ACCENTURE MANAGED EXTENDED DETECTION & RESPONSE (MxDR)

Revision Date: October 1, 2021

This Service Description, together with any documents incorporated by reference ("**Service Description**") describes the service features, components and terms for Accenture's **MANAGED EXTENDED MONITORING & DETECTION SERVICES** (each an "**MxDR Service**", or collectively, the "**MxDR Services**") and is subject to the terms of the Agreement.

1. DEFINITIONS.

Capitalized terms used in this Service Description, and not otherwise defined in the Agreement (as applicable), have the meaning given below:

"**Accenture**" shall mean the Accenture entity named in the Order confirmation and/or its Affiliates.

"**Acceptable Use Policy**" shall mean Accenture's Acceptable Use Policy published by Accenture at https://www.accenture.com/us-en/support/security/legal-terms-managed-security (or succesor URL).

"**AER Tool**" shall mean either a Client-owned Endpoint Detection and Response (EDR) tool, or an EDR tool provided by Accenture.

"**Agreement**" shall mean collectively the Order Confirmation, this Service Description, and the Security Terms (in that order of precedence).

"**Affiliate**" shall mean an entity controlled by, under common control with, or controlling a party, where control is denoted by having (directly or indirectly) more than 50% of the voting power (or equivalent) of the applicable entity.

"**Block of Device(s)**" shall mean Device(s) that are purchased in multiples as specified in the Order Confirmation.

"Credit Request" shall mean a notification which Client must submit to Accenture by email with the subject line "Credit Request" (unless otherwise notified by Accenture).

"Client" shall mean the Client identified in the Order Confirmation.

"**Device(s)**" shall mean an endpoint(s), security device(s) and/or product(s) owned or licensed by the Client that is specified in the Supported Product List ("**SPL**") and that receives MxDR Services e.g. servers, workstations, network firewalls, intrusion detection sensors, cloud based applications and products.

"**Force Majeure Event**" shall mean any fire, flood, earthquake, epidemic or pandemic, act of nature, act of God, general strike, riot, war, act of terrorism or other unforeseen causes beyond a party's control and that prevents performance of a party's obligations.

"**Log Collection Platform**" or "**LCP**" shall mean the log collection MxDR Service Component described in this Service Description.

"Security Terms" shall mean Accenture's security terms and conditions published by Accenture at https://www.accenture.com/us-en/support/security/legal-terms-managed-security (or succesor URL), unless otherwise specified in the Order Confirmation.

"**Meter**" shall mean the applicable unit(s) of measurement by which Accenture offers the applicable MxDR Service, as further described in this Service Description.

"MxDR Operations Manual" shall mean Accenture's Managed Extended Detection and Response Operation Manual, which provides information on accessing and/or the delivery of the MxDR Service purchased by Client.

"**MxDR Portal**" shall mean Accenture's web portal through which Client may access and use the MxDR Services and which is made available by Accenture to Client for use during the Subscription Term.

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

"**MxDR Service Delivery Lead**" shall mean Accenture's point of contact available to Client for questions, training and resolution of service delivery issues.

"**Node**" shall mean a virtual or physical unique network address, such as an Internet protocol address.

"**Order Confirmation**" shall mean a signed services order confirmation and/or statement of work that confirms the Client's purchase of its Subscription to an MxDR Service. The specific quantity and Meter applicable to the MxDR Service purchased by Client shall be as indicted in the Order Confirmation.

"**Pack of Units**" shall mean a unit of measure in which an MxDR Service may be purchased by Client as further specified in the Order Confirmation. A "Pack of Units" is available for purchase by Client as follows: (i) Small Pack of Units – up to 4 Units; (ii) Medium Pack of Units – 5 or 6 Units; or (iii) Large Pack of Units – 7 to 10 Units. Each "**Unit**" comprises of 1 Device or 1 Block of Device(s).

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

"**Service Provider**" shall mean a service provider authorized by Accenture to deliver the MxDR Services as an outsourced service to its end user client.

"**SOC Infrastructure**" shall mean individually or collectively, SOC(s) (as defined below) data storage, SOC(s) log analysis processing, any Hosted Management Consoles, the MxDR Portal, and SOC(s) / Client communication methods (i.e., phone, email, the MxDR Portal).

"**Software**" shall mean each Accenture and/or third-party licensor software program, in object code format, as applicable, including without limitation new releases or updates.

"**Subscription**" shall mean, a right to access, use and/or benefit from an MxDR Service during the Subscription Term subject to the terms of the Agreement.

"**Subscription Term**" shall mean the term of the Subscription of the MxDR Service as specified in the Order Confirmation.

2. SERVICE OVERVIEW.

The MxDR Services, comprise one or more of the following services, depending on the MxDR Service purchased by Client as indicated in the Order Confirmation and as further described in this Service Description.

- **Advanced Security Monitoring and Detection Service**, provides 24x7 real-time security monitoring, analysis and reporting, and early warning intelligence. The Advanced Security Monitoring and Detection Service is 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 Client's critical infrastructure.
- **Hosted Log Management 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 Service**, provides 24x7 alarm and incident management, lifecycle management support and emergency access to security practitioners.
- **Advanced Endpoint Response Service**, provides additional investigation of identified suspicious activities utilizing an AER Tool in an effort to provide enhanced context, refine incident severity and proactive response (as applicable) and is available in the following two ways:
  - **Add-on to Advanced Security Monitoring and Detection Service**. Available for Clients that have subscribed to the Advanced Security Monitoring and Detection Service (*separate purchase required*).
  - **Advanced Endpoint Response Service on a standalone basis**. Available to Clients that do not have a subscription to the Advanced Security Monitoring and Detection Service and have an Endpoint Protection product ("**EPP**") running on their endpoints that is supported for the Advanced Security Monitoring and Detection Service, as specified in the SPL.
- **Advanced Network Response Service,** provides additional investigation of identified suspicious activities in an effort to provide enhanced context, refine incident severity and proactive response (as applicable) and is available for Clients that have subscribed to the Advanced Security Detection and Monitoring Service (*separate purchase required*) and own or license an Accenture-approved Network Forensics Investigation Devices (as defined below).

3. TECHNICAL/BUSINESS FUNCTIONALITY AND CAPABILITIES.

3.1 **MxDR Services Features**. The MxDR Services are further described in the MxDR Services offering charts set forth in Attachment 1 of this Service Description (each an "**MxDR Services Offering Chart**"). In addition to the MxDR Service Offering Chart, the following service features apply to the MxDR Services:

3.1.1. **MxDR Portal**. Client shall have access to and use of the MxDR Portal, which is made available by Accenture to Client for use solely with respect to the MxDR Services during the Subscription Term. Notwithstanding anything to the contrary in the Security Terms, Accenture may provide Client with information and notices about the MxDR Services electronically, including via email, through the MxDR Portal, or through a web site that Accenture identifies. Notice is given as of the date it is made available by Accenture.

3.1.2. **MxDR Operations Manual**. The MxDR Operations Manual, which is available via the MxDR Portal, provides further details regarding Client's use and access to the MxDR Services, including additional Client responsibilities which may be applicable to the MxDR Services. Accenture will use commercially reasonable efforts to give Client 30 days' notice through the MxDR Portal of any material change to the MxDR Operations Manual.

3.1.3 **Security Operations Centers**. All MxDR Services are performed remotely from Security Operations Centers ("**SOC(s)**").

3.1.4 **Scheduled Outages**. Accenture will, from time to time, schedule regular maintenance on the SOC Infrastructure or on Device(s) that are subject to Device(s) management MxDR Services (as indicated in the applicable MxDR Services Offering Chart), requiring a maintenance outage. The protocol for any such maintenance outage is described in the MxDR Operations Manual ("**Scheduled Outage**").

3.2 **Hosted Management Consoles**. Client may renew the use of Hosted Management Consoles located in Accenture's environment for centralized management of certain Device(s) receiving MxDR Services. Client is responsible for obtaining any required license(s) from the technology vendor to allow applicable use of the Hosted Management Console (Note: Hosted Management Console is no longer available for new purchases).

3.3 **Supported Platforms and Technical Requirements.** Supported platforms for the MxDR Services are listed in the MxDR Portal. Hardware requirements can be found in the LCP deployment guide (and such other applicable guide based on Client's purchase) distributed by Client's MxDR Service Delivery Lead ("**LCP Deployment Guide**"). The SPL describes the supported versions of the Device(s) that may receive MxDR Services.

3.4 **Technical Support**. Technical assistance for the MxDR Services will be provided by Accenture as further specified in the MxDR Operations Manual. Notwithstanding the foregoing, in the event that Client is entitled to receive technical support from an authorized reseller or Service Provider, Client must refer to Client's agreement with such authorized reseller or Service Provider for details regarding such technical support, and the technical support described in the MxDR Operations Manual shall not apply to Client.

4. MxDR SERVICE COMPONENT LICENSE, INTERNAL USE & RESTRICTIONS.

4.1 **MxDR Service Component License**. The use of any enabling software as an MxDR Service Component is governed by this Service Description together with the MxDR Operations Manual and, if applicable, any additional terms published with this Service Description at https://www.accenture.com/us-en/support/security/legal-terms-managed-security (collectively the "**MxDR Service Component License**"). For the avoidance of doubt, Open Source Software included in a MxDR Service Component is not licensed under the terms of the MxDR Service Component License, but is instead under a license meeting the 'Open Source Definition' (as defined by the Open Source Initiative) or any substantially similar license (including Creative Commons licenses), and Client's use of the Open Source Software is subject to the terms of each such applicable Open Source Software license(s).

4.2 **LCP Installation**. The MxDR Services may include an LCP as a MxDR Service Component. Further details on the LCP can be found in the LCP Deployment Guide. Accenture grants to Client a non-exclusive, non-transferable right to install the LCP on the Device(s), and additionally, the right to make a single uninstalled copy of the LCP for archival purposes which Client may use and install for disaster-recovery purposes (i.e. where the primary installation of the LCP becomes unavailable for use). Client shall be solely responsible for successfully installing an LCP on Client's Device(s) and establishing the necessary network access to allow the SOC(s) to remotely manage the LCP, and to allow the LCP to collect, compress, encrypt, and send event log data to the SOC(s) for analysis and reporting from the Device(s). Client 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 LCP Deployment Guide). In addition, for select logging technologies (as

specified in the SPL), Client may also be required to install collectors on Client provided systems (other than the LCP) and enable access to/from the LCP. Client acknowledges and agrees that Accenture must have access to event log data from the Device(s) in a format that is compatible with Accenture's collectors and in some cases this may require configuration changes to the Device(s). Client agrees to make any necessary changes to the configuration of the Device(s), as requested by Accenture, to conform with the supported format. Client's rights to the LCP and collectors shall automatically end upon the expiration or earlier termination of the Subscription, at which time, Client shall immediately stop using and destroy all copies of the LCP and collectors.

4.3 **Internal Use Only**. Client's Subscription to access and use the MxDR Services and/or an MxDR Service Component during the Subscription Term is on a limited, non-exclusive, non-transferable basis, solely for Client's internal business purposes and strictly in accordance with the terms of the Agreement, including without limitation: (i) use of the MxDR Services and/or an MxDR Service Component in accordance with the Acceptable Use Policy; and (ii) use of the MxDR Services up to the Meter amount for which Client purchased such MxDR Services (as specified in the Order Confirmation). Client's Affiliates may use the MxDR Services: (i) solely for Client's and/or Client's Affiliates' internal business purpose; (ii) up to the Meter amount for which Client purchased the applicable MxDR Service; and (iii) in accordance with the Agreement. Client assumes full responsibility for all actions in connection with such use of the applicable MxDR Service by Client's Affiliates.

4.4 **Restrictions**. Client shall not, and may not cause or permit others to: (i) modify, make derivative works of, disassemble, decompile, reverse engineer, reproduce, republish or copy any part of the MxDR Services and/or an MxDR Service Component), unless permitted by applicable law for interoperability purposes; (ii) access or use the MxDR Services and/or an MxDR Service Component to build or support, directly or indirectly, products or services competitive to Accenture; or (iii) license, sell, transfer, assign, distribute, outsource, permit timesharing or service bureau use of, commercially exploit, or make available the MxDR Services and/or an MxDR Service Component to any third party except as permitted by the Agreement.

5. SERVICES METER.

The MxDR Services are available for purchase by Client either on an "**ENTERPRISE WIDE**" or "**PER UNIT**" basis as further described below:

5.1 **MxDR Services Meter - Enterprise Wide**. Client's purchase of an MxDR Service on an Enterprise Wide basis entitles Client to receive the applicable MxDR Service subject to the following:

(i) the applicable Device(s) are owned or used by Client (and/or any Affiliate of Client) and conform to the Device(s) version requirements specified in the SPL;

(ii) Client maintains the required Node Count (as specified in the Order Confirmation) during the Subscription Term. The term "**Node Count**" shall mean the total number of Nodes owned or used by Client (and/or any Affiliate of Client) at the time of Client's purchase and specified in the Order Confirmation, regardless of whether each such Node directly interacts with the applicable MxDR Service. If Client is a Service Provider and purchases an MxDR Service on an Enterprise Wide basis for the benefit of its end user client, the quantity of the MxDR Service purchased must reflect the total Node Count for the applicable end user client receiving outsourced services from Service Provider; and

(iii) if, at any time during the Subscription Term, Client's Node Count increases by more than 5% over the Node Count specified in the Order Confirmation, Client agrees to promptly, and in any case no later than 30 days following the increase in Node Count, purchase an additional quantity of the MxDR Service to become compliant with such increased Node Count. In the event that Client fails to purchase such additional quantity of the MxDR Service, Accenture reserves the right to suspend the provision of the MxDR Service upon written notice to Client. Accenture may, at its discretion, but no more than once every 12 months, request Client to validate the Node Count to Accenture in writing.

5.2 **MxDR Services Meter - Per Unit**. Client's purchase of an MxDR Service on a Per Unit basis entitles Client to receive the MxDR Service solely for quantity of Device(s) specified in the Order Confirmation subject to the Device(s) being owned or used by Client (and/or any Affiliate of Client and such Device(s) conform to the Device(s) version requirements specified in the SPL. Per Unit MxDR Services are available on a per Device(s), Block of Device(s) or Pack of Units basis.

5.3 **Services Meter – Advanced Endpoint Response.** Client's purchase of the Advanced Endpoint Response Service shall entitle Client to receive the Advanced Endpoint Response Service specifically for quantity of Client endpoints ("**AER Endpoint**") specified in an Order Confirmation. Client is required to purchase 1 quantity of the Advanced Endpoint Response Service for each AER Endpoint to be included in the Advanced Endpoint Response Service. Minimum

versions/specifications required for the Advanced Endpoint Response Service are as specified in the MxDR Operations Manual.

6. SERVICE LEVEL AGREEMENT

Subject always to Client meeting its responsibilities as specified in the '**Client Responsibilities**' section, the following service levels (each a "**Service Level**" and collectively the "**Service Levels**") shall apply to the MxDR Services as indicated in the applicable MxDR Services Offering Chart. Accenture's sole and exclusive obligation and Client's sole and exclusive remedy for Accenture's failure to meet a Service Level shall be limited to the payment of a Service Credit, as described below:

6.1 **Device(s) Registration Service Level**. Subject to Client providing Accenture with all technical and license information for each Device(s) ("**Registration Requirements**") prior to such Device(s) being recognized by and connected to the applicable MxDR Service, Accenture shall register each Device(s) ("**Device(s) Registration**") upon the last of the following: (i) the start date of the MxDR Service as specified in the Order Confirmation; (ii) 15 business days after receipt by Accenture of the Registration Requirements from Client; or (iii) 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 MxDR Service requires registration of 10 or more Device(s).

Accenture will credit Client's account for each day Device Registration is missed, as follows: (i) **Enterprise Wide Services** - 1 Service Credit for each day Device Registration is missed; or (ii) **Per Unit Services** - 1 Service Credit for each day Device Registration is missed for the Device(s), Block of Device(s) or Pack of Units, as applicable.

6.2 **Severe Event Notification Service Level**. Accenture shall initiate contact to notify Client of an Emergency and Critical Incident (as defined in the MxDR Operations Manual) within 10 minutes following a determination by Accenture that an Emergency and Critical Incident has occurred.

Accenture will credit Client's account if Accenture fails to initiate contact within the specified time pursuant to the Severe Event Notification Service Level as follows: (i) **Enterprise Wide Services** - 1 Service Credit for each day the deadline is missed; or (ii) **Per Unit Services** - 1 Service Credit for each day the deadline is missed for the Device(s), Block of Device(s) or Pack of Units, as applicable; unless the Device(s) that is subject to the Emergency or Critical incident is deemed to be a Runaway Device (as defined in the MxDR Operations Manual).

6.3 **SOC Infrastructure Up-Time Service Level**. SOC Infrastructure shall be available 99.90% during each calendar month during the Subscription Term (excluding Scheduled Outage, hardware/software failures, failures resulting from changes made by Client, and circumstances beyond the reasonable control of Accenture, as further described in the MxDR Operations Manual).

Accenture will credit Client's account, if the SOC Infrastructure is not available pursuant to the SOC Infrastructure Up-Time Service Level with 1 Service Credit for each twenty four (24) hour period, or portion thereof for which the SOC Infrastructure Up-Time Service Level is not met.

6.4 **Device(s) Availability Up-Time Service Level**. Device(s) shall be available in accordance with the Device Availability Up-time Percentage specified in the applicable MxDR Service Offerings Chart, of each calendar month during the Subscription Term (excluding Scheduled Outage, hardware/software failures, failures resulting from changes made by Client, and circumstances beyond SOC control, as further described in the MxDR Operations Manual).

Accenture will credit Client's account, if the Device(s) is not available pursuant to the Device(s) Availability Up-Time Service Level with 1 Service Credit for each twenty four (24) hour period, or portion thereof for which the Device(s) Availability Up-Time Service Level is not met. Client acknowledges and agrees that in the event that 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), Accenture shall not be liable for meeting the Device(s) Availability Up-Time Service Level for such non-conforming Device(s).

6.5 **Standard Changes Completion Time Service Level**. Accenture will complete Standard Changes within the Standard Changes Completion Time specified in the applicable MxDR Service Offerings Chart.

Accenture will credit Client's account with 1 Service Credit in the event that Accenture fails to complete the Standard Changes within the Standard Changes Completion Time Service Level.

6.6 **Minor Changes Completion Time Service Level**. Accenture will complete the Minor Changes within the Minor Changes Completion Time specified in the applicable MxDR Service Offerings Chart.

Accenture will credit Client's account with 1 Service Credit in the event that Accenture fails to complete the Minor Changes within the Minor Changes Completion Time Service Level.

6.7 **Emergency Change or Assistance Response Time Service Level**. In the event that an emergency change request or other emergency assistance is required, a SOC engineer will be made available to commence work on or assist with such request or assistance in accordance with the timeline specified in the applicable MxDR Service Offerings Chart.

Accenture will credit Client's account with 1 Service Credit in the event that Accenture fails to meet the Emergency Change or Assistance Response Time Service Level provided that Client has not exceeded their contracted Emergency Change or Assistance Requests for the applicable month as indicated in applicable MxDR Service Offerings Chart.

6.8 **Monthly Reporting Service Level**. Accenture shall provide the monthly report(s) (as specified in the MxDR Operations Manual), to Client prior to the end of the 5th business day following the end of each calendar month.

Accenture will credit Client's account with 1 Service Credit in the event that Accenture fails to provide the monthly report(s) pursuant to the Monthly Reporting Service Level.

6.9 **Service Level Limitation**. Notwithstanding anything to the contrary in the Security Terms, Accenture shall have no liability whatsoever (including without limitation, issuing any Service Credits) in the event that Accenture's failure to deliver an MxDR Service or to meet a Service Level is attributable to Client's (or Client's third-party vendor's/service provider's): (i) failure to perform any of its responsibilities set forth in the Agreement; (ii) acts, errors, omissions, or breaches of the Agreement; (iii) willful misconduct or violations of law; and/or (iv) any Force Majeure event.

6.10 **Service Credit Calculation.** A Service Credit shall be calculated as 10% of the prorated daily fee received by Accenture for the affected MxDR Service. For avoidance of doubt, Accenture will issue 1 Service Credit per verified Service Level failure, regardless of the number of affected Device(s).

6.11 **Service Credit Limitation.** Notwithstanding anything to the contrary in the Security Terms, in no event will Accenture be required to credit Client more than the value of the prorated MxDR Service fees received by Accenture for the affected MxDR Service for the period of time in which any Service Levels were missed. Service Credits will first be applied towards Client's next invoice due for the applicable MxDR Service during the Subscription Term, or if no additional invoices are due for such MxDR Service, shall be provided as a payment.

6.12 **Requesting Service Credits.** The process for requesting a Service Credit in the event of Accenture not meeting a Service Level is specified in the MxDR Operations Manual and must be initiated by Client within 30 days of Accenture's failure to meet the applicable Service Level.

7. SUBSCRIPTION TERM.

7.1 **Subscription Term**. Client's Subscription Term shall commence on the '**Start Date**' and automatically end on '**End Date**' as specified in the Order Confirmation, even if, no Device(s) undergo Device Registration or receive MxDR Services during the Subscription Term.

7.2 **Subscription Changes**. Communication regarding permitted changes of Client's Subscription must be sent to MDR.BusOps@accenture.com. Any notice given according to this procedure shall be deemed to have been given when received by Accenture. In the event that Client has purchased its Subscription from an Accenture authorized reseller ("**Reseller**") or Service Provider, Client is required to contact the Reseller or Service Provider (as applicable).

7.3 **End of Life**. Each MxDR Service may be terminated (in whole or in part) by Accenture upon 90 days prior written notice to Client, in the event that such MxDR Service (in whole or in part) is affected by Accenture's cessation of, or designation of 'End of Life' of, such MxDR Service (in whole or in part). In the event that Accenture exercises this termination right, as good and valuable consideration, Accenture will credit Client's account any prorated, unused fees received by Accenture for the MxDR Service (in whole or in part).

8. CONSENT & AUTHORIZATION.

Client acknowledges 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. Accordingly, Client is: (i) explicitly confirming to Accenture that it has obtained all applicable consents and authority for Accenture to deliver the MxDR Services; and (ii) giving Accenture explicit permission to perform the MxDR Services and to access and process any and all Client Data related to the MxDR Services, 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 Client'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 MxDR Services (including to store any malware and metadata supplied by Client, or anyone else working with or for Client), and (iii) representing that such access and processing by Accenture does not violate any applicable law or any obligation Client owes to a third party; and (iv) accepting sole responsibility and liability with respect to engagement of such MxDR Services. Accordingly, Client 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 MxDR Services ("**Client Systems**"), which may be visible as Client Data in connection with the MxDR Services, and that Client is authorized to instruct Accenture to perform the MxDR Services on such Client Systems. Client shall fully indemnify and hold harmless Accenture for any claims by any third parties related to the MxDR Services.

9. CLIENT RESPONSBILITIES.

In addition to any Client obligations and requirements specified in the Security Terms, the following is a non-exhaustive list of Client obligations and responsibilities (collectively "**Client Responsibilities**") necessary for Accenture to deliver the MxDR Services and for Client to access and use of the MxDR Services. Accordingly, Client acknowledges and agrees that: (i) Accenture's ability to perform the MxDR Services during the Subscription Term is be subject to Client meeting all Client Responsibilities during the Subscription Term; and (ii) Accenture shall have no liability whatsoever for any failure to perform the MxDR Services if such failure arises out of Client's act or omission inconsistent with the Client Responsibilities which impede Accenture's ability to perform the MxDR Services. Without prejudice to the foregoing, any such failure to perform the MxDR Services by Accenture due to the foregoing shall not postpone or delay the Subscription Term nor be deemed a breach of the Agreement:

9.1 **Reasonable Assistance**. Client must provide reasonable assistance to Accenture, including, but not limited to, providing access to adequate personnel, technical and license information related to the MxDR Services as may be reasonably requested by Accenture, and to enable Accenture to perform the MxDR Services. Where applicable to the MxDR Services, Client must provide Accenture remote access to the Device(s) and necessary administrative credentials to enable Accenture to perform the MxDR Services.

9.2 **Accurate Information**. Client must provide Accenture with accurate and up-to-date information, including, the name, email, landline and mobile number(s) for all designated, authorized Client points of contact who will be provided access to the MxDR Portal. Client must provide the name, email, and phone number(s) for Client's installation and security points of contact. Client is responsible for its data, and Accenture does not endorse and has no control over what Client submits while using the MxDR Services. Client assumes full responsibility to back-up and protect Client Data against loss, damage, or destruction.

9.3 **Client's Outage**. Client must provide Accenture at least 12 hours advance notice of any scheduled outage (maintenance), network, or system administration activity that would affect Accenture's ability to deliver the MxDR Services.

9.4 **Daily Service Summary**. Client shall review the daily applicable MxDR Service summary to understand the current status of applicable MxDR Service delivered and actively work with Accenture to resolve any tickets requiring Client input or action.

9.5 **Device Maintenance & Management.** Client shall be solely responsible for: (i) maintaining its current maintenance and technical support contracts with Client's third-party vendors ("**Vendors**") for any Device(s) receiving the MxDR Services; (ii) ensuring any Device(s) receiving MxDR Services conform to the version requirements stated in the SPL; (iii) interacting with Device(s) Vendors to ensure that the Device(s) are scoped and implemented in accordance with Vendors' suggested standards; (iv) interacting with Device(s) Vendors regarding the resolution of any issues related to Device(s) scoping, feature limitations or performance issues; (v) remediation and resolution of changes to Device(s) which negatively impact the MxDR Services or the functionality, health, stability, or performance of Device(s). Accenture may charge additional fees in the event that Client requires Accenture's assistance for remediation or resolution activities.

9.6 **Reporting.** Client acknowledges and agrees that in the course of delivering the MxDR Services, 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 Client is subject to in one of more territories in which Client operates. Accordingly, Client shall remain solely responsible for all such reporting requirements and Accenture shall have no liability in this regard whatsoever.

10. OUT OF SCOPE.

10. 1 **General**. Anything not specifically described in this Service Description is out of scope and is not included in the MxDR Services. Client acknowledges and agrees that Accenture does not guarantee or otherwise warrant that the MxDR Services,

or Accenture's recommendations and plans made by Accenture as a result of that MxDR Services, will result in the identification, detection, containment, eradication of, or recovery from all of Client's System threats, vulnerabilities, malware, malicious software, or other malicious threats. Client agrees not to represent to anyone that Accenture has provided such a guarantee or warranty. Client further acknowledges and agrees that Accenture's ability to perform the MxDR Services may be limited due to applicable laws and/or regulation(s).

10.2 **Exception Services**. From time to time, Client may request and Accenture may provide, certain services not currently described in this Service Description ("**Exception Services**"). Accordingly, the description and fees for any Exception Services must be mutually agreed in writing.

10.3 **Litigation Support Services.** Litigation Support Services are explicitly excluded from the MxDR Services specified in this Service Description. Although the parties acknowledge that the MxDR Services may be sought by Client at the direction of Client's legal counsel, it is neither Accenture's nor Client's intention for Accenture to perform Litigation Support Services. In the event that Accenture is compelled to perform any Litigation Support Services, Client and Accenture agree as follows, regardless of whether such Litigation Support Services are sought directly by Client or by a third party, and notwithstanding any conflict with other terms:

10.3.1 the then-current hourly rate shall 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;

10.3.2 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; and

10.3.3 Client 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 Client has engaged Accenture to provide the MxDR Services, regardless of fault.

This section shall survive the expiration or earlier termination of the Subscription Term.

10.4 **Other Services**. Unless otherwise specified in this Service Description, the following services are out of scope for the purposes of the MxDR Services: (i) incident response services for the Client systems; (ii) remediation activities; (iii) quality assurance or review of any implementation of mitigations or recommendations by or on behalf of Client; (iv) penetration testing; (v) vulnerability scanning; (vi) obtaining the technical architecture diagram of the Client systems and validate such Client systems; (vii) installation of software unless expressly authorized by the Client in writing as part of its operational change management processes, and which may require additional terms and conditions to be agreed; (viii) implementation of available Device(s) updates/patches from third party vendor; (ix) representing Client in any audit or compliance assessments of relevant security controls; (x) any activity which Accenture reasonably determines would breach applicable law or infringe the rights of a third party; and/or (xi) the investigation, observation, monitoring, detection or analysis of Client's OT Environment; (xii) any direct interaction (e.g. physical or remote manipulation) with Client's OT Environment.

11. DATA PRIVACY

11.1 Client may be required to supply certain business information which is necessary for Accenture to provide the MxDR Services 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 MxDR Services, Personal Information provided during configuration of the MxDR Services or any subsequent service call and other Personal Information as described in the Agreement (**"Provisioning Data"**). Additionally, Client acknowledges that in performing certain MxDR Services, Accenture may, on behalf of Client, 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"**).

11.2 Client acknowledges that it is the controller of 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 MxDR Services and that those individuals have given their consent to such processing, where required. Client will comply with its responsibilities as data controller in accordance with applicable laws and/or regulations. By providing Personal Information, Client 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 MxDR Services, to generate statistical information about the MxDR Services, 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 Client 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. Client 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 MxDR Services on behalf of Client and that Accenture will only process the Personal Information provided by Client in both Log Data and Provisioning Data in accordance with the instructions of Client, 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 Attachment 2.

accenture

ATTACHMENT 1
MxDR Services Offering Charts

1. ADVANCED SECURITY MONITORING AND DETECTION SERVICE	
SERVICE FEATURE	**DESCRIPTION**
Services Meter	Per Unit or Enterprise Wide[1]
SERVICE LEVEL AGREEMENT	
Device Registration	As described in the Service Level Agreement
Severe Event Notification	As described in the Service Level Agreement
SOC Infrastructure Up-Time	As described in the Service Level Agreement
Monthly Reporting	As described in the Service Level Agreement
LOG RETENTION (DURATION THE SUBSCRIPTION TERM ONLY):	
Online MxDR Portal access to logs	12 months[2]
Online Incident Data Retention	Subscription Term
SECURITY INCIDENT ANALYSIS	
Log/Alert data collection, aggregation, and normalization.	X
Logs available for SOC Analyst inspection.	X
Analyze security data and Client 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 Client-specified bad/blocked URLs. ▪ connections to malicious URLs (identified through parsing of web proxy data). ▪ Emerging Threats (as defined by the MxDR Operations Manual).	X
Analyze security data and Client 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.	X
Vulnerability Data Correlation Integration provides the ability to ingest output from Client's vulnerability scanning to provide additional context for the MxDR Service.	X
Validate, assess and prioritize impact of Incident to Enterprise in accordance with processes described in the MxDR Operations Manual.	X
SECURITY INCIDENT ESCALATION	
Method of Notification of Security Incidents: Voice (as defined in the MxDR Operations Manual), MxDR Portal, Email (per Incident or Digest).	X
Method of Notification of Outage Incidents: Voice, MxDR Portal, Email (per Incident or Digest).	X
GENERAL SERVICE FEATURES	
Detection and response capability updated for emerging threats.	X
Daily Service Summary delivered by e-mail.	X
Log/device unavailability alerting and notification.	X[3]
Online logs may be queried by Client via the MxDR Portal.	X
Compliance reporting available on the MxDR Portal.	X

1: Refer to SPL to determine which MxDR Services are available in Per Unit or Enterprise Wide models, at which level of service, and for which supported technologies.

2: Subject to Runaway Device definition per the MxDR Operations Manual.

3: 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.

2. HOSTED LOG MANAGEMENT SERVICE	
SERVICE FEATURE	**DESCRIPTION**
Services Meter	Per Unit or Enterprise Wide[1]
SERVICE LEVEL AGREEMENT	
Device Registration	As described in the Service Level Agreement
SOC Infrastructure Up-Time	As described in the Service Level Agreement
Monthly Reporting	As described in the Service Level Agreement
LOG RETENTION (DURING SUBSCRIPTION TERM ONLY):	
Online MxDR Portal access to logs	12 months[2]
Online Incident Data Retention	Subscription Term
SECURITY INCIDENT ANALYSIS	
Log/Alert data collection, aggregation, and normalization.	X
Logs available for SOC Analyst inspection.	X[3]
GENERAL SERVICE FEATURES	
Log/device unavailability alerting and notification	X[4]
Online logs may be queried by Client via the MxDR Portal.	X
Compliance reporting available on the MxDR Portal.	X

1: Refer to SPL to determine which MxDR Services are available in Per Unit or Enterprise Wide models, at which level of service, and for which supported technologies.

2: Subject to Runaway Device definition per the MxDR Operations Manual.

3: Retention alone performs no security analysis.

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.

3. ADVANCED MANAGEMENT IDS OR IPS SERVICE	
SERVICE FEATURE	**DESCRIPTION**
Services Meter	Per Unit
SERVICE LEVEL AGREEMENT	
Device Registration	As described in the Service Level Agreement
Device Availability Up-Time Percentage	99.95%
SOC Infrastructure Up-Time Percentage	99.90%
Monthly Reporting	As described in the Service Level
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 the SOC engineer available immediately; but not later than within 30 minutes of request.
CHANGE MANAGEMENT	
Standard Changes (liicludes a single, low-risk configuration or policy change using MxDR 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 MxDR Portal standard change request templates. Includes endpoint Anti-virus / Firewall / IPS / Application Control / Device Control / Host Integrity policy management).	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 Client. Client initiated change requests require 5 business days' advance notice.
Major Changes (includes changes that modify architecture, technology or that require advance design).	N/A (Available only as anException Services).
Emergency Change or Assistance Requests.	5 per calendar month[1]
SERVICE FEATURES	
Provide management and configuration assistance for the features listed[3].	Policy management, Signature update, In-line configuration support Configuration for High Availability[3].
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
Monitor Managed Device for detected fault messages[2].	X
Monitor for content update failure messages[3].	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 MxDR Portal
Visibility into current tickets, Device status, Log Outage alerts	Available on MxDR the Portal

1: Additional requests available with purchase of Exception Services.

2: Subject to the technology support of features.

3: Support of the High Availability feature refers explicitly to configuring that component on a Device(s) for which the Advanced Management IDS or IPS Service has been purchased. For avoidance of doubt, Client must purchase the Advanced Management IDS or IPS Service for each Device(s) that Client requires to be managed, regardless of whether or not the Device(s) is configured as part of a High Hvailability pair.

4. ADVANCED ENDPOINT RESPONSE SERVICE	
SERVICE FEATURES	**DESCRIPTION**
Services Meter	AER Model
Advanced Endpoint Response Investigation ("**AER Investigation**")	An incident triage investigation is initiated when suspicious activities are detected by Accenture to determine if the activity is a threat and if the severity of suspicious activity is correct. Performed by Accenture security analysts remotely connecting to the AER Tool and investigating host traffic[1]. Based on the nature and type of the suspicious activity, such AER Investigation may include the following activities performed by Accenture security analysts using the AER Tool[2]: ▪ Investigate Client Data comprised of host forensic data (memory, disk and system), network traffic and logs. ▪ Correlate collected findings and indicators of compromise with the Accenture global threat intelligence capability. ▪ Other remote investigation as deemed necessary by Accenture. ▪ Perform automated threat hunting using the AER Tool. ▪ Contain known malware on individual endpoints that are discovered as part of an alert created by the Advanced Endpoint Response Service.
SERVICE LEVEL AGREEMENT	See the MxDR Service Offering Chart for Advanced Security Monitoring and Detection Service
LOG RETENTION (DURING SUBSCRIPTION TERM ONLY)	See the MxDR Service Offering Chart for Advanced Security Monitoring and Detection Service
SECURITY INCIDENT ANALYSIS	See the MxDR Service Offering Chart for Advanced Security Monitoring and Detection Service
SECURITY INCIDENT ESCALATION	See the MxDR Service Offering Chart for Advanced Security Monitoring and Detection Service
GENERAL SERVICE FEATURES	See the MxDR Service Offering Chart for Advanced Security Monitoring and Detection Service

1: Offsite Investigation. AER Investigation is performed remotely. Accenture reserves the right to assign any suitable skilled resource(s) available to provide the Advanced Endpoint Response Services. Accenture is not obligated to provide a specific Accenture resource or third-party resource. Client authorizes Accenture to perform any AER Investigation of Client Data necessary for the Advanced Endpoint Response Service. Accordingly, Client acknowledges and agrees that Accenture gathers Client Data from Client's computer network using the AER Tool, as well as the supported EPP. Client explicitly consents to Accenture collecting such Client Data from Client's computer network and Client assumes all risk and liability in this regard and Accenture shall have no liability in this regard whatsoever.

2: **AER Tool – Additional Terms.**

A. Restrictions. Notwithstanding anything to the contrary in the Agreement, the following shall apply where Client is using an Accenture provided AER Tool:

(i) Client shall prohibit its employees or contractors from accessing the AER Tool;

(ii) the AER Tool is provided to Client on a limited, personal, non-transferable, and non-exclusive basis;

(iii) the AER Tool is licensed, not sold, and title to and ownership of the AER Tool and any portion thereof shall remain exclusively with Accenture and/or its licensors;

(iv) Accenture and its licensors provide the AER Tool on an "as is" basis and disclaim all express and implied warranties with respect to such AER Tool including any implied warranties of merchantability, fitness for purposes or title;

(v) notwithstanding anything to the contrary in the Agreement, Accenture and its licensors shall have no liability whatsoever for any direct, special, indirect, exemplary, incidental or consequential damages with respect to the AER Tool;

(vi) where the Advanced Endpoint Response Service includes software belonging to a third party, such third party is a third-party beneficiary of the Agreement;

(vii) the AER Tool shall at all times be treated by Client as "commercial computer software" and "commercial computer software documentation", developed entirely at private expense, under any applicable governmental laws, regulation or rules and is otherwise provided to the government with the restricted rights and provided subject to the terms of such written agreement; and

(viii) Client may not: (a) copy the AER Tool, except as reasonably necessary for back-up or archival purposes; (b) distribute or transfer the AER Tool to any third party; (c) modify the AER Tool; (d) reverse engineer, decompile or disassemble or otherwise attempt to derive the source code from the AER Tool, in whole or in part; or (e) export the AER Tool or any underlying technology in contravention of any applicable or export laws and regulations.

B. Implementation of AER Tool. When the AER Tool is included with the Advanced Endpoint Response Service, Client must work with Accenture to deploy and implement the AER Tool in the environment that will be part of the Advanced Endpoint Response Service, in accordance with the specifications set forth in the MxDR Operations Manual. If the Client already owns the AER Tool, it is the Client's responsibility to deploy, implement and maintain the AER Tool.

C. Implementation of LCP. Client must work with Accenture to deploy and implement an appropriate LCP.

D. Remote Access. In the event that Client is providing the AER Tool, Client must provide Accenture with remote access to: (i) Client's implementation of the AER Tool; and (ii) necessary administrative credentials to enable Accenture to perform the Advanced Endpoint Response Service.

E. Client Security Testing. Client must provide Accenture at least 12 hours advance notice of any scheduled security testing including but not limited to penetration testing, application testing, vulnerability assessments to prevent false alarms.

4. ADVANCED NETWORK RESPONSE SERVICE	
SERVICE FEATURES	**DESCRIPTION**
Services Meter	Per Unit
Advanced Network Response Investigation ("**AER Investigation**")	Accenture's security analysts will initiate an incident forensic investigation when a suspicious activity is detected by Accenture in an effort to determine if the activity is a threat. An ANR Investigation is performed by Accenture security analysts remotely connecting to Client-owned Network Forensics Investigation Devices[1] and investigating network traffic to aid Client 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 an ANR Investigation. Such ANR Investigation may include the following activities[2]: ▪ Monitoring hostile activity. ▪ Investigating Client Data comprised of network packet capture data and network traffic logs. ▪ Correlating collected findings and indicators of compromise with the Accenture global threat intelligence capability. ▪ Other remote investigation as deemed necessary by Accenture.

1: A list of Accenture approved Network Forensics Investigation Device(s) ("**NFID**") is found in the SPL. NFIDs to be covered by the Advanced Network Response Service must be appropriately deployed and configured according to the standards defined by MxDR security analysts and must be online and available for an ANR Investigation for Accenture to perform the Advanced Network Response Service. Client must maintain and keep the approved NFIDs properly running and functioning. Failure to do so does not constitute a failure to deliver the Advanced Network Response Service on Accenture's part.

2: In addition to the Client Responsibilities in the Service Description, Client shall:

A. Client Security Testing: Client must provide Accenture at least 12 hours notice in advance of any scheduled security testing including but not limited to penetration testing, application testing, vulnerability assessments to prevent false alarms.

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

C. Offsite Investigation. An ANR Investigation is performed remotely. Client authorizes Accenture to perform any ANR Investigation of Client Data necessary for the Advanced Network Response. Accordingly, Client acknowledges and agrees that Accenture may be required to connect its computers and equipment to Client's computer network. Client explicitly consents to Accenture connecting its computers and equipment to Client's computer network and Client assumes all risk and liability in this regard and Accenture shall have no liability in this regard whatsoever.

D. Personnel. Accenture reserves the right to assign any suitable skilled resource(s) available to provide the Advanced Network Response Services. Accenture is not obligated to provide a specific Accenture resource or third-party resource.

E. Access Rights. Client will ensure that Accenture has access to all NFIDs necessary to complete the Advanced Network Response Services at all times. Where applicable, such access shall include appropriate user accounts to perform remote investigation of Client Data collected by NFIDs.

ATTACHMENT 2
Data Safeguards for Client Data

These data safeguards ("**Data Safeguards**") set forth the security framework that Client and Accenture will follow with respect to protecting Client 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 Client Data includes Personal Data, and taking into consideration the nature, scope and purposes of the processing of the Client 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 Client Personal Data.

I. Controlling Standards. Client 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 Client 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, Client will not be entitled to (i) data or information of other Clients or Clients 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 Client 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 Client 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 Client Data in connection with the Agreement.

2. ASSET MANAGEMENT

a) **Asset Inventory**. Accenture will maintain an inventory of all media on which Client 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 Client 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 Client Data to what is minimally necessary to perform services and have procedures for disposing of printed materials that contain Client Data.

iii. Accenture will require its personnel to obtain appropriate authorization prior to storing Client Data outside of contractually approved locations and systems, remotely accessing Client Data, or processing Client 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 Client Data are located.

b) **Physical Access to Components**. Accenture will maintain records of the incoming and outgoing media containing Client Data, including the kind of media, the authorized sender/recipients, date and time, the number of media, and the types of Client 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 CyberSecurity Framework, as applicable) processes to delete Client 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 Client Data.

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

i. Enforces device encryption;

ii. Protects and limits use of Client 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 Client 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 Client Data, including malicious software originating from public networks.

e) **Data Beyond Boundaries**. Accenture will

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

ii. Protect Client 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 Client 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 Client Data via its systems. b) Access Authorization. Accenture will

i. Maintain and update a record of personnel authorized to access Accenture systems that contain Client 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 Client Data, the individuals have unique identifiers/log-ins.

c) **Least Privilege**.

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

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

iii. Accenture will limit access to Client 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 Client 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-Client and non-Accenture environments from the Client 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 Client 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 Client Data are located.

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