Managed Security Services

Service Description

May 2020

This Service Description, with any attachments included by reference, is provided under the following terms and conditions in addition to any terms and conditions referenced in the order confirmation issued by Accenture (or Symantec, as predecessor to Accenture) related to Customer's purchase of Services or any similar document which further defines Customer's rights and obligations related to the Services, such as a Symantec certificate (the "Order Confirmation") which incorporates this Service Description by reference (the Order Confirmation, this Service Description and any other documents referenced therein collectively, the "Agreement"). Any terms that are used but not defined herein shall have the meaning set forth in the Agreement. This Service Description may be updated from time to time by Accenture.

Service Overview

The Managed Security Services (each a "**Service**" or collectively, "**MSS**" or "**Services**") comprise one or more of the following services, depending on the offering purchased by Customer as indicated in the Order Confirmation and as further described in this Service Description.

- **Advanced Security Monitoring Service** provides 24x7 real-time security monitoring, analysis and reporting, and early warning intelligence. The Services are performed utilizing a combination of skilled analysts and proprietary technology in conjunction with Accenture's global threat intelligence capability in an effort to identify known and emerging technology security threats to Customer's critical infrastructure.

- **Hosted Log Retention Service** provides log collection and storage in a resilient technology environment hosted by Accenture.

- **Advanced Managed IDS/IPS Intrusion Detection System (IDS) and Intrusion Prevention System** provides 24x7 alarm and incident management, lifecycle management support and emergency access to security practitioners.

- **Managed Endpoint Detection and Response Service ("MEDR")** provides additional investigation of identified suspicious activities utilizing the MEDR tool in an effort to provide enhanced context, refine incident severity and proactive response, as applicable. MEDR is available in the following two ways:

    - MEDR as an MSS add-on. Available for customers who use the MSS Advanced Security Monitoring Service (separate purchase required).
    - MEDR on a standalone basis. Available to customers that do not currently have MSS Advanced Security Monitoring Service and have an End Point Protection product (EPP) running on their endpoints that is supported for advanced monitoring, as set forth on the Supported Product List (SPL).

Managed Security Services

Service Description

May 2020

This Service Description shall apply to Services purchased or renewed by Customer on or after July 19, 2017.

For Services purchased by Customer prior to July 19, 2017, the Service Description dated April 2017 shall apply, a copy of which is available at www.accenture.com/us-en/insights/security/legal-terms or upon request to Accenture.

For Services purchased by Customer prior to November 1, 2016, the Service Attributes dated January 1, 2015 shall apply, a copy of which is available at www.accenture.com/us-en/insights/security/legal-terms or upon request to Accenture.

Table of Contents

TECHNICAL/BUSINESS FUNCTIONALITY AND CAPABILITIES

Service Features

- The MSS Offerings Chart, contained in Attachment 1 of this Service Description ("**MSS Offerings Chart**"), details certain information and attributes associated with each of the Services. In addition to those service features identified in the MSS Offerings Chart, the following service features apply to all the Services:
  - ***MSS Portal.*** Each of the Services includes access to and use of the MSS portal ("**Portal**"), which is made available

to Customer for use during the Term.

- ***Managed Security Services Operations Manual***. The Operations Manual, which is available on the Portal, provides further description of the Service(s), and details additional Customer responsibilities which may be applicable to the Service(s). Accenture will use commercially reasonable efforts to give Customer thirty (30) days' notice through the Portal of any material change to the Operations Manual.
- ***Security Operations Centers***. All Service(s) are performed remotely from Security Operations Centers("**SOC(s)**").
- ***Scheduled Outages***. Accenture will, from time to time, schedule regular maintenance on the SOC Infrastructure (defined below) or on Device(s) (defined below) receiving Management Service(s) (defined below), requiring a maintenance outage. The protocol for any such maintenance outage is described in the Operations Manual.

- **HOSTED MANAGEMENT CONSOLES**. Customer may renew the use of Hosted Management Consoles located in Accenture's environment for centralized management of certain Device(s) 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 (Hosted Management Console is no longer available for new purchases).

- **MANAGED NETWORK FORENSICS SERVICE ("MNF").** MNF provides additional investigation of identified suspicious activities in an effort to provide enhanced context, refine incident severity and proactive response, as applicable. MNF is available for customers who also use the Advanced Security Monitoring Service of MSS to enhance its service features and own Accenture-approved Network Forensics Investigation Devices (defined below). For more details, please refer to **Attachment 2**. NOTE: The version of the Service Description for MSS that applies to you continues to apply during your use of MNF.

- **ADDITIONAL / OUT OF SCOPE SERVICE(S)**. From time to time, Customer may request and Accenture may provide, certain services not currently described in the Service(s) Offerings Chart (hereinafter "**Exception Services**"). The description and fees for any Exception Services must be mutually agreed in writing.

Out of Scope/Additional Terms.
Anything not specifically described in this Service Description is out of scope and is not included in the Service. Customer acknowledges, understands and agrees that Accenture does not guarantee or otherwise warrant that the Service, or Accenture's recommendations and plans made by Accenture as a result of that Service, will result in the identification, detection, containment, eradication of, or recovery from all of Customer's system threats, vulnerabilities, malware, malicious software, or other malicious threats. Customer agrees not to represent to anyone that Accenture has provided such a guarantee or warranty.

Litigation Support Services. The following services ("**Litigation Support Services**") are explicitly excluded from the Services provided under this Service Description:

- Depositions, fact witness testimony, expert witness testimony, affidavits, declarations, expert reports;
- Responding to discovery requests, subpoenas;
- eDiscovery services; or
- Other forms of litigation support or participation in any legal proceeding relating to the subject matter of the engagement (including those involving a governmental entity).

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

- The then-current hourly rate would apply for all Accenture personnel who perform any Litigation Support Services. Litigation Support Services are provided on a time and materials basis, since the actual time required to complete Litigation Support Services may vary.
- The parties will work in good faith to document the terms in this "Litigation Support Services" section as well as any additional necessary terms and conditions in a separate agreement at such time as the need for Litigation Support Services should occur.
- Indemnification. Customer will fully indemnify and reimburse Accenture for all losses, damages, liabilities, expenses, costs, and fees (including reasonable attorney's fees) and for Accenture personnel time (at the hourly rate listed above for Litigation Support Services) incurred in connection with any allegation, claim, demand, subpoena, or legal proceeding (including those involving a governmental entity) arising from any incident for which Customer has engaged Accenture to provide the Service, regardless of fault.
- This "Litigation Support Services" Section will survive termination or expiration of the Agreement.

Customer Responsibilities

Customer may use the Services only in accordance with the use meter or model under which Customer has obtained use of the Service: (i) as indicated in the Order Confirmation; and (ii) as defined in this Service Description or the Agreement.

Accenture will only perform the Service if Customer provides required information or performs required actions. If Customer does not provide/perform per the following responsibilities, Accenture's performance of the Service may be delayed, impaired or prevented, and/or eligibility for Service Level Agreement benefits may be voided, as noted below.

- Adequate Customer Personnel: Customer must provide adequate personnel to assist Accenture in delivery of the Service, upon reasonable request by Accenture.
- Device Registration: 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 Accenture, prior to such Device being recognized by and connected to the Service ("**Device Registration**"). Customer acknowledges and agrees that the Term will expire upon the last day of the Term, even if no Devices undergo Device Registration or receive Service(s) during the Term.
- Reasonable Assistance: Customer must provide reasonable assistance to Accenture, including, but not limited to, providing all technical and license information related to the Service(s) reasonably requested by Accenture, and to enable Accenture to perform the Service(s). For management Service(s) (as labeled in the MSS Offerings Chart ("**Management Service(s)**"), Customer must provide Accenture remote access to the managed Device(s) and necessary administrative credentials to enable Accenture to perform the Service(s).
- Use of Log Collection Platform: For monitoring Service (as further described in the MSS Offerings Chart ("**Monitoring Service(s)**"), Customer may be required to successfully install an Accenture Log Collection Platform ("**LCP**") image within the Customer's environment, and establish the necessary network access to allow the SOC to remotely manage the LCP, and to allow the collector to extract log data of the Device(s) and transport such log data back to the SOC. LCP must be a supported version as specified in the Supported Product List ("**SPL**") available on the Portal (requires log-in). Customer must provide all required hardware or virtual machines necessary for the LCP, and enable access to such hardware or virtual machines by Accenture (as specified in the Operations Manual). In addition, for select logging technologies (as specified in the SPL), Customer may also be required to install collectors on customer provided systems other than the LCP and enable access to/from the LCP. Customer understands that Accenture must have access to log data of the Device(s) in a format that is compatible with Accenture's collectors and in some cases this may require configuration changes to Device(s). Customer agrees to make any necessary changes to the configuration of the Device(s), as requested by Accenture, to conform with the supported format.
- Accurate Information: Customer must provide Accenture with accurate and up-to-date information, including, the name, email, landline, mobile, and pager numbers for all designated, authorized points of contact who will be provided access to the portal. Customer must provide the name, email, and phone numbers for all shipping, installation and security

points of contact.

- Customer's Outage: Customer must provide Accenture at least twelve (12) hours in advance of any scheduled outage (maintenance), network, or system administration activity that would affect Accenture's ability to perform the Service(s).
- Daily Service Summary: Customer must review the Daily Service Summary to understand the current status of Service(s) delivered and actively work with Accenture to resolve any tickets requiring Customer input or action.
- Customer Software and Hardware: It is Customer's sole responsibility to maintain current maintenance and technical support contracts with Customer's software and hardware vendors for any Device(s) affected by Service(s). Customer must ensure any Device(s) receiving Service(s) conform to the version requirements stated in the SPL. It is Customer's responsibility to interact with Device(s) manufacturers and vendors to ensure that the Device(s) are scoped and implemented in accordance with manufacturer's suggested standards. Customer is also responsible for interactions with Device(s) manufacturers or vendors regarding the resolution of any issues related to Device(s) scoping, feature limitations or performance issues. For those Service(s) where Accenture is not solely responsible for the management of Customer's Device(s), Customer is responsible for remediation and resolution of changes to Device(s) which negatively impact the Service(s) or the functionality, health, stability, or performance of Device(s). Accenture may charge additional fees in the event that Customer requires Accenture's assistance for remediation or resolution activities.
- Consent and Authorization: Customer acknowledges, understands and agrees that unauthorized access to computer systems or data or intrusion into hosts and network access points may be prohibited by applicable local law. Customer is: (i) explicitly confirming to Accenture that it has obtained all applicable consents and authority for Accenture to deliver the Service; and (ii) giving Accenture explicit permission to perform the Service and to access and process any and all Customer Data related to the Service, including without limitation, if applicable, consent to analyze host forensics including but not limited to, memory, disk, logs, data, network traffic in real time to detect evidence of known malicious communication patterns and traffic containing unrecognized malicious code (malware), connect to Customer's computer network, archive and retain all host forensics data including but not limited to, memory, disk, logs, data, network traffic captured as part of Services (including to store any malware and metadata supplied by Customer, or anyone else working with or for Customer), and (iii) representing that such access and processing by Accenture does not violate any applicable law or any obligation Customer owes to a third party; and (iv) accepting sole responsibility and liability with respect to engagement of such Service. Accordingly, Customer warrants and represents that it is the owner or licensee of any network, systems, IP addresses software, appliances, code, templates, tools, policies, records, working papers, data and/or computers upon which Accenture performs the Service ("Customer Systems"), which may be visible as Customer Data in connection with the Service, and that Customer is authorized to instruct Accenture to perform the Service on such Customer Systems. Customer shall fully indemnify and hold harmless Accenture for any claims by any third parties related to the Service.
- Acceptable Use Policy: Customer is responsible for complying with the *CSS Online Services Acceptable Use Policy*, a copy of which is available at: www.accenture.com/us-en/insights/security/legal-terms or upon request to Accenture.
- Reporting: Customer acknowledges and agrees that in the course of delivering the Service, Accenture may become aware of issues such as data breaches, network intrusions, or the presence of malware, and that such issues may give rise to regulatory reporting obligations which Customer is subject to in one of more territories in which Customer operates. Accordingly, Customer shall remain solely responsible for all such reporting requirements and Accenture shall have no liability in this regard whatsoever.

In addition, Customer will be responsible for the Customer obligations described in the MSS Offerings Chart and the Operations Manual.

Supported Platforms and Technical Requirements

Supported platforms for the Service are listed in the Portal.

Hardware requirements can be found in the MSS Deployment Guide (and such other applicable guide based on your purchase)

distributed by Customer's Service Manager.

The SPL describes the supported versions of the Device(s) that may receive Service(s). In the event the SPL indicates a Device can only be supported at a lower level of Service than what was purchased (i.e., Hosted Log Retention or Advanced), Customer shall receive the highest supported level of Service indicated on the SPL, not to exceed the level purchased.

Service Component

The use of any enabling software as a Service Component is governed by the Agreement and, if applicable, any additional terms published with this Service Description on www.accenture.com/us-en/insights/security/legal-terms.

The Service includes the LCP Software as a Service Component. Customer's use of the LCP Software is governed by the Agreement and the following additional terms:

- Subject to Your compliance with the Agreement and during the Term of the Agreement, Accenture grants to you a non-exclusive, non-transferable right to install the LCP Software in your environment, and, additionally, the right to make a single uninstalled copy of the LCP Software for archival purposes which you may use and install for disaster-recovery purposes (i.e. where the primary installation of the LCP Software becomes unavailable for use).
- You may not, without Accenture's prior written consent, use, copy, publish, distribute, modify, reverse engineer, disassemble, decompile, sublicense, assign, or otherwise transfer the LCP Software.
- The LCP Software is provided for the Term of the Agreement; your rights to the LCP Software shall end at the termination of the Agreement, at which time, you shall immediately stop using and destroy all copies of the LCP Software.

Assistance and Technical Support

- Technical assistance for the Service(s) will be provided by Accenture as described in the Operations Manual available on the Portal.
- Notwithstanding the foregoing, if Customer is entitled to receive technical support from an authorized reseller, please refer to Customer's agreement with that reseller for details regarding such technical support, and the technical support described in the Operations Manual will not apply to Customer.

SERVICE-SPECIFIC TERMS

Changes to Subscription
If Customer has received Customer's subscription directly from Accenture, communication regarding permitted changes of Customer's subscription must be sent to SCSS.BusOps@accenture.com, unless otherwise noted in Customer's Agreement. Any notice given according to this procedure will be deemed to have been given when received. If Customer has received Customer's subscription through an authorized reseller, please contact Customer's reseller.

Use Model

Use of the Service(s) is limited to the *Enterprise Wide Model* or *Per Unit Model* as set forth in the Order Confirmation, and as further described below: Enterprise Wide Model.

- End User(s); Nodes. For Service(s) identified in the Order Confirmation as 'Enterprise Wide' ("**Enterprise Wide Service(s)**"), Customer represents and warrants 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. Enterprise Wide Service(s) entitle the End User to receive Service(s) for an unlimited quantity of Device(s) owned or used by End User, subject always to End User's Node Count Compliance as set forth below and each such Device conforming to the version requirements stated in the SPL.
- 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. Accenture may, at its discretion, but no more than once every twelve (12) months, request Customer to validate the End User(s)' Node Count to Accenture in writing.

- **Per Unit Model.**
  - For Service(s) not identified in the Order Confirmation as 'Enterprise Wide' ("**Per Unit Services**"), Accenture will provide the Service(s) to Customer commensurate with the quantity of Service(s) entitlement purchased as identified in the Order Confirmation. Per Unit Services are offered on a per Device pricing basis.
- **MEDR Model.**
  - For MEDR, Accenture will provide the MEDR Service to Customer commensurate with the quantity of entitlement purchased as identified in the Order Confirmation. Customer is required to purchase one license per each endpoint to be included in the MEDR Service ("**MEDR Endpoint**"). Minimum versions/specifications required for this service are as set forth in the Operations Manual.

Termination Due to End of Service Availability

- The Service(s) (or a portion) may be terminated upon ninety (90) days prior written notice by Accenture to Customer, in the event that the Service(s) (or a portion) are affected by Accenture's cessation of, or designation of 'end of life' of, such Service(s) (or a portion thereof). In the event that Accenture exercises this termination right, as good and valuable consideration, Accenture will credit Customer's account any prorated, unused fees received by Accenture for the impacted Service(s) (or a portion).

The Service(s) are non-cancellable by Customer, and except otherwise specified in this Service Description, payments for the Service(s) are non- refundable.

SERVICE LEVEL AGREEMENT.

SERVICE LEVEL AGREEMENTS & SERVICE CREDITS.

The service level agreements ("**SLAs**") listed below will apply to those Service(s) listed in the MSS Offerings Chart. The MSS Offerings Chart additionally details the SLA(s) applicable for each of the Service(s). Accenture's sole and exclusive obligation and Customer's sole and exclusive remedy for failure to meet the SLAs listed below shall be limited to the payment of Service Credit(s), as further described below.

- **Device Registration**.
  - The *Customer Responsibilities* set forth above must be met for Device(s) prior to Device Registration ("**Registration Requirements**").
  - Accenture will register each Device(s) upon the last of the following:

- fifteen (15) business days after completion of the Registration Requirements; or
- upon the Start Date identified in the Order Confirmation; or
- in accordance with the registration date or timeline identified in a mutually agreed upon deployment schedule. A deployment schedule created by Accenture may be required, in Accenture's sole discretion, in the event that the Service(s) require registration of ten (10) or more Device(s).

o If Accenture fails to register one or more Device(s) as required above, then Accenture will credit Customer's account for each day the deadline is missed, as follows:

- for Enterprise Wide Service(s), one (1) Service Credit for each day the deadline is missed; or
- for Per Unit Service(s) and solely with respect to a Device Block, one (1) Service Credit for each day the deadline is missed, regardless of how many Device(s) are contained within such Device Block. A "**Device Block**" refers to the unit of measure in which certain Per Unit Service(s) are purchased (e.g., a block of 2500 endpoints, a block of 10 HIDS/HIPS, a block of 150 servers of applications/OS); or
- for all other Per Unit Service(s), one (1) Service Credit for each day the deadline is missed for each Device.

- **Severe Event Notification**. For Monitoring Service(s) (as further described in the MSS Offerings Chart), Accenture will initiate contact to notify Customer of Emergency and Critical incidents (as defined in the Operations Manual) within the specified Severe Event Notification Time identified in the MSS Offerings Chart, once the determination that an Emergency and Critical incident has occurred (as specified in the Operations Manual). If Accenture does not initiate contact within the specified time, Accenture will credit Customer's account with one (1) Service Credit(s) for impacted Enterprise Wide Service(s) or one (1) Service Credit for each impacted Device Block or Device, as applicable, unless the Device(s) subject to the Emergency or Critical incident is deemed to be a "**Runaway Device**," as defined in the Operations Manual.

- **Managed Device Availability Up-Time**. For Management Service(s), Device(s) shall be available in accordance with the Managed Device Availability Up-time Percentage, as identified in the MSS Offerings Chart, of each calendar month during the Term (excluding scheduled outage, hardware/software failures, failures resulting from changes made by Customer, and circumstances beyond SOC control, as further described in the Operations Manual). If the Device(s) is not available as specified in the preceding sentence, Accenture will credit Customer's account with one (1) Service Credit for each 24-hour period, or portion thereof for which this SLA is not met. If the Device(s) 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 Accenture will not be liable for this SLA for such non-conforming Device(s).

- **Standard Changes Completion Time**. For Management Service(s), Accenture will complete Standard Changes within the Standard Changes Completion Time, as identified in the MSS Offerings Chart. If Accenture does not meet this SLA, Accenture will credit Customer's account with one (1) Service Credit.

- **Minor Changes Completion Time**. For Management Service(s), Accenture will complete Minor Changes within the Minor Changes Completion Time, as identified in the MSS Offerings Chart. If Accenture does not meet this SLA, Accenture will credit Customer's account with one (1) Service Credit.

- **Emergency Change or Assistance Response Time**. For Management Service(s), 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 MSS Offerings Chart. If Accenture does not meet this SLA, and Customer has not exceeded their contracted Emergency Change or Assistance Requests for the month as specified in MSS Offerings Chart, Accenture will credit Client's account with one (1) Service Credit.

- **SOC Infrastructure Up-Time**. SOC data storage, SOC log analysis processing, any Hosted Management Consoles, the Portal, and SOC customer communication methods (i.e., phone, email, the Portal) (together, the "**SOC Infrastructure**") shall be available in accordance with the SOC Infrastructure Up-time Percentage identified in the MSS Offerings Chart, for each calendar month during the Term (excluding scheduled outage, hardware/software failures, failures resulting from changes made by Customer, and circumstances beyond SOC control, as further described in the Operations Manual). If any or all of the SOC Infrastructure is not available as specified in the preceding sentence, Accenture will credit Customer's account with one (1) Service Credit for each 24-hour period, or portion thereof for which the SLA is not met.

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

- **Service Credits**. The process for requesting a Service Credit for an SLA failure is set forth in the Operations Manual and must be initiated by the Client within thirty (30) days of occurrence of the SLA failure. A Service Credit shall be calculated as follows:
    - For Enterprise Wide Service(s): A Service Credit shall be calculated as ten percent (10%) of the prorated daily fee payable to Accenture for the affected Enterprise Wide Service(s). For avoidance of doubt, Accenture will issue one (1) Service Credit per verified SLA failure, regardless of the number of affected Device(s).
    - For Per Unit Service(s): For Per Unit Service(s) purchased for a Device Block, a Service Credit shall be calculated as the prorated daily fee payable to Accenture for the affected Device Block, regardless of how many Device(s) within the Device Block are affected. For all other Per Unit Service(s), a Service Credit shall be calculated as the prorated daily fee payable to Accenture for the affected Device(s) (excluding any one-time fees).
    - Service Credit(s) 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.

- **Limitation of Service Credit Obligation.** Notwithstanding anything to the contrary in this Service Description, in no event will Accenture be required to credit Customer more than the value of the prorated Service(s) fees received by Accenture for the affected Service(s) for the period of time in which any SLAs were missed. Accenture's sole and exclusive obligation and Customer's sole and exclusive remedy for each respective SLA set forth in this Service Description will be limited to the issuance of Service Credit(s).

DATA PRIVACY NOTICE.

Customer may be required to supply certain business information which is necessary for Accenture to provide the Service and which may contain personally identifiable information (**"Personal Information"**), including but not limited to, names, e-mail address, IP address and contact details of designated users and contacts for the Service, Personal Information provided during configuration of the Service(s) or any subsequent service call and other Personal Information as described in the Agreement (**"Provisioning Data"**). Additionally, Customer acknowledges that in performing certain Service(s), Accenture may, on behalf of Customer, collect and process log data which may include certain source and destination IP addresses, host name, username, and policy names which may be classed as Personal Information (**"Log Data"**). Customer acknowledges that it is the controller of such Log Data and Provisioning Data, and agrees that it is will take all necessary measures to ensure that it, and all of its employees or other third parties, are aware that their Personal Information may be processed as part of the Service(s) and that those individuals have given their consent to such processing, where required. Customer will comply with its responsibilities as data controller in accordance with applicable laws and/or regulations. By providing Personal Information, Customer consents, for itself, its users and contacts, to the following: Personal Information will be processed and accessible on a global basis by Accenture, its affiliates, agents and subcontractors for the purposes of providing the Service(s), to generate statistical information about the Service(s), for internal research and development, and as otherwise described

in the Agreement, including in countries that may have less protective data protection laws than the country in which Customer or its users are located. Accenture may disclose the collected Personal Information as required or permitted by law or in response to a subpoena or other legal process. Customer understands and agrees that Accenture has no control or influence over the content of the Log Data processed by Accenture and that Accenture performs the Service(s) on behalf of Customer and that Accenture will only process the Personal Information provided by Customer in both Log Data and Provisioning Data in accordance with the instructions of Customer, provided that such instructions are not incompatible with the terms of the Agreement. Accenture will also take appropriate technical and organizational measures to protect personal information against accidental loss or destruction of, or damage to, that Personal Information, as set forth in the Security Protocols attached as **Attachment 3**.

DEFINITIONS

Capitalized terms used in this Service Description, and not otherwise defined in the Agreement, this Services Description or the Operations Manual, have the meaning given below:

"**Accenture**" means the Accenture entity named in the Order confirmation and/or its affiliates.

"Credit Request" means the notification which Customer must submit to Accenture by email with the subject line "Credit Request" (unless otherwise notified by Accenture).

"Customer" means the customer identified in the Order Confirmation.

"Operations Manual" means the Managed Security Services Operation Manual.

"**Service Component**" means certain enabling Software, hardware peripherals and associated documentation which may be separately provided by Accenture as an incidental part of a Service.

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

"**Software**" means each Accenture or third party licensor software program, in object code format, as applicable, including without limitation new releases or updates as provided hereunder.

"Online Services Terms and Conditions" means the Online Services Terms and Conditions located at or accessed through www.accenture.com/us-en/insights/security/legal-terms.

"**Term**" shall mean the term of the subscription of the Service(s) as specified in the applicable Order Confirmation.

END OF SERVICE DESCRIPTION

ATTACHMENT 1

MSS OFFERINGS CHARTS

	MSS SECURITY MONITORING SERVICES	
Feature	**Hosted Log Retention Service**	**Advanced Security Monitoring Service**
Service Use Model[1]	Per Unit or Enterprise Wide	Per Unit or Enterprise Wide
Service Level Agreement Metrics		
Device Registration	As described in the Service Level Warranties	
Severe Event Notification Time	N/A	10 minutes
SOC Infrastructure Up-Time Percentage	99.90%	99.90%
Monthly Reporting Time	by 5th business day	by 5th business day
Log Retention (duration @ SOC during Services Term only):		
Online Portal access to logs	12 months[2]	12 months[2]
Online Incident Data Retention	Service Term	Service Term
Security Incident Analysis		
Log/Alert data collection, aggregation, and normalization	X	X
Logs available for SOC Analyst inspection	X[3]	X

	MSS SECURITY MONITORING SERVICES	
Feature	**Log Retention Service**	**Advanced Security Monitoring Service**

Analyze security data and customer context in an effort to detect the following signs of malicious activity, as applicable based on the log output received from the monitored Device(s): • firewall port scans and brute force threshold exceptions •host and network intrusions or suspect traffic •connections to backdoors and Trojans •events detected by endpoint security solutions • internal systems attacking other internal systems • connect to/from customer-specified bad/blocked URLs • connections to malicious URLs (identified through parsing of web proxy data) • Emerging Threats (as defined by the Operations Manual)	N/A	X
Analyze security data and customer context in an effort to detect the following signs of malicious activity, as applicable based on the log output received from the monitored Device(s): • threats that connect to/from IP addresses or URLs that are identified by Accenture's threat intelligence capability as malicious. • anomalous traffic to/from an IP address within a registered network	N/A	X
Vulnerability Data Correlation Integration provides the ability to ingest output from customer's vulnerability scanning to provide additional context for the Services	N/A	X
Validate, assess and prioritize impact of Incident to Enterprise in accordance with processes described in the Operations Manual	N/A	X
Security Incident Escalation		
Method of Notification of Security Incidents:		
Voice (as defined in the Operations Manual), Portal, Email (per Incident or Digest)	N/A	X

	MSS SECURITY MONITORING SERVICES

Feature	Log Retention Service	Advanced Security Monitoring Service
Method of Notification of Outage Incidents:		
Voice (as defined in the Operations Manual), Portal, Email (per Incident or Digest)	N/A	X
General Service Features		
Detection and response capability updated for emerging threats	N/A	X
Daily Service Summary delivered by e-mail	N/A	X
Log/device unavailability alerting and notification[4]	X	X
Online logs may be queried by customer via the Portal	X	X
Compliance reporting available on the Portal	X	X

[1] Refer to SPL to determine which Service(s) are available in Per Unit or Enterprise Wide models, at which level of service, and for which supported technologies.
[2] Subject to Runaway Device limits per the Operations Manual.
[3] Log Retention alone performs no security analysis. However, the retained log data is automatically associated with security incidents generated by other devices under Security Monitoring service(s) and is available for SOC analyst inspection.
[4] 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.

	MSS SECURITY MANAGEMENT SERVICES
Feature	**Advanced Management IDS or IPS**
Service Use Model	Per Unit only[3]
Service Level Agreement Metrics	
Device Registration	As described in the Service Level Warranties
Managed Device Availability Up-Time Percentage	99.95%
SOC Infrastructure Up-Time Percentage	99.90%
Monthly Reporting Time	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	Accenture 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 Portal standard change request templates. For endpoints, includes basic administrative tasks on the Management Console)	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 Portal standard change request templates. Includes endpoint Anti-virus / Firewall / IPS / Application Control / Device Control / Host Integrity policy management)	Unlimited Requests

	MSS SECURITY MANAGEMENT SERVICES
Feature	**Advanced Management IDS or IPS**
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 as Exception Services)
Emergency Change or Assistance Requests	5 per calendar month[1]
Service Features	

Provide management and configuration assistance for the features listed[2]	• Policy management • Signature update • In-line configuration support • Configuration for High Availability[4]
Rule / VPN limits (per Device):	
Maximum Rules in Firewall/UTM Policy	N/A
Maximum VPN Policy (site-to-site VPNs)	N/A
Incident / Fault Management:	
Monitor Managed Device for accessibility by SOC	X

	MSS SECURITY MANAGEMENT SERVICES
Feature	**Advanced Management IDS or IPS**
Monitor Managed Device for detected fault messages[2]	X
Monitor for content update failure messages[2]	X
Respond to and troubleshoot Managed Device issues	X
Lifecycle Management - Maintenance Notification:	
Standard Maintenance	24 hours' notice
Emergency Maintenance	1 hours' notice
Reporting:	
Monthly Service Report	Available on the Portal
Visibility into current tickets, Device status, Log Outage alerts	Available on the Portal

[1] Additional available with purchase of Exception Services.
[2] Subject to the technology support of features.
[3] For Enterprise Wide Advanced Management IDS/IPS purchased prior to July 2, 2012, these same features and SLA's apply.
[4] Support of the HA feature refers explicitly to configuring that component on a Device for which the Management Service has been purchased. For avoidance of doubt, Customer must purchase the Management Service for each Device they require to be managed, regardless of whether or not the Device is configured as part of a high availability pair.

	MANAGED ENDPOINT DETECTION AND RESPONSE SERVICE	
Features	**MEDR Only**	**MEDR as Add-on to MSS Advanced Security Monitoring Service**
Service Usage Model	MEDR Model	
Managed Endpoint Detection and Response Investigation ("**MEDR Investigation**")	• An incident triage investigation is initiated when suspicious activities are detected by MEDR to determine if the activity is a threat and if the severity of suspicious activity is correct. • Performed by MSS security analysts remotely connecting to the proprietary MEDR tool and investigating host traffic.[5] • Based on the nature and type of the suspicious activity, Such MEDR Investigation may include the following activities performed using the MEDR tool: o Investigate host forensic data (memory, disk and system), network traffic and logs ("**Customer Data**") o Correlate collected findings and indicators of compromise with the Accenture global threat intelligence capability o Other remote investigation as deemed necessary by Accenture o Perform automated threat hunting using the MEDR tool • Contain known malware on individual endpoints that are discovered as part of an alert created by MEDR o	
Service Level Agreement		
	See the Offering Chart for the MSS Advanced Security Monitoring Service	
Log Retention		
	See the Offering Chart for the MSS Advanced Security Monitoring Service	
Security Incident Analysis		
	See the Offering Chart for the MSS Advanced Security Monitoring Service	

[5] **Offsite Investigation**. MEDR Investigation is performed remotely. Customer authorizes Accenture to perform any MEDR Investigation of Customer Data necessary for the Service. Accordingly, Customer acknowledges and agrees that Accenture gathers Customer Data from Customer's computer network using the MEDR tool, as well as ATP, SEDR and SEP (as applicable). Customer explicitly consents to Accenture collecting such Customer Data from Customer's computer network and Customer assumes all risk and liability in this regard and Accenture shall have no liability in this regard whatsoever.

	MANAGED ENDPOINT DETECTION AND RESPONSE SERVICE[5]
Security Incident Escalation	
	See the Offering Chart for the MSS Advanced Security Monitoring Service
General Service Features	
	See the Offering Chart for the MSS Advanced Security Monitoring Service
Additional Service Terms and Conditions	
Implementation of MEDR Tool	Customer must work with Accenture to deploy and implement the MEDR tool in the environment that will be part of the MEDR Service, in accordance with the specifications set forth in the Operations Manual.
Implementation of LCPs	Customer must work with Accenture to deploy and implement appropriate LCPs.
Remote Access	If Customer is providing the MEDR Tool (vs. using an Accenture-provided tool) Customer must provide remote access to (1) Customer's implementations of the MEDR tool and (2) necessary administrative credentials to enable Accenture to perform the MEDR Service.

	MANAGED ENDPOINT DETECTION AND RESPONSE SERVICE[5]
Customer Security Testing	• Customer must provide Accenture at least twelve (12) hours in advance of any scheduled security testing including but not limited to penetration testing, application testing, vulnerability assessments to prevent false alarms.

ATTACHMENT 2

MANAGED NETWORK FORENSICS SERVICE

SERVICE FEATURES.

*Managed Network Forensics Investigation ("**MNF Investigation**")*

Accenture's MSS security analysts will initiate an incident forensic investigation when a suspicious activity is detected by MSS in an effort to determine if the activity is a threat. MNF Investigation is performed by MSS security analysts remotely connecting to Customer-owned Network Forensics Investigation Devices (as defined below) and investigating network traffic to aid Customer in determining if the severity of suspicious activity is correctly identified.

Based on the nature and type of the suspicious activity, Accenture will attempt to perform the MNF Investigation. Such MNF Investigation may include the following activities:

- Monitoring hostile activity
- Investigating network packet capture data and network traffic logs ("**Customer Data**")
- Correlating collected findings and indicators of compromise with the Accenture global threat intelligence capability
- Other remote investigation as deemed necessary by Accenture

CUSTOMER RESPONSIBILITIES

In addition to the Customer Responsibilities in the Service Description, Customer will:

- *Network Forensics Investigation Devices("**NFID**"):*
  - The List of Accenture approved NFIDs are found in the Supported Product List available on the MSS Portal (requires login).
  - NFIDs to be covered by the Service must be appropriately deployed and configured according to the standards defined by MSS security analysts.
  - NFIDs must be online and available for MNF Investigation for Accenture to perform the Service. Customer must maintain and keep the approved NFIDs properly running and functioning. Failure to do so does not constitute a failure to deliver the Service on Accenture's part.

- *Customer Security Testing:* Customer must provide Accenture at least twelve (12) hours in advance of any scheduled security testing including but not limited to penetration testing, application testing, vulnerability assessments to prevent false alarms.

- *Customer Software and Hardware*: It is Customer's sole responsibility to maintain current maintenance and technical support contracts with Customer's software and hardware vendors for any NFID(s) affected by the Service. It is Customer's responsibility to ensure that the NFID(s) are scoped and implemented in accordance with manufacturer's suggested standards. Customer is responsible for remediation and resolution of changes to NFID(s) which negatively impact the Service or the functionality, health, stability, or performance of NFID(s).

SERVICE-SPECIFIC TERMS SERVICE CONDITIONS

- *Offsite Investigation*. MNF Investigation is performed remotely. Customer authorizes Accenture to perform any MNF Investigation of Customer Data necessary for the Service. Accordingly, Customer acknowledges and agrees that Accenture may be required to connect its computers and equipment to Customer's computer network. Customer explicitly consents to Accenture connecting its computers and equipment to Customer's computer network and Customer assumes all risk and liability in this regard and Accenture shall have no liability in this regard whatsoever.
- *Personnel*. Accenture reserves the right to assign any suitable skilled resource(s) available to provide Services. Accenture is not obligated to provide a specific Accenture resource or third-party resource.

- *Access Rights*. Customer will ensure that Accenture has access to all NFIDs necessary to complete the Service at all times. Where applicable, such access shall include appropriate user accounts to perform remote investigation of Customer Data collected by NFIDs. Customer acknowledges, understands and agrees that unauthorized access to computer systems or data, intrusion into network access points or similar activities may be prohibited by applicable local law. By agreeing to this Agreement, Customer is: (i) explicitly confirming to Accenture that it has obtained all applicable consents and authority for Accenture to deliver the Service; and (ii) giving Accenture explicit permission to perform the Service and to access and process any and all Customer Data related to the Service, including without limitation, consent to analyze network traffic in real time to detect evidence of known malicious communication patterns and traffic containing unrecognized malicious code (malware), connect to Customer's computer network, archive and retain all network traffic captured as part of Services (including to store any malware and metadata supplied by Customer, or anyone else working with or for Customer), and (iii) representing that such access and processing by Accenture does not violate any applicable law or any obligation Customer owes to a third party; and (iv) accepting sole responsibility and liability with respect to engagement of such Service. Accordingly, Customer warrants and represents that it is the owner or licensee of any network, systems, IP addresses software, appliances, code, templates, tools, policies, records, working papers, data and/or computers upon which Accenture performs the Service ("**Customer Systems**"), which may be visible through MNFIDs as Customer Data, and that Customer is authorized to instruct Accenture to perform the Service on such Customer Systems. Customer shall fully indemnify and hold harmless Accenture for any claims by any third parties with respect to the Service.

- *Service Limitation*. Applicable law or regulation(s) of the country in which the Service, including without limitation MNF Investigation, will be performed may limit or alter the scope of the Service.

ATTACHMENT 3
Data Safeguards for Customer Data

These data safeguards ("**Data Safeguards**") set forth the security framework that Customer and Accenture will follow with respect to protecting Customer Data in connection with the Agreement in place between the Parties. In the event of a conflict between these Data Safeguards and any terms and conditions set forth in the Agreement, the terms and conditions of these Data Safeguards shall prevail.

To the extent the Customer Data includes Personal Data, and taking into consideration the nature, scope and purposes of the processing of the Customer Personal Data, the implementation of and compliance with these Data Safeguards and any additional security measures set out in the Service Description are designed to provide an appropriate level of security in respect of the processing of the Customer Personal Data.

I. **Controlling Standards**. Customer and Accenture will each maintain and comply with globally applicable policies, standards and procedures intended to protect data within their own respective environments (e.g., systems, networks, facilities) and such policies will govern and control in their respective environments. For clarity, each Party will comply with the other Party's policies when accessing or operating within the other Party's environments. Each Party will provide timely notice of any changes to such policies that may materially degrade the security of the Services.

II. **Penetration Testing and Vulnerability Scanning**. At least annually, Accenture shall perform penetration and vulnerability assessments on Accenture's IT environments in accordance with Accenture's internal security policies and standard practices. Accenture agrees to share with Customer summary level information related to such tests as conducted by Accenture to the extent applicable to the Services. For clarity, as it relates to such penetration and vulnerability testing, Customer will not be entitled to (i) data or information of other customers or Customers of Accenture; (ii) test third party IT environments except to the extent Accenture has the right to allow such testing; (iii) any access to or testing of shared service infrastructure or environments, or (iv) any other Confidential Information of Accenture that is not directly relevant to such tests and the Services.

III. **Technical and Organizational Measures**. Without limiting the generality of the foregoing and subject to any other express written agreement between the Parties with respect to the Services, Accenture has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect Customer Data in its environments against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction, as follows:

1. **Organization of Information Security**

   a) **Security Ownership.** Accenture will appoint one or more security officers responsible for coordinating and monitoring the security rules and procedures.

   b) **Security Roles and Responsibilities.** Accenture personnel with access to Customer Data will be subject to confidentiality obligations.

   c) **Risk Management Program.** Accenture will have a risk management program in place to identify, assess and take appropriate actions with respect to risks related to the processing of the Customer Data in connection with the Agreement.

2. **Asset Management**

   a) **Asset Inventory.** Accenture will maintain an inventory of all media on which Customer Data is stored. Access to the inventories of each Parties' media will be restricted to that Parties' personnel authorized in writing to have such access.

b) Data Handling.

i. Accenture will classify Customer Data to help identify such data and to allow for access to it to be appropriately restricted (e.g., through encryption).

ii. Accenture will limit its printing of Customer Data to what is minimally necessary to perform services and have procedures for disposing of printed materials that contain Customer Data.

iii. Accenture will require its personnel to obtain appropriate authorization prior to storing Customer Data outside of contractually approved locations and systems, remotely accessing Customer Data, or processing Customer Data outside the Parties' facilities.

3. Human Resources Security

a) Security Training.

i. Each Party will inform its personnel about relevant security procedures and their respective roles. Each Party also will inform its personnel of possible consequences of breaching the security rules and procedures.

ii. Each Party will only use anonymous data in training.

4. Physical and Environmental Security

a) Physical Access to Facilities. Accenture will only allow authorized individuals to access Accenture facilities where information systems that process Customer Data are located.

b) Physical Access to Components. Accenture will maintain records of the incoming and outgoing media containing Customer Data, including the kind of media, the authorized sender/recipients, date and time, the number of media, and the types of Customer Data they contain.

c) Protection from Disruptions. Accenture will use a variety of industry standard (e.g., ISO 27001, CIS Sans 20, and/or NIST Cyber-Security Framework, as applicable) systems to protect against loss of data due to power supply failure or line interference.

d) Component Disposal. Accenture will use industry standard (e.g., ISO 27001, CIS Sans 20, and/or NIST Cyber-Security Framework, as applicable) processes to delete Customer Data when it is no longer needed.

5. Communications and Operations Management

a) Operational Policy. Accenture will maintain security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data.

b) Mobile Device Management (MDM). Accenture will maintain a mobile device policy that:

i. Enforces device encryption;

ii. Protects and limits use of Customer Data accessed or used on a mobile device; and

iii. Prohibits enrollment of mobile devices that have been "jail broken."

c) Data Recovery Procedures. Accenture will

i. Have specific data recovery procedures in place designed to enable the recovery of Customer Data being maintained in its systems.

ii. Review its data recovery procedures at least annually.

iii. Log data restoration efforts with respect to its systems, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process.

d) Malicious Software. Accenture will have anti-malware controls to help avoid malicious software gaining unauthorized access to Customer Data, including malicious software originating from public networks.

e) Data Beyond Boundaries. Accenture will

i. Encrypt Customer Data that it transmits over public networks.

ii. Protect Customer Data in media leaving its facilities (e.g., through encryption).

iii. Implement automated tools where practicable to reduce the risks of misdirected email, letters, and / or faxes.

f) Event Logging.

i. For systems containing Customer Data, Accenture will log events consistent with its stated policies or standards.

6. Access Control

a) Access Policy. Accenture will maintain a record of security privileges of individuals having access to Customer Data via its systems.

b) Access Authorization. Accenture will

i. Maintain and update a record of personnel authorized to access Accenture systems that contain Customer Data.

ii. Where responsible for access provisioning, each party will promptly provision authentication credentials.

iii. Deactivate authentication credentials where such credentials have not been used for a period of time (such period of non-use not to exceed six months).

iv. Deactivate authentication credentials upon notification that access is no longer needed (e.g. employee termination, project reassignment, etc.) within two business days.

v. Identify those personnel who may grant, alter or cancel authorized access to data and resources.

vi. Ensure that where more than one individual has access to systems containing Customer Data, the individuals have unique identifiers/log-ins.

c) Least Privilege.

i. Technical support personnel will only be permitted to have access to Customer Data when needed.

ii. Accenture will restrict access to Customer Data within its systems to only those individuals who require such access to perform their job function.

iii. Accenture will limit access to Customer Data within its systems to only that data minimally necessary to perform the services.

iv. Accenture will support segregation of duties between its environments and between key roles.

d) Integrity and Confidentiality. Accenture will instruct its personnel to disable administrative sessions when leaving premises or when computers are otherwise left unattended.

e) Authentication.

i. Accenture will use industry standard (e.g., ISO 27001, CIS Sans 20, and/or NIST Cyber-Security Framework, as applicable) practices to identify and authenticate users who attempt to access its information systems.

ii. Where authentication mechanisms are based on passwords, Accenture will require that the passwords are renewed regularly.

iii. Accenture will ensure that de-activated or expired identifiers are not granted to other individuals.

iv. Accenture will monitor repeated attempts to gain access to its information systems using an invalid password.

v. Accenture will maintain industry standard (e.g., ISO 27001, CIS Sans 20, and/or NIST Cyber-Security Framework, as applicable) procedures to deactivate passwords that have been corrupted or inadvertently disclosed.

vi. Accenture will use industry standard (e.g., ISO 27001, CIS Sans 20, and/or NIST Cyber-Security Framework, as applicable) password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, as well as during storage.

f) Multi Factor Authentication. Accenture will implement Multi-Factor Authentication for internal access and remote access over virtual private network (VPN) to its systems.

7. Network and Application Design and Management. Accenture will

a) Have controls to avoid individuals gaining unauthorized access to Customer Data in its systems.

b) Use network-based data loss prevention to monitor or restrict movement of sensitive data in its systems.

c) Use network-based web filtering to prevent access to unauthorized sites.

d) Use network intrusion detection and / or prevention.

e) Use secure coding standards.

f) Scan for and remediate OWASP vulnerabilities.

g) If applicable and to the extent technically possible, the parties will work together to limit the ability of Accenture personnel to access non-Customer and non-Accenture environments from the Customer systems.

h) Maintain up to date server and network device security configuration standards.

i) Scan its environments to ensure identified configuration vulnerabilities have been remediated.

8. Patch Management

a) Accenture will have a patch management procedure that deploys security patches for systems used to process Customer Data that includes:

i. Defined time allowed to implement patches (not to exceed 90 days for all patches); and

ii. Established process to handle emergency patches in a shorter time frame.

b) Each party agrees that no software or hardware that is past its End of Life (EOL) will be used in the scope of services without a risk management process for such items.

9. Workstations

a) Accenture will implement controls for all workstations it provides that are used in connection with service delivery/receipt incorporating the following:

i. Users cannot change or modify default security controls

ii. Encrypted hard drive

iii. Software agent that manages overall compliance of workstation and reports a minimum on a monthly basis to a central server

iv. Patching process to ensure workstations are current on all required patches

v. Ability to prevent unapproved software from being installed

vi. Antivirus with a minimum weekly scan

vii. Firewalls installed

10. Information Security Breach Management

a) Security Breach Response Process. Each Party will maintain a record of its own security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the process for recovering data.

b) Service Monitoring. Each Party's security personnel will review their own logs as part of their security breach response process to propose remediation efforts if necessary.

11. Business Continuity Management

a) Each Party will maintain emergency and contingency plans for the facilities in which the Parties' information systems that process Customer Data are located.

b) Each Party's redundant storage and procedures for recovering data will be designed to reconstruct Customer Data stored by a Party in its original state from before the time it was lost or destroyed.