ACCENTURE MANAGED EXTENDED DETECTION & RESPONSE (MxDR)

Revision Date: April 5, 2022

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

1. DEFINITIONS.

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

"**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/security-legal-terms (or succesor URL).

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

"**Agreement**" shall mean collectively the Order Confirmation, this Service Description, and the Terms and Conditions (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. The MxDR Services may be performed by Accenture or any of its Affiliates.

"**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 individual, the company or legal entity named in the Order Confirmation.

"**Client's System**" shall mean (as applicable) Client's or a third party's computer environment, operational technology environment, including systems that reside within such environment (e.g. mechanical systems, automation control systems, electronic systems for monitoring or controlling physical processes, networked electronic systems with automation or control capabilities involved in the operation, production and delivery of goods and services and/or industrial control systems) and related services.

"**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 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 Accenture's log collection platform which is provided by Accenture and installed by Client on Client's hardware or virtual infrastructure. Further details on the LCP and Client infrastructure requirements can be found in the LCP deployment guide distributed by Client's MxDR Service Delivery Lead ("**LCP Deployment Guide**").

"**Managed Device(s)**" shall mean a Device(s) that is managed by Accenture pursuant to the Advanced Managed IDS/IPS Intrusion Detection System (IDS) and Intrusion Prevention System Service.

"**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 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 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).

"**Subscription**" shall mean, a fixed term 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 period of time for which a Subscription is valid, as set forth in the Order Confirmation.

"**Supported Product List**" or "**SPL**" shall mean Accenture's list of supported products for the MxDR Services, which is available on the MxDR Portal.

"Terms and Conditions" shall mean Accenture's terms and conditions published by Accenture at https://www.accenture.com/us-en/support/security/security-legal-terms (or successor URL), unless otherwise 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:

- **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. (**Note: No longer available for new purchases.**)
- **Advanced Endpoint Response Service**, provides investigation of identified suspicious endpoint activities utilizing an AER Tool in an effort to provide enhanced context, refine incident severity and proactive response (as applicable).
- **Advanced Network Response Service,** provides investigation of identified suspicious network activities in an effort to provide enhanced context, refine incident severity and proactive response (as applicable).

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 Terms and Conditions, 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 on the MxDR Portal, provides further details regarding Client's use and access to the MxDR Services, including procedural and operational processes, to be performed by the Client for its receipt of the applicable 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 a Managed Device(s) 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 Managed Device(s) receiving the Advanced Managed IDS/IPS Intrusion Detection System (IDS) and Intrusion Prevention System Service. Client is responsible for obtaining any required license(s) from the technology vendor(s) to allow applicable use of the Hosted Management Console (**Note: No longer available for new purchases**).

3.3 **Supported Device(s).** The SPL specifies the list of supported technologies that may receive MxDR Services.

3.4 **Technical Support**. Technical assistance for the MxDR Services will be provided by Accenture as specified in the MxDR Operations Manual. 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. LCP LICENSE, INSTALLATION, INTERNAL USE & RESTRICTIONS.

4.1 **LCP License**. Accenture grants to Client a non-exclusive, non-transferable right to install and use the LCP on the Client hardware or virtual infrastructure (as further specified in the LCP Deployment Guide), 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). For the avoidance of doubt, Open Source Software included in the LCP is not licensed under the terms of the LCP 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). Client's rights to the LCP 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.

4.2 **LCP Installation.** Client shall be solely responsible for successfully installing the LCP on Client's hardware or virtual infrastructure (as specified in the LCP Deployment Guide) 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) in a format that is compatible with the MxDR Services, which may require configuration changes to the Device(s). Accordingly, 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 must provide all required hardware or virtual infrastructure necessary for the LCP and enable access to such hardware or virtual infrastructure by Accenture (as specified in the LCP Deployment Guide).

4.3 **Internal Use Only**. Client's Subscription to access and use the MxDR Services and/or the LCP 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 the LCP 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: (a) solely for Client's and/or Client's Affiliates' internal business purpose; (b) up to the Meter amount for which Client purchased the applicable MxDR Service; and (c) 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 the LCP, unless permitted by applicable law for interoperability purposes; (ii) access or use the MxDR Services and/or the LCP to build or support,

directly or indirectly, products or services competitive to Accenture; (iii) license, sell, transfer, assign, distribute, outsource, permit timesharing or service bureau use of, commercially exploit, or make available the MxDR Services and/or the LCP to any third party except as permitted by the Agreement; or (iv) export the MxDR Services and/or the LCP in contravention of any applicable or export laws and regulations.

4.5 **MxDR Services related information**. Client acknowledges and agrees that Accenture shall retain, use and analyze information derived from Client's use of the MxDR Services (in a de-identified manner), including indicators of compromise, malware, anomalies, or other information that may be found as part of, or related to the performance of the MxDR Services for the purposes of gathering and compiling security event log data to look at trends and real or potential security threats, improving and developing Accenture's security products and services, preparing and distributing statistical reports related to security trends and data patterns, internal research, and for providing general security related services.

4.6 **Intellectual Property.** Client acknowledges and agrees that the MxDR Services, LCP and related processes, instructions, methods, and techniques are owned by or have been developed by Accenture and/or its licensors, and that the same shall remain the sole and exclusive property of Accenture and/or its licensors. Client will not assert any rights in Accenture's intellectual property or data, including limitations provided in FAR 12.212 and DFAR Section 227-7202.

5. SERVICES METER.

The MxDR Services are available for purchase by Client 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) Client does not exceed 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) as specified in the Order Confirmation. If Client is a Service Provider and purchases the applicable MxDR Service on an Enterprise Wide basis for the benefit of its end user client, the applicable total Node Count shall be for the applicable end user client receiving outsourced services from Service Provider; and

(ii) if, at any time during the Subscription Term, Client's Node Count increases by more than 10% 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 applicable MxDR Service to become compliant with such increased Node Count. In the event that Client fails to purchase such additional quantity of the applicable MxDR Service, Accenture reserves the right to suspend the applicable 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 the quantity of Device(s) specified in the Order Confirmation. Per Unit MxDR Services are available on a per Device(s), Block of Device(s) or Pack of Units basis.

5.3 **Services Meter - AER Model.** Client's purchase of the Advanced Endpoint Response Service shall entitle Client to receive the Advanced Endpoint Response Service specifically for the 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.

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

6.5 **Standard Changes for Managed Device(s) Completion Time Service Level**. Accenture will complete Standard Changes for Managed Device(s) 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 for Managed Device(s) Completion Time Service Level**. Accenture will complete the Minor Changes for Managed Device(s) 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 for Managed Device(s) Response Time Service Level**. In the event that an emergency change request or other emergency assistance is required with respect to a Managed Device(s), 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 Terms and Conditions, 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 Terms and Conditions, 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 set forth 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 Service Availability**. Accenture will provide 90 days notice of the last date of the availability of an MxDR Service. Accenture will provide such notification to Client's reseller, then-current business or technical contact, or by publication on the MxDR Portal, as applicable. Once an MxDR Service is no longer available, Client will no longer have access to or use of such MxDR Service. Accenture will credit Client's account any prorated, unused fees received by Accenture for the applicable MxDR Service that is subject to an end of service availability notification.

7.4 **Termination of Services.** Either party may terminate a Subscription (in whole or part) without penalty and/or liability, upon written notice to the other party (and as of the date specified in such written notice), in the event that any law, statue, rule, decree, executive order, regulation, judgement, decision, ruling and/or award of any government agency in any jurisdiction, anywhere in the world materially impacts on (in the reasonable opinion of the terminating party) Accenture's compliance obligations, its delivery of the MxDR Services and/or Client's receipt of the MxDR Services.

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, Permissions and authority for Accenture to deliver the MxDR Services;(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); (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 (v) 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 Clients Systems, and that Client is authorized to instruct Accenture to perform the MxDR Services. 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 Agreement, 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 delays and/or failure to perform the MxDR Services if such delays and/or failure arise out of Client's act or omission inconsistent with the Client Responsibilities which impact Accenture's ability to deliver the MxDR Services. Without prejudice to the foregoing, any such delay and/or 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' recommended 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 **Recommendations**. Client is solely responsible for assessing (and as applicable, implementing) any recommendations, advice and/or instructions provided by Accenture in the course of providing the MxDR Services.

9.7 **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 or 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 **Incremental Services**. Client may request Accenture provide services that are in addition to the scope of the MxDR Services specified in this Service Description ("**Incremental Services**"). Upon receipt of a request for Incremental Services, the parties will: (i) cooperate with each other in good faith in discussing the scope, terms and conditions and nature of any

request for Incremental Services, and the basis upon which Accenture shall be compensated for such Incremental Services; and (ii) enter into a mutually agreed upon change order to cover the scope of the Incremental Services.

10.3 **Litigation Support Services.** Litigation support services of any kind are excluded from the MxDR Services provided under this Service Description, including but not limited the following: (a) depositions, fact witness testimony, expert witness testimony, affidavits, declarations, expert reports; (b) responding to discovery requests, subpoenas; (c) eDiscovery services; and/or (d) 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).

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; (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 Client Systems and validation of such Client Systems; (vii) installation of software; (viii) implementation of available Device(s) or updates/patches from third party vendor; (ix) representing Client in any audit or compliance assessments of relevant security controls; and/or (x) any activity which Accenture reasonably determines would breach applicable law or infringe the rights of a third party.

11. DATA PROTECTION

11.1 **Collection and Processing of Client Personal Data.** Client acknowledges that in performing the MxDR Services, Accenture shall, on behalf of Client, collect, process and store certain Client Personal Data in accordance with the data protection terms set forth in the Terms and Conditions. The: (i) subject matter and duration of the processing; (ii) nature and purpose of the processing; and (iii) types of Client Personal Data and categories of data subjects shall be as specified in the MxDR Services Transparency Notice ("**Transparency Notice**") published by Accenture at https://www.accenture.com/us-en/support/security/security-legal-terms (or successor URL). Client acts as a controller for the processing of such Client Personal Data and Accenture acts as a processor under applicable Data Protection Laws. In certain cases, Accenture may also collect and process certain Client Personal Data as a controller (e.g. in order to provide Client with access and use of the MxDR Portal) in accordance with the Privacy Statement published by Accenture at https://www.accenture.com/us-en/support/security/security-legal-terms (or successor URL). Each party will comply with the requirements of the Data Protection Laws as applicable to such party with respect to the processing of Client Personal Data.

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	See Section 6.1 of the Service Description
Severe Event Notification	See Section 6.2 of the Service Description
SOC Infrastructure Up-Time	See Section 6.3 of the Service Description
Monthly Reporting	See Section 6.8 of the Service Description
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.	Included
Logs available for SOC Analyst inspection.	Included
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). ▪ 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 malicious user and entity activity.	Included
Vulnerability Data Correlation Integration provides the ability to ingest output from Client's vulnerability scanning to provide additional context for the MxDR Service.	Included
Validate, assess and prioritize impact of Incident to Client in accordance with processes described in the MxDR Operations Manual.	Included
SECURITY INCIDENT ESCALATION	
Method of Notification of Security Incidents: Voice (as defined in the MxDR Operations Manual), MxDR Portal, Email (per Incident or Digest).	Included
Method of Notification of Outage Incidents: Voice, MxDR Portal, Email (per Incident or Digest).	Included
GENERAL SERVICE FEATURES	
Detection and response capability updated for emerging threats.	Included
Daily Service Summary delivered by e-mail.	Included
Log/device unavailability alerting and notification.	Included [3]
Online logs may be queried by Client via the MxDR Portal.	Included
Compliance reporting available on the MxDR Portal.	Included

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 technologies registered in netblock ranges shall be based on outage monitoring of the netblock range.

2. HOSTED LOG MANAGEMENT SERVICE	
SERVICE FEATURE	**DESCRIPTION**
Services Meter	Per Unit or Enterprise Wide[1]
SERVICE LEVEL AGREEMENT	
Device Registration	See Section 6.1 of the Service Description
SOC Infrastructure Up-Time	See Section 6.3 of the Service Description
Monthly Reporting	See Section 6.8 of the Service Description
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.	Included
GENERAL SERVICE FEATURES	
Log/device unavailability alerting and notification	Included[3]
Online logs may be queried by Client via the MxDR Portal.	Included
Compliance reporting available on the MxDR Portal.	Included

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 technologies registered in netblock ranges shall be based on outage monitoring of the netblock range.

3. ADVANCED MANAGEMENT IDS OR IPS SERVICE	
SERVICE FEATURE	**DESCRIPTION**
Services Meter	Per Unit
SERVICE LEVEL AGREEMENT	
Device Registration	See Section 6.1 of the Service Description
Managed Device Availability Up-Time Percentage	99.95%
SOC Infrastructure Up-Time Percentage	See Section 6.3 of the Service Description
Monthly Reporting	See Section 6.8 of the Service Description
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 (Includes a single, low-risk configuration or policy change using MxDR Portal standard change request templates.	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 through the MxDR Portal standard change request templates.	Unlimited Requests
Significant Changes (includes software changes or high- risk policy changes that interrupt device functionality).	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 an Incremental Service).
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].
INCIDENT / FAULT MANAGEMENT	
Monitor Managed Device for accessibility by SOC.	Included
Monitor Managed Device for detected fault messages[2].	Included
Monitor for content update failure messages[3].	Included
Respond to and troubleshoot Managed Device issues	Included
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 the MxDR Portal

1: Additional requests available with purchase of Incremental Services.

2: Subject to the technology support of features.

3: Support of the High Availability feature refers explicitly to configuring that component on a Managed 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 Managed Device(s) that Client requires to be managed, regardless of whether or not the Managed Device(s) is configured as part of a High Availability pair.

4. ADVANCED ENDPOINT RESPONSE SERVICE	
SERVICE FEATURES	**DESCRIPTION**
Services Meter	AER Model
SERVICE LEVEL AGREEMENT	
Device Registration	See Section 6.1 of the Service Description
Severe Event Notification	See Section 6.2 of the Service Description
SOC Infrastructure Up-Time	See Section 6.3 of the Service Description
Monthly Reporting	See Section 6.8 of the Service Description
LOG RETENTION (DURATION THE SUBSCRIPTION TERM ONLY):	
Online MxDR Portal access to logs	12 months
Online Incident Data Retention	Subscription Term
ADVANCED ENDPOINT RESPONSE INVESTIGATION	
An Advanced Endpoint Response Investigation ("**AER 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. An AER Investigation is performed by Accenture security analysts remotely by connecting to the AER Tool. Based on the nature and type of the suspicious activity, an AER Investigation may include the following activities performed by Accenture security analysts using the AER Tool: ▪ 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 AER Investigation.	Included
SECURITY INCIDENT ANALYSIS	
Log/Alert data collection, aggregation, and normalization.	Included
Logs available for SOC Analyst inspection.	Included
Analyze security data (which includes endpoint telemetry and artifacts) and Client context in an effort to improve visibility and detect the following signs of malicious activity, as applicable based on the log output received from the monitored Device(s), such as: ▪ adversary behavior ▪ fileless/memory resident attacks ▪ emerging exploit chains ▪ low and slow attacks ▪ 'living off the land' attacks	Included
Vulnerability Data Correlation Integration provides the ability to ingest output from Client's vulnerability scanning to provide additional context for the MxDR Service.	Included
Validate, assess and prioritize impact of Incident to Client in accordance with processes described in the MxDR Operations Manual.	Included
SECURITY INCIDENT ESCALATION	
Method of Notification of Security Incidents: Voice (as defined in the MxDR Operations Manual), MxDR Portal, Email (per Incident or Digest).	Included
Method of Notification of Outage Incidents: Voice, MxDR Portal, Email (per Incident or Digest).	Included
GENERAL SERVICE FEATURES	
Detection and response capability updated for emerging threats.	Included
Daily Service Summary delivered by e-mail.	Included
Log/device unavailability alerting and notification.	Included
Online logs may be queried by Client via the MxDR Portal.	Included
Compliance reporting available on the MxDR Portal.	Included

Client's access and use of the Advanced Endpoint Response Services shall be subject to the following additional terms:

1: AER Investigation. An AER Investigation is performed remotely. Client acknowledges and agrees that Accenture gathers Client Data from Client's computer network using the AER Tool. Accordingly, Client authorizes Accenture to perform an AER Investigation of Client Data necessary for the Advanced Endpoint Response Service. Client assumes all risk and liability in this regard and Accenture shall have no liability in this regard whatsoever.

2. **Accenture AER Tool.** The following shall apply where Client is using an Accenture provided AER Tool ("**Accenture AER Tool**"):

(i) The Accenture AER Tool is provided to Client on a limited, personal, non-transferable, and non-exclusive basis. Client shall at all times, prohibit its employees or contractors from accessing the Accenture AER Tool. Title to and ownership of the Accenture AER Tool and any portion thereof shall remain exclusively with Accenture and/or its licensors.

(ii) Accenture and/or its licensors provide the Accenture AER Tool on an "**AS-IS**" basis and disclaim all express and implied warranties with respect to the Accenture AER Tool including any implied warranties of merchantability, fitness for purposes or title. Accenture and its licensors shall have no liability whatsoever for any direct, special, indirect, exemplary, incidental or consequential damages with respect to the Accenture AER Tool. With respect to an Accenture AER Tool that is owned by an Accenture licensor, such licensor is a third-party beneficiary of the Agreement.

(iii) Client shall at all times treat the Accenture AER Tool 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.

(iv) 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 Accenture AER Tool, unless permitted by applicable law for interoperability purposes; (ii) access or use the Accenture AER Tool to build or support, directly or indirectly, products or services competitive to Accenture; (iii) license, sell, transfer, assign, distribute, outsource, permit timesharing or service bureau use of, commercially exploit, or make available the Accenture AER Tool to any third party except as permitted by the Agreement; or (iv) export the AER Tool or any underlying technology in contravention of any applicable or export laws and regulations.

(v) Client shall work with Accenture to deploy, implement and maintain the Accenture AER Tool in the Client's environment, as further specified in the MxDR Operations Manual.

3. Client AER Tool. The following shall apply where Client is using a a Client provided AER Tool ("**Client AER Tool**"):

(i) Client shall be solely responsible for deploying, implementing and maintaining the Client AER Tool. Accordingly, the Client AER Tool must be: (a) specified in the SPL; and (b) if the Client AER Tool does not have an end point protection agent ("**EPP**") as specified in the SPL, Client is also required to deploy, implement and maintain an EPP that is specified on the SPL;

(ii) Client shall be solely responsible for maintaining current maintenance and technical support contracts for the Client AER Tool with Client's third-party vendors. Client shall ensure that Client AER Tool is scoped and implemented in accordance with manufacturer's recommended standards. Client is solely responsible for remediation and resolution of changes to Client AER Tool which negatively impact the Advanced Endpoint Response Service or the functionality, health, stability, or performance of Client AER Tool; and

(iii) Client shall be solely responsible for the following to enable Accenture to perform the Advanced Endpoint Response Services: (a) obtaining consent from any applicable third-party vendor for Accenture to use or access the Client AER Tool; and (b) providing Accenture with remote access to the necessary administrative credentials for the Client AER Tool.

5. ADVANCED NETWORK RESPONSE SERVICE	
SERVICE FEATURES	**DESCRIPTION**
Services Meter	Per Unit
ADVANCED NETWORK RESPONSE 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 Advanced Network Response Service Investigation ("**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.	Included

1: A list of Accenture approved Network Forensics Investigation Device(s) ("**NFID**") is specified 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.

Accordingly, Client be solely responsible for:

(i) deploying, implementing and maintaining the NFID;

(ii) maintaining current maintenance and technical support contracts for NFID with Client's third party vendors. Client shall ensure that the NFID is scoped and implemented in accordance with manufacturer's recommended standards. Client solely responsible for remediation and resolution of changes to the NFID which negatively impact the Advanced Network Response Service or the functionality, health, stability, or performance of the NFID; and

(iii) Client shall be solely responsible for: (a) obtaining consent from any applicable third-party vendor for Accenture to use or access the NFID; and (b) providing Accenture with access to all the NFID 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 NFID.

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

A. Advanced Security Monitoring and Detection Service. Client may only subscribe to receive the Advanced Network Response Service during such time as Client also has and maintains a valid subscription for Accenture' Advanced Security Monitoring and Detection Service.

B. Offsite Investigation. An ANR Investigation is performed remotely. Client acknowledges and agrees that Accenture gathers Client Data from Client's computer network. Accordingly, Client authorizes Accenture to perform an ANR Investigation of Client Data necessary for the Advanced Network Response Service. Client assumes all risk and liability in this regard and Accenture shall have no liability in this regard whatsoever.