec Material(s)**"**:** means the materials provided in connection with each Service purchased, including but not limited to the Alert Information, Reports, but not including any third party websites, or content thereon, that may be reached from any link contained in any such materials. **"TMS Website":** means Symantec's password-protected threat management website currently located at TMS.symantec.com, including any Symantec subsites accessible via the TMS Website, and all content accessible on such sites.

2. REGISTRATION; SERVICES. Licensee or Ordering Activity (as applicable) must first register the serial number(s) printed on the initial page of this Certificate in the Symantec licensing portal located at https://licensing.symantec.com and designate the Administrative User(s) associated with the Services ("**Registration**"). Symantec will use commercially reasonable efforts to provide the Services in accordance with the terms and conditions set forth herein. Each Service will commence upon the earlier of: (i) the issue date(s) set forth on the front of this Certificate; or (ii) the date(s) the Service(s) are registered, and will continue through the end date(s) ("**End Date**") set forth on the front of the Certificate ("**Service Period**"). Any delay in Registration may delay the start date of the Services, and that Symantec will not be liable for any such delay arising out of any failure to register the Service. Services will expire upon the expiration of the Service Period, even if Licensee or Ordering Activity (as applicable) do not complete Registration during the Service Period. .

3. LICENSE GRANT; ADMINISTRATIVE USER(S); DEEPSIGHT WEBSITE. Symantec grants to Licensee and/or Ordering Activity (as applicable) the following non-exclusive, non-transferable, limited license rights, which may be exercised by the permitted number of Administrative User(s) for each applicable Service (as further described below), solely for the internal business operations of Licensee and/or Ordering Acvitity (as applicable). For the Core Services, the permitted number of Administrative User(s) shall be two (2). For DSAD Services, the permitted number of Administrative User(s) shall be one (1). Administrative User(s) of Starter Services and DSAM Services will have access to the Alert Website only. Administrative User(s) of Advanced Services and DSAD Services will have access to the TMS Website only. Administrative User(s) may use the Symantec Materials and may access the DeepSight Website associated with Services purchase, but may not distribute content from the Symantec Materials other than to quote or use sentences or paragraphs of the Symantec Materials (not to exceed two (2) contiguous paragraphs) solely for internal communications. Use of the Symantec Materials by Administrative User(s) must be in accordance with this Certificate at all times.

4. TECHNICAL SUPPORT. Symantec will provide technical support services in accordance with Section 6 of the Agreement.

5. PRIVACY AND DATA PROTECTION. For the purpose of providing Services pursuant to this Certificate, Symantec will require Licensee and/or Ordering Activity to supply certain personal information (such as business contact names, business telephone numbers, business e-mail addresses). Licensee and/or Ordering Activity acknowledge that Symantec is a global organization, and such personal information may be accessible on a global basis by Symantec's affiliates, Symantec partners and subcontractors, including in countries that may have less protective data protection laws than the country in which Licensee and/or Ordering Activity are located. By providing such personal information, Licensee and/or Ordering Activity consent, to Symantec using, transferring and processing this information on a global basis for the use described above. For any question regarding the use of personal information, Licensee or Ordering Activity may contact Symantec Corporation - Privacy Lead, 350 Ellis Street, PO Box 7011, Mountain View, CA 94043, U.S.A. Telephone 650-527-8000 Email: privacy@symantec.com.

6. MISCELLANEOUS. Symantec reserves the right to make changes to the Services, including but not limited to the content and/or format of the Symantec Materials, without notification. However, if, in Symantec's reasonable discretion such modifications would materially degrade the Symantec Materials or the Services, then Symantec agrees to use commercially reasonable efforts to provide Licensee and/or Ordering Activity with thirty (30) days' advance notice of such changes. Licensee and/or Ordering Activity are solely responsible for acquiring and maintaining the Internet or telecommunications services and devices required for Administrative User(s) to receive, access and/or use the Services purchased and / or associated Symantec Materials. Symantec will not be liable for any downtime of the DeepSight Website, or subsites due to reasonable scheduled maintenance, maintenance for critical issues or forces beyond the reasonable control of Symantec.

Attachment 4
Managed Security Services

- **Managed Security Services Certificate (“Certificate”) - Enterprise Wide**
- **Managed Security Services Certificate (“Certificate”) - Per Unit**
- **Managed Security Services Attributes Document**

Attachment 4
Managed Security Services

Managed Security Services Certificate ("Certificate") - Enterprise Wide

Where the terms of a Managed Security Services Certificate – Enterprise Wide – issued separately to the Customer conflict with the terms of these Attachment 4 Certificates, the terms of this Attachment 4 Certificate shall control:

1. AGREEMENT TERMS; SUPPORT ENTERPRISE WIDE USE. The term **"Agreement"** shall mean, collectively, the Master License Agreement, this Certificate, the MSS service attributes document found at www.symantec.com/docs/TECH131855 containing general terms and conditions, Service(s) description(s), and service level warranties ("**SLWs**") applicable to the Service(s) ("**MSS Service Attributes**"), and the Managed Security Services Operations Manual ("**Ops Manual**") available on the Secure Internet Interface ("**SII**"), all of which are incorporated herein by reference, in that order of precedence . Service(s) are subject to the terms of the Agreement.. The MSS Attributes and Ops Manual may be revised and updated by Symantec from time to time. Symantec will use commercially reasonable efforts to notify Customer of such revisions and updates by posting a revised version of the MSS Service Attributes at the URL referenced above and a revised Ops Manual on the SII. For the avoidance of doubt, revisions and updates to the MSS Service Attributes and Ops Manual will not materially degrade the Service(s). Technical assistance for the Service(s) will be provided by the Security Operations Center ("**SOC**") as described in the Ops Manual. Any capitalized terms not defined herein shall have the meaning set forth in the MSS Services Attributes and the Ops Manual, as applicable. Use of the Service(s) will be limited to the Enterprise Wide Model, as described in the MSS Services Attributes.

2. TERM; POINTS OF CONTACT; DEVICE REGISTRATION; TERMINATION. The term of Service(s) ("**Term**") will begin on the Start Date specified on the initial page(s) of this Certificate ("**Start Date**") and end on the End Date specified on the initial page(s) of this Certificate ("**End Date**"). Service(s) are non-cancellable, non-refundable and are available to Customer immediately upon the Start Date, however, Customer acknowledges and agrees that to access the Service(s), Customer must first register the serial number(s) printed on the initial page(s) of this Certificate in the Symantec licensing portal located at https://licensing.symantec.com and designate its authorized points of contact for the Service(s) ("**POC(s)**"). Upon serial number registration, Customer will be given access to the SII and SOC technical staff. Customer must provide all technical and license information for each firewall, server, intrusion detection device, or other hardware or software (each, a "**Device**") reasonably requested by Symantec, prior to such Device being recognized by the Service(s) and connected to the SOC ("**Device Registration**"). Customer acknowledges and agrees that the Term will expire upon the End Date, even if no Devices undergo Device Registration or receive Service(s) during the Term.

Except as otherwise stated in Section (iii) below, Customer acknowledges and agrees that the Service(s) (or a portion thereof) may be terminated by: (a) either Party upon written notice if the other Party breaches any material term of the MSS Terms & Conditions (including failure to meet the Customer Responsibilities), and such breach remains uncorrected for thirty (30) days following such notice, or (b) by Symantec for convenience upon thirty (30) days prior written notice to the Customer or Ordering Activity, or (c) by the Customer or Ordering Activity in accordance with the applicable GSA Schedule contract. In the event that Symantec exercises its termination rights under (b), Symantec will credit Customer's account any prorated, unused fees received by Symantec for the applicable Service(s) terminated hereunder.

i. In the event that Customer exercises its termination rights under the above paragraph, Customer acknowledges and agrees that in order to terminate the Service(s) (or a portion thereof), Customer must submit a duly authorized termination letter ("**Termination Letter**") in accordance with the terms of the applicable GSA Schedule

ii. If Customer terminates the MSS Terms & Conditions and/or the Service(s) (or a portion thereof) prior to the end of the Term as described in the foregoing two paragraphs, Customer agrees to pay Symantec, or Customer's designated reseller (as applicable) a termination fee ("Termination Fee") equal to (a) if terminated in the first year of the Service, fifty percent (50%) of the amount of remaining fees that would have been due and payable to Symantec had the Service(s) been performed for the entire Term; or (b) if terminated in the second or third year of the Service, twenty-five percent (25%) of the amount of remaining fees that would have been due and payable to Symantec had the Service(s) been performed for the entire Term. . If Service(s) have been prepaid for the Term, Symantec will credit Customer's account any prorated, unused fees received by Symantec for the applicable Service(s) terminated hereunder less the calculated Termination Fee. Pursuant to FAR 52.212-(I), the Termination Fee in this paragraph shall satisfy and be deemed to represent the "reasonable termination costs" which shall be due and payable by the government in addition to the fees due and payable for the Services provided up to the date of termination.

iii. Notwithstanding anything contained in Sections (i)-(iii) above, Customer acknowledges and agrees that those Services identified as "Enterprise Wide" in the Certificate cannot be partially terminated. Any termination of Service(s) identified in the Certificate as "Enterprise Wide" must apply to the entire quantity of Enterprise Wide Service(s) purchased under the Certificate.

3. PRIVACY AND DATA PROTECTION. For the purpose of providing Service(s) to Customer pursuant to the Agreement, Symantec will require Customer to supply certain personal information (such as business contact names, business telephone numbers, business e-mail addresses). Customer acknowledges that Symantec is a global organization, and such personal information may be accessible on a global basis by Symantec affiliates, by Symantec partners and subcontractors, including in countries that may have less protective data protection laws than the country in which Customer is located. By providing such personal information, Customer consents to Symantec using, transferring and processing this information on a global basis for the use described above. For any question regarding the use of personal information, Customer may contact Symantec Corporation - Privacy Lead, 350 Ellis Street, PO Box 7011, Mountain View, CA 94043, U.S.A. Telephone 650-527-8000 Email: privacy@symantec.com.

4. USE OF INFORMATION POLICY. Symantec may use certain information derived from the Service(s), once anonymized ("**Anonymized Information**") for the following purposes: (a) preparing and distributing statistical reports related to security trends and data patterns; (b) distributing Anonymized Information to Symantec customers, in compiled or original formats, for the purposes of providing computer security information; and / or (c) analysis; internal research, product or services development, or for providing general security related services. Anonymized Information shall not include personal information or any information that could identify Customer.

5. **INTELLECTUAL PROPERTY RIGHTS.** Symantec retains all title, copyright, and other proprietary rights in the Service(s), and any improvements, enhancements, modifications, and derivative works thereof, including without limitation all patent, copyright, trade secret and trademark rights. Customer's rights to use the Service(s) shall be limited to those expressly granted in the Agreement. All rights not expressly granted to Customer are retained by Symantec.

6. **INTELLECTUAL PROPERTY INDEMNITY.**

To the extent this Certificate includes provisions providing an express intellectual property indemnity for licensed software, such provision(s) are supplemented to add the Services to the scope of the parties' obligations under such indemnification provisions, to the same extent as for such licensed software. Where Customer's use of the Services is terminated pursuant to such provisions, Symantec's sole liability, in addition to its indemnification obligations herein, shall be to refund to Customer the fees paid to Symantec for the relevant Services or portion thereof.

7. **CHARGES AND PAYMENT.** If Symantec is unable to make the Service(s) available due to a failure by Customer to meet its Customer responsibilities as specified in the MSS Attributes, Symantec shall still be entitled to payment for the Service(s) as if the Service(s) had been made available. If Customer's failure to pay the Service fees constitutes a material breach of the contract, then Symantec shall have the right to temporarily suspend or terminate the provision of Services. A material breach shall be deemed to occur if the Customer fails to pay the contractually specified Services fees without justification for a period of sixty (60) days or more from the date payment was due.

Managed Security Services Certificate ("Certificate") - Per Unit

1. AGREEMENT TERMS; SUPPORT; PER UNIT USE. The term **"Agreement"** shall mean, collectively, this Certificate, the MSS service attributes document found at www.symantec.com/docs/TECH131855 containing general terms and conditions, Service(s) description(s), and service level warranties ("**SLWs**") applicable to the Service(s) ("**MSS Service Attributes**"), and the Managed Security Services Operations Manual ("**Ops Manual**") available on the Secure Internet Interface ("**SII**"), all of which are incorporated herein by reference, in that order of precedence. Service(s) are subject to the terms of the Agreement. The MSS Attributes and Ops Manual may be revised and updated by Symantec from time to time. Symantec will use commercially reasonable efforts to notify Customer of such revisions and updates by posting a revised version of the MSS Service Attributes at the URL referenced above and a revised Ops Manual on the SII. For the avoidance of doubt, revisions and updates to the MSS Service Attributes and Ops Manual will not materially degrade the Service(s). Technical assistance for the Service(s) will be provided by the Security Operations Center ("**SOC**") as described in the Ops Manual. Any capitalized terms not defined herein shall have the meaning set forth in the MSS Services Attributes and the Ops Manual, as applicable. Use of the Service(s) will be limited to the Per Unit Model, as described in the MSS Services Attributes.

2. TERM; POINTS OF CONTACT; DEVICE REGISTRATION; TERMINATION. The term of Service(s) ("**Term**") will begin on the Start Date specified on the initial page(s) of this Certificate ("**Start Date**") and end on the End Date specified on the initial page(s) of this Certificate ("**End Date**"). Service(s) are non-cancellable, non-refundable and are available to Customer immediately upon the Start Date, however, Customer acknowledges and agrees that to access the Service(s), Customer must first register the serial number(s) printed on the initial page(s) of this Certificate in the Symantec licensing portal located at https://licensing.symantec.com and designate its authorized points of contact for the Service(s) ("**POC(s)**"). Upon serial number registration, Customer will be given access to the SII and SOC technical staff. Customer must provide all technical and license information for each firewall, server, intrusion detection device, or other hardware or software (each, a "**Device**") reasonably requested by Symantec, prior to such Device being recognized by the Service(s) and connected to the SOC ("**Device Registration**"). Customer acknowledges and agrees that the Term will expire upon the End Date, even if no Devices undergo Device Registration or receive Service(s) during the Term.

Except as otherwise stated in Section (iii) below, Customer acknowledges and agrees that the Service(s) (or a portion thereof) may be terminated by: (a) either Party upon written notice if the other Party breaches any material term of the MSS Terms & Conditions (including failure to meet the Customer Responsibilities), and such breach remains uncorrected for thirty (30) days following such notice, or (b) by Symantec for convenience upon thirty (30) days prior written notice to the Customer or Ordering Activity, or (c) by the Customer or Ordering Activity in accordance with the applicable GSA Schedule contract. In the event that Symantec exercises its termination rights under (b), Symantec will credit Customer's account any prorated, unused fees received by Symantec for the applicable Service(s) terminated hereunder.

i. In the event that Customer exercises its termination rights under the above paragraph, Customer acknowledges and agrees that in order to terminate the Service(s) (or a portion thereof), Customer must submit a duly authorized termination letter ("**Termination Letter**") in accordance with the terms of the applicable GSA Schedule. .

ii. If Customer terminates the MSS Terms & Conditions and/or the Service(s) (or a portion thereof) prior to the end of the Term as described in the foregoing two paragraphs, Customer agrees to pay Symantec, or Customer's designated reseller (as applicable) a termination fee ("Termination Fee") equal to (a) if terminated in the first year of the Service, fifty percent (50%) of the amount of remaining fees that would have been due and payable to Symantec had the Service(s) been performed for the entire Term; or (b) if terminated in the second or third year of the Service, twenty-five percent (25%) of the amount of remaining fees that would have been due and payable to Symantec had the Service(s) been performed for the entire Term. If Service(s) have been prepaid for the Term, Symantec will credit Customer's account any prorated, unused fees received by Symantec for the applicable Service(s) terminated hereunder less the calculated Termination Fee. Pursuant to FAR 52.212-(l), the Termination Fee in this paragraph shall satisfy and be deemed to represent the "reasonable termination costs" which shall be due and payable by the government in addition to the fees due and payable for the Services provided up to the date of termination.

iii. Notwithstanding anything contained in Sections (i)-(iii) above, Customer acknowledges and agrees that those Services identified as "Enterprise Wide" in the Certificate cannot be partially terminated. Any termination of Service(s) identified in the Certificate as "Enterprise Wide" must apply to the entire quantity of Enterprise Wide Service(s) purchased under the Certificate.

3. PRIVACY AND DATA PROTECTION. For the purpose of providing Service(s) to Customer pursuant to the Agreement, Symantec will require Customer to supply certain personal information (such as business contact names, business telephone numbers, business e-mail addresses). Customer acknowledges that Symantec is a global organization, and such personal information may be accessible on a global basis by Symantec affiliates, by Symantec partners and subcontractors, including in countries that may have less protective data protection laws than the country in which Customer is located. By providing such personal information, Customer consents to Symantec using, transferring and processing this information on a global basis for the use described above. For any question regarding the use of personal information, Customer may contact Symantec Corporation - Privacy Lead, 350 Ellis Street, PO Box 7011, Mountain View, CA 94043, U.S.A. Telephone 650-527-8000 Email: privacy@symantec.com.

4. USE OF INFORMATION POLICY. Symantec may use certain information derived from the Service(s), once anonymized ("**Anonymized Information**") for the following purposes: (a) preparing and distributing statistical reports related to security trends and data patterns; (b) distributing Anonymized Information to Symantec customers, in compiled or original formats, for the purposes of providing computer security information; and / or (c) analysis; internal research, product or services development, or for providing general security related services. Anonymized Information shall not include personal information or any information that could identify Customer.

5. INTELLECTUAL PROPERTY RIGHTS. Symantec retains all title, copyright, and other proprietary rights in the Service(s), and any improvements, enhancements, modifications, and derivative works thereof, including without limitation all patent, copyright, trade secret and trademark rights. Customer's rights to use the Service(s) shall be limited to those expressly granted in the Agreement. All rights not expressly granted to Customer are retained by Symantec.

6. INTELLECTUAL PROPERTY INDEMNITY. To the extent this Certificate includes provisions providing an express intellectual property indemnity for licensed software, such provision(s) are supplemented to add the Services to the scope of the parties' obligations under such indemnification provisions, to the same extent as for such licensed software. Where Customer's use of the Services is terminated pursuant to such provisions, Symantec's sole liability, in addition to its indemnification obligations herein, shall be to refund Customer the fees paid to Symantec for the relevant Services or portion thereof.

7. CHARGES AND PAYMENT. If Symantec is unable to make the Service(s) available due to a failure by Customer to meet its Customer responsibilities as specified in the MSS Attributes, Symantec shall still be entitled to payment for the Service(s) as if the Service(s) had been made available. If Customer's failure to pay the Service fees constitutes a material breach of the contract, then Symantec shall have the right to temporarily suspend or terminate the

provision of Services. A material breach shall be deemed to occur if the Customer fails to pay the contractually specified Services fees without justification for a period of sixty (60) days or more from the date payment was due.

8. Miscellaneous. Symantec may assign the Service(s) or any part thereof subject to FAR Part 42.12, and may additionally subcontract the Agreement and / or Service(s), provided that it remains responsible for any subcontractors performing on its behalf.

MANAGED SECURITY SERVICES ATTRIBUTES DOCUMENT

("MSS Service Attributes") is made a part of and wholly incorporated into the Agreement, as defined in the Symantec order confirmation certificate referencing these MSS Service Attributes ("Certificate"), and apply to the Symantec Managed Security Services (individually a "Service" or collectively "Service(s)") set forth on the initial page(s) of such Certificate. Any capitalized terms not defined herein shall have the same meaning as in the Certificate or in the Managed Security Services Operation Manual ("Ops Manual").

This MSS Service Attributes document is made up of the following sections:

- Section 1: Managed Security Services - General Terms and Conditions;
- Section 2: Managed Security Services - Service Descriptions;
- Section 3: Managed Security Services - Service Level Warranties; and
- Section 4: Managed Security Services - Attachment A – Service(s) Offerings Chart.

SECTION 1

MANAGED SECURITY SERVICES
GENERAL TERMS AND CONDITIONS

The Parties acknowledge and agree that the following terms and conditions apply to the Service(s):

1. **Service(s) Use Model:** Use of the Service(s) is subject to the limitations set forth below, as applicable to the Service(s) identified on the face of the Certificate:

1.1 **Enterprise Wide Model.**

a) **End User(s); Nodes.** For Service(s) identified on the initial page(s) of the Certificate as 'Enterprise Wide', Customer warrants and represents that the quantity of Service(s) purchased by Customer reflects the total number of Nodes owned or used by Customer or the legal entity or entities benefiting from the Service(s) (each, an "**End User**", collectively, "**End User(s)**") at the time of purchase, regardless of whether each such Node directly interacts with or is protected by the Service(s) ("**Node Count**"). Each "**Node**" is a virtual or physical unique network address, such as an Internet protocol Address.

b) **Outsourcer Purchases.** If Customer is a provider of outsourced services and purchases Enterprise Wide Service(s) for the benefit of an End User pursuant to an outsourcing agreement with such End User, Customer warrants and represents that the quantity of Service(s) purchased by Customer reflects the total Node Count for such End User receiving the Customer outsourced services.

c) **Node Count Compliance.** If, during the Term, End User(s) applicable Node Count increases by more than five percent (5%) over the Node Count associated with the Service(s) purchased, then Customer agrees to promptly, but no later than thirty (30) days following the increase in Node Count, purchase additional Service(s) to become compliant with such expanded Node Count. Symantec may, at its discretion, but no more than once every twelve (12) months, request Customer to validate the End User(s)' Node Count to Symantec in writing.

1.2 **Per Unit Model:** For Service(s) not designated on the face of the Certificate as "Enterprise Wide", (such Service(s), the "**Per Unit** Model"), Symantec will provide Service(s) to Customer commensurate with the quantity of Service(s) entitlement purchased as identified on the initial page(s) of the Certificate.

2. **Customer Obligations / Responsibilities:** Customer acknowledges and agrees that Symantec's ability to perform the Service(s) during the Term may be subject to Customer meeting all of its obligations and Customer responsibilities as described in the Agreement (including without limitation the Customer responsibilities in Clause 2.1 below) during the Term. Customer acknowledges and agrees that Symantec will have no liability whatsoever for any failure to perform the Services(s) if such failure arises out of Customer's act or omission inconsistent with Customer's obligations described in the Agreement (including, without limitation the Customer responsibilities described in Clause 2.1 below) which impede Symantec's ability to perform the Service(s). Without prejudice to the foregoing, any such failure to perform the Service(s) by Symantec due to the foregoing shall not postpone or delay the Term nor be deemed a breach of the Agreement

2.1 The following list of Customer responsibilities is the minimum required to ensure Symantec's ability to perform the Service(s). At a minimum, Customer is responsible for the following:

2.1.1 Providing reasonable assistance to Symantec, including, but not limited to, providing all technical and license information related to the Service(s) reasonably requested by Symantec, and to enable Symantec to perform the Service(s).

2.1.2 Providing all required hardware, virtual machines, or software necessary for the Symantec log collection platform (to be located at Customer site), and enabling access to such hardware, virtual machines, or software by Symantec (as specified in the Ops Manual).

2.1.3 Providing a permanent, dedicated analog telephone line to support the Out-of-Band Management Solution if Symantec provides an Out-of-Band Management Solution to Customer. Customer is responsible for maintaining the functionality of this dedicated line. Details on the Out-of-Band Management Solution are contained in the Services Description section of this MSS Service Attributes and in the Ops Manual.

2.1.4 Providing Symantec with accurate and up-to-date information, including, the name, email, landline, mobile, and pager numbers for all designated, authorized POC(s) who will be provided access to the SII.

2.1.5 Providing the name, e-mail address, and landline, mobile, and pager numbers for all shipping, installation and security points of contact.

2.1.6 Notifying Symantec at least twelve (12) hours in advance of any scheduled maintenance, network, or system administration activity that would affect Symantec's ability to perform the Service(s).

2.1.7 Reviewing the Daily Service Summary (as defined in the Ops Manual) to understand the current status of Service(s) delivered and actively work with the SOC to resolve any tickets requiring Customer input or action.

2.1.8 Sole responsibility for maintaining current maintenance and technical support contracts with Customer's software and hardware vendors for any Device affected by Service(s).

2.1.9 Ensuring any Devices receiving Service(s) conform to the version requirements stated in the Symantec Supported Product List, available on the SII ("**SPL**"). The SPL describes the supported versions of the Devices that may receive service under the Service(s).

2.1.10 Intentionally Omitted.

2.1.11 Interact with Device manufacturers and vendors to ensure that the Device(s) are scoped and implemented in accordance with manufacturer's suggested standards. Customer is responsible for interactions with Device manufacturers or vendors regarding the resolution of any issues related to Device scoping, feature limitations or performance issues.

2.1.12 Remediation and resolution of issues caused by Customer initiated changes to Device(s) which negatively impact the Services or the functionality, health, stability, or performance of Device(s). Symantec will charge additional fees (Tokens) in the event that Customer requires Symantec's assistance for remediation or resolution activities.

3. For those Service(s) purchased prior to July 12, 2011, in addition to the terms contained herein, Customer acknowledges and agrees to continue compliance with sub-sections 3, 6, 7, 8, 9, 12, and 13 of Section 1 of the Managed Security Services Attributes dated May 27, 2010 (20100527) ("MSSA"). A copy of the MSSA is available at www.symantec.com/docs/TECH131855, or upon request from Symantec by emailing DL-MSS-BusinessOperations@symantec.com.

SECTION 2
MANAGED SECURITY SERVICES
SERVICES DESCRIPTIONS

A. SERVICE FEATURES. The Managed Security Service(s) Offerings Chart, contained in Attachment A hereto ("Service(s) Offerings Chart"), details certain information and attributes associated with each of the Service(s). In addition to those services features identified in the Service(s) Offerings Chart, the following service features apply to all the Service(s):

1. **Secure Internet Interface ("SII").** Each of the Service(s) includes access to and use of the web portal ("**Secure Internet Interface**" or "**SII**"), which is made available to Customer for use during the Term.

2. **Managed Security Services Operations Manual.** The Ops Manual, which is available on the SII, provides further description of the Service(s), and details additional Customer responsibilities which may be applicable to the Service(s). Symantec will use commercially reasonable efforts to give Customer thirty (30) days' notice through the SII of any material change to the Ops Manual. Upon request, the Ops Manual will be made available to Customer or the Ordering Activity. The MSS Attributes and Ops Manual may be revised and updated by Symantec from time to time. Symantec will use commercially reasonable efforts to notify Customer of such revisions and updates by posting a revised version of the MSS Service Attributes at the URL referenced above and a revised Ops Manual on the SII. For the avoidance of doubt, revisions and updates to the MSS Service Attributes and Ops Manual will not materially degrade the Service(s).

3. **Security Operations Centers.** All Service(s) are performed remotely from Security Operations Centers ("**SOC(s)**"**).**

4. **Monitored & Managed Device Scheduled Maintenance Outages**. Symantec will, from time to time, schedule regular maintenance on Devices, requiring a maintenance outage. The protocol for any such maintenance outage is described in the Ops Manual.

B. TECHNICAL SERVICE COORDINATOR. The Technical Service Coordinator, described in the Service(s) Offerings Chart and the Ops Manual, is a resource responsible for coordinating installation and ongoing support for Customer. Symantec must first receive a purchase order sufficient to cover all travel and incidental expenses if Customer has purchased the Technical Service Coordinator service and requests that the Technical Service Coordinator perform Service(s) at Customer's site.

C. HOSTED MANAGEMENT CONSOLES. Customer may purchase the use of Hosted Management Consoles (as described in the Ops Manual) located at the SOC for centralized management of certain Devices receiving Service(s). Customer is responsible for obtaining any required license(s) from the technology vendor to allow applicable use of the Hosted Management Console.

D. REPAIR AND REPLACEMENT OF THE OUT-OF-BAND MANAGEMENT SOLUTION HARDWARE. The "**Out-of-Band Management Solution**" means a third-party hardware product which Symantec may provide, at its sole discretion, for Customer's use to facilitate the remote configuration and management of Customer's Devices. Customer acknowledges and agrees that Symantec and/or its licensors are the owner(s) of any Out-of-Band Management Solution and only grants Customer the right to use the Out-of-Band Management Solution during the Term. In the event the Out-of-Band Management Solution fails due to a defect during the Term, Symantec will replace it subject to notification and reasonable cooperation from Customer. Customer acknowledges and agrees that Symantec is not responsible for any outages that may occur during the time that the Out-of-Band Management Solution is being replaced. Customer further acknowledges and agrees that Customer is responsible for the cost of replacing the Out-of-Band Management Solution if failure is due to misuse or negligence of Customer.

E. ADDITIONAL / OUT OF SCOPE SERVICE(S); HELP DESK TOKENS.

1. Additional Service(s), features, or options described in the Service(s) Offerings Chart may be ordered through the submission of a purchase order.

2. Hour-long telephone technical support sessions (each, an "**Out-of-Scope Help Desk Token**") provided from the SOC Help Desk are available for purchase by Customer by submitting a purchase order designating such. An Out-of-Scope Help Desk Token may only be used for services that fall outside of the scope of Service(s) ordered. The scope of such support is further described in the Ops Manual. Out-of-Scope Help Desk Tokens are only valid for one (1) year from the date of order receipt by Symantec.

SECTION 3
MANAGED SECURITY SERVICES
SERVICE LEVEL WARRANTIES

A. SERVICE LEVEL WARRANTIES & SERVICE CREDITS.

The SLWs listed below will apply to those Service(s) listed in the Service(s) Offerings Chart. The Service(s) Offerings Chart additionally details the SLW(s) applicable for each SLW. Symantec's sole and exclusive obligation and Customer's sole and exclusive remedy for failure to meet the SLWs listed below shall be limited to the payment of Service Credit(s), as described in Section B of these SLWs.

1. **Device Registration Warranty**. Symantec will register a Device that conforms to the SPL by the later of: (i) the Start Date identified on the initial page(s)of the Certificate, (ii) the mutually agreed upon Device Registration date (if applicable), or (iii)fifteen (15) business days following Symantec's receipt of all reasonably requested technical and license information for each Device, as further specified in the Certificate. If Symantec fails to register a Device that conforms to the SPL in accordance with the timeline listed above then Symantec will credit Customer's account with one (1) Service Credit for each day this deadline is missed.

2. **Severe Event Notification Warranty**. Symantec will initiate contact to notify Customer of Emergency and Critical Events (as defined in the Ops Manual) within the specified Severe Event Notification Time identified in the Service(s) Offerings Chart, once the determination that an Emergency and Critical Event has occurred (as specified in the Ops Manual). If Symantec does not initiate contact within the specified time, Symantec will credit Customer's account with one (1) Service Credit, unless the Device subject to the Emergency or Critical Event is deemed to be a Runaway Device, as defined in the Ops Manual.

3. **Managed Device Availability Up-Time Warranty**. Devices shall be available in accordance with the Managed Device Availability Up-time Percentage, as identified in the Service(s) Offerings Chart, of each calendar month during the Term (excluding Scheduled Outages, Maintenance, Hardware/Software Failures, Failures, as such terms are defined in the Ops Manual) resulting from changes made by the Customer, and circumstances beyond SOC control). If the Device is not available as specified in the preceding sentence, Symantec will credit Customer's account with one (1) Service Credit for each 24 hour period, or portion thereof for which this SLW is not met. If the Device does not meet the version prerequisites as specified in the current SPL or the immediately prior supported version prerequisites (as specified in a prior version of the SPL), then Symantec will not be liable for this SLW for such non-conforming Device.

4. **Standard Changes Completion Time Warranty**. Symantec will complete Standard Changes within the Standard Changes Completion Time, identified in the Service(s) Offerings Chart. If Symantec does not meet this SLW, Symantec will credit Customer's account with one (1) Service Credit.

5. **Minor Changes Completion Time Warranty.** Symantec will complete Minor Changes within the Minor Changes Completion Time, as identified in the Service(s) Offerings Chart. If Symantec does not meet this SLW, Symantec will credit Customer's account with one (1) Service Credit.

6. **Emergency Change or Assistance Response Time Warranty**. When an emergency change request or other emergency assistance is required, a SOC engineer will be made available to begin work on or assist with the emergency request in accordance with the timeline identified in the Service(s) Offerings Chart. If Symantec does not meet this SLW, and the Customer has not exceeded their contracted Emergency Change or Assistance Requests for the month as specified in Service(s) Offerings Chart, Symantec will credit Client's account with one (1) Service Credit.

7. **SOC Infrastructure Up-Time Warranty**. Symantec warrants that the SOC data storage, SOC log analysis processing, any Hosted Management Consoles (as described in the Ops Manual), the SII, and SOC customer communication methods (phone, email, SII) (together, the "**SOC Infrastructure**") shall be available in accordance with the SOC Infrastructure Up-time Percentage identified in the Service(s) Offerings Chart, for each calendar month during the Term (excluding scheduled maintenance). If any or all of the SOC Infrastructure is not available as specified in the preceding sentence, Symantec will credit Customer's account with one (1) Service Credit for each 24 hour period, or portion thereof for which the warranty is not met.

8. **Monthly Reporting Warranty**. If Symantec does not provide the applicable monthly reports, as specified in the Ops Manual, to Customer by or before the Monthly Reporting Time, as identified in the Service(s) Offerings Chart, of the immediately following calendar month, Symantec agrees to credit Customer's account with one (1) Service Credit.

B. SERVICE CREDITS; LIMITATION OF SERVICE CREDIT LIABILILTY.

1. **Service Credits.** A service credit ("**Service Credit**") shall be calculated as 10% of the computed daily fee payable to Symantec for the Service(s) purchased on the initial page(s) of the Certificate. Each Service Credit granted hereunder will first be applied towards Customer's next invoice due for the applicable Service(s) during the Term, or if no additional invoices are due for such Service(s), shall be provided as a payment.

2. **Limitation of Service Credit Obligation.** Notwithstanding anything to the contrary in the Agreement, in no event will Symantec be required to credit Customer more than the value of thirty (30) days of Service(s), per month, for any failure to meet the SLWs for any Service(s) that Symantec is providing for Customer at the time the credit is accrued. Symantec's sole and exclusive obligation and Customer's sole and exclusive remedy for each respective SLW set forth in the Agreement will be limited to the issuance of Service Credits.

SECTION 4
MANAGED SECURITY SERVICES

SERVICE(S) OFFERINGS CHARTS

SYMANTEC MSS SECURITY MONITORING SERVICES

Feature	SYMANTEC MSS SECURITY MONITORING SERVICES		
	Log Retention Service	**Essential Security Monitoring Service**	**Advanced Security Monitoring Service**
Service Use Model	Per Unit or Enterprise Wide	Per Unit or Enterprise Wide	Per Unit or Enterprise Wide
Service Level Warranty Metrics			
Device Registration	As described in the Service Level Warranties		
Severe Event Notification Time	N/A	10 minutes	10 minutes
SOC Infrastructure Up-Time Percentage	99.90%	99.90%	99.90%
Monthly Reporting Time	by 5th business day	by 5th business day	by 5th business day
Hosted Log Retention (duration @ SOC during Services Term only):			
Online Raw Log Retention	3 months (92 days)[3]	3 months (92 days)[3]	3 months (92 days)[3]
Additional 1 year Online Raw Log Retention	optional, 12 month increments	optional, 12 month increments	optional, 12 month increments
Offline (removeable media) Raw Log Retention[4]	12 months	12 months	12 months
Online Incident Data Retention	Service Term	Service Term	Service Term
Security Incident Analysis			
Log/Alert data collection, aggregation, and normalization	X	X	X
Logs available for SOC Analyst inspection	X[1]	X	X
Analyze security data and customer context to detect signs of malicious activity •Identify firewall port scans and brute force threshold exceptions •Identify host and network intrusions or suspect traffic •Identify connections to backdoors and Trojans •Identify events detected by endpoint security solutions •Identify internal systems attacking other internal systems •Identify connect to/from customer-specified bad/blocked URLs •Identify threats through parsing of web proxy data for connections to malicious URLs	N/A	 X X X X X X X	 X X X X X X X
Advanced security data analysis and correlation with Symantec global threat intelligence (GIN) to detect/validate signs of malicious activity. •Identify hosts connecting to command and control botnet servers •Identify content matches to a list of known bad IP addresses •Identify content matches to a list of known bad URL addresses •Identify anomalous traffic to/from an IP address within a registered network	N/A	N/A	 X X X X
Vulnerability Data Correlation Integration	N/A	X	X
Validate, Assess and Prioritize impact of Incident to Enterprise	X	X	X
Incident Escalation			
Method of Notification of Security Incidents:			
Voice (as defined in the Manual), SII, Email (per Incident or Digest)	N/A	X	X
Method of Notification of Outage Incidents[2]:			
Voice (as defined in the Manual), SII, Email (per Incident or Digest)	N/A	X	X
General Service Features			
Detection and response updated for emerging threats	N/A	X	X
Daily Service Summary delivered by e-mail	N/A	X	X
Log/device unavailability alerting and notification[2]	X	X	X
Online logs may be queried by customer via the SII	X	X	X
Compliance reporting available on the SII	X	X	X
Access to the Secure Internet Interface	X	X	X

[1]Log Retention alone performs no security analysis. However, the retained log data is automatically associated with security incidents generated by other devices under Essential or Advanced Security Monitoring service(s) and is available for SOC analyst inspection.

[2]Notification of outage incidents for the HIPS/HIDS and Endpoint monitoring technologies shall apply to Manager/Management consoles only. Notification of outage incidents for all other technologies registered in netblock ranges shall be based on outage monitoring of the netblock range, Log Collection Platform, or Remote Importer.

[3]Subject to run away device limits per the Manual.

[4]Restoral fees apply - customer must purchase Out-of-Scope Service Tokens commensurate with level of effort for data restoration.

SYMANTEC MSS SECURITY MANAGEMENT SERVICES

	SYMANTEC MSS SECURITY MANAGEMENT SERVICES				
Feature	**Essential Management Firewall or UTM**	**Advanced Management Firewall or UTM**	**Essential Management Endpoint Protection**	**Enterprise Wide or Advanced Management Endpoint Protection**	**Enterprise Wide or Advanced Management IDS or IPS**
Service Use Model	Per Unit only	Per Unit only	Per Unit only	Per Unit or Enterprise Wide	Per Unit or Enterprise Wide
Service Level Warranty Metrics					
Device Registration	As described in the Service Level Warranties				
Managed Device Availability Up-Time Percentage	99.90%	99.95%	N/A	N/A	99.95%
SOC Infrastructure Up-Time Percentage	99.90%	99.90%	99.90%	99.90%	99.90%
Monthly Reporting Time	by 5th business day	by 5th business day	by 5th business day	by 5th business day	by 5th business day
Standard Changes Completion Time	6 hours for changes performed and completed by SOC				
Minor Changes Completion Time	24 hours for changes performed and completed by SOC				
Emergency Change or Assistance Response Time	Symantec will attempt to make SOC engineer available immediately; but not later than within 30 minutes of request				
Change Management					
Standard Changes (Includes a single, low-risk configuration or policy change using SII standard change request templates. For endpoints, includes basic administrative tasks on the Management Console)	Customer Responsibility (The SOC will complete up to 5 Standard or Minor changes each calendar month).	Unlimited Requests	Customer Responsibility[2] (The SOC is available to assist in up to 5 Standard changes each calendar month).	Unlimited Requests	Updates to detection definitions occurs automatically when the signature update is released by the vendor.
Minor Changes (Includes a single change that is too complex to be requested thru the SII standard change request templates. Includes endpoint Anti-virus/Firewall/IPS/Application Control/Device Control/Host Integrity policy management)	Customer Responsibility (The SOC will complete up to 5 Standard or Minor changes each calendar month).	Unlimited Requests	Customer Responsibility[2] (The SOC is available to assist in up to 2 Minor changes each calendar month).	Unlimited Requests	Unlimited Requests
Significant Changes (Includes software changes or high-risk policy changes that interrupt device functionality. Includes Endpoint patch and maintenance updates to Management Console and Endpoint Protection Database)	SOC will initiate change requests for software upgrades/patches and schedule with customer. Customer initiated change requests require 5 business days advance notice.				
Major Changes (Includes changes that modify architecture, technology or that require advance design)	Not included in scope of Services (Available with purchase of Out-of-Scope Help Desk Service Tokens)				
Emergency Change or Assistance Requests	2 per calendar month[1]	5 per calendar month[1]	2 per calendar month[1]	5 per calendar month[1]	5 per calendar month[1]
Service Features					
Provide management and configuration assistance for the features listed[3]	• Firewalling • Network address translation (NAT) • Anti-virus • Intrusion Protection • Content Filtering • High Availability • Site-to-site VPNs	• Firewalling • Network address translation (NAT) • Anti-virus • Intrusion Protection • Content Filtering • High Availability • Site-to-site VPNs • Cluster Architectures • Remote Access VPN	• Database Configuration • Database Replication • Manager Administration • Anti-virus/Desktop or System Firewall /IPS /Application Control/ Device Control/Host Integrity policy change assistance	• Database Configuration • Database Replication • Manager Administration • Group/Location Administration • Installation Packages • Anti-virus/Desktop or System Firewall /IPS /Application Control/ Device Control/Host Integrity policy management	• Policy management • Signature update • In-line configuration support • High Availability
Rule / VPN limits (per device):					
Maximum Rules in Firewall/UTM Policy	Unlimited Rules		N/A		N/A
Maximum VPN Policy (site-to-site VPNs)	Unlimited VPNs (restricted to connections to other SOC Managed Firewalls)	Unlimited VPNs (no connection restrictions)	N/A	N/A	N/A
Incident / Fault Management:					
Monitor Managed Device for accessibility by SOC	X	X	X	X	X
Monitor Managed Device for detected fault messages[3]	X	X	X	X	X
Monitor for content update failure messages[3]	X	X	X	X	X
Respond to and troubleshoot issues for Managed Device	X	X	For Manager/Management Console only. Troubleshooting issues affecting Endpoint agent software is not included in scope of service(s)[4].		X
Lifecycle Management - Maintenance Notification:					
Standard Maintenance	24 hours' notice		24 hours' notice		24 hours' notice
Emergency Maintenance	1 hour's notice		1 hour's notice		1 hour's notice
Reporting:					
Monthly Service Report	Available on the SII		Available on the SII		Available on the SII
Visibility into current tickets, Device status, Log Outage alerts	Available on the SII		Available on the SII		Available on the SII
Access to the Secure Internet Interface	X	X	X	X	X

[1]Additional available with purchase of Out-of-Scope Help Desk Service Tokens.

[2]For Endpoints, User Administration for the Management Console always performed by Symantec MSS.

[3]Subject to the technology support of features

[4]For Symantec products, SOC will facilitate escalation to Symantec Product Support (Customer should work directly with product support as applicable for resolution)

SYMANTEC MSS TECHNICAL SERVICE COORDINATOR

Function	MSS Technical Service Coordinator[1]
Service and Device Provisioning	
Manage client project plan over selected implementation schedule	X
Communicate status of implementation via e-mail on a weekly basis	X
Participate in daily or weekly provisioning calls to expedite provisioning of a complex order	X
Assist in the establishment of client specific testing criteria and procedures	X
Routine Service Delivery	
Named liaison for all service related requests and/or problems available during business hours	X
Assist in remediation coordination of critical incidents	X
Review all aspects of service delivery with client on a monthly basis (client schedule permitting)	X
Assist in the coordination of any major technology upgrades	X
Participate in daily/weekly client status calls	X
Optional Assistance (Dependent on resource availability & client request)	
Prepare client program-specific procedural guides	X
Coordinate and assist in fulfilling requests for adhoc reporting	X

[1]MSS Technical Service Coordinator functions are performed remotely.