Managed Extended Detection and Response (MXDR) with Accenture

1. **General**
MXDR Services provide 24x7 real-time security monitoring, analysis, detection, reporting plus response. The MXDR Service is performed utilizing a combination of skilled analysts and market leading technology in conjunction with Accenture's global threat intelligence capability in an effort to identify, isolate and contain known and emerging security threats to Customer's infrastructure. This Schedule ("Schedule") describes the MXDR Services, the responsibilities of Customer and Accenture with respect to such services and terms and conditions applicable thereto. In the event of any conflict or inconsistency between this Schedule and the Customer agreement with Verizon under which MXDR Services are provided to Customer (the **"Customer Agreement"**), notwithstanding anything to the contrary in the Customer Agreement, the terms of this Schedule will control including with respect to descriptions, features and performance of the MXDR Services set forth therein.

1.1 **Scope of Work**

1.1.1 **Scope of Work.** Accenture will provide the MXDR Services as pursuant to this Schedule for the Service Commitment using a global delivery model to Customer including customer support, as described herein, on a 24 x 7 basis from global delivery centers and includes a remote Service Delivery Lead during USA ET normal business hours (8 x 5 Monday - Friday).

1.2 **Solution Overview**

MXDR Services have the following features:

1.2.1 **MXDR Portal.** Customer shall have read-only access to and use of the MXDR Portal, which is made available by Accenture to the Customer for use solely with respect to MXDR Services during the applicable Service Commitment.

1.2.2 **MXDR Full Stack Infrastructure.** Accenture will provision and maintain an environment for Customer on Accenture's multi-tenant platform to deliver the MXDR Services for the Service Commitment. Accenture will use the Security Incident and Event Management **(SIEM)** Platform to normalize, index, correlate and analyze Customer's log data to detect security events, triage and prioritize response actions. Accenture will use the Security Orchestration, Automation and Response **(SOAR)** Platform to support its coordination, investigation, and response to security events, including automated containment or escalation in accordance with agreed Playbooks. Customer will have read-only access to the SIEM/SOAR via the Accenture MXDR Portal. All MXDR Full Stack components such as SIEM and SOAR are maintained and managed by Accenture.

1.2.3 **CyberHub.** Accenture's will provide Customer with read-only access to its CyberHub log collection tool, which is provided by Accenture and installed by Customer on virtual infrastructure. Further details on the CyberHub and Customer infrastructure requirements can be found in the CyberHub deployment guide distributed by Accenture ("CyberHub Deployment Guide").

1.2.4 **Cyber Intelligence.** Accenture will supplement native cyber intelligence capabilities of the SIEM and SOAR Platforms with API feeds from Accenture's proprietary Cyber Intelligence **(ACI)** to support the provision of the MXDR Services for the Service Commitment. Customer supplied threat intelligence is not supported.

1.2.5 **Security AI Assistant.** The MXDR Services includes the use of generative AI-powered tools **("Gen AI Tools")** to enhance accuracy, efficiency and/or user experience of the services. Accenture shall be

exclusively responsible for complying with any terms and conditions provided by the supplier(s) of the Gen AI Tools. The use of Gen AI Tools is required for the use of Security AI Assistant Tool. The Customer that purchases Security AI Assistant acknowledge that Accenture will input Customer data, including MXDR Personal Data into the Gen AI Tools to prompt the relevant context, and Accenture warrants that such Gen AI Tools will not retain any Customer data nor reuse it for any purpose other than to reply to such users' prompts.

1.2.6 **Security Operations Centers.** MXDR Services are performed remotely by Accenture security staff aligned to one of Accenture's Security Operations Centers **("SOC(s)")**. A list of SOC locations can be found in Attachment 1 to this Schedule. Accenture may provide Customer with information and notices about the MXDR Services electronically, including via email through the MXDR Portal. Notice is given as of the date it is made available by Accenture.

1.2.7 **Continuous Threat Hunting.** As Cyber Intelligence feeds identify new threats, Accenture will perform a retrospective threat hunt over the preceding 12 months of log data using SOC Infrastructure capabilities.

1.2.8 **Scheduled Maintenance**. Accenture will, from time to time, schedule regular maintenance of the platform and the SOC Infrastructure. Accenture will provide notice of upcoming maintenance via the MXDR Portal.

1.2.9 **Emergency Maintenance.** Accenture might on rare occasions schedule emergency maintenance due to unforeseen circumstances.

1.2.10 **Supported Device(s).** The Supported Products List – Full Stack **("SPL-FS")** specifies, on the MXDR Platform, the list of supported technologies that may be integrated with MXDR Services.

1.2.11 **Technical Support**. Customer is responsible for maintaining its Devices. Accenture will provide reasonable technical assistance for issues regarding integration of Customer Devices with the MXDR Services.

1.2.12 **Permitted Nodes**. The term **"Node Count"** shall mean the total number of Nodes owned or used by Customer (and/or any Affiliate Entity of Customer) that are active in the MXDR Service for at least four hours within a 24-hour period.

1.3 **Intentionally Omitted**

1.4 **Out of Scope.** The following activities are beyond the scope of the MXDR Service in this Schedule:

1.4.1 Incident response services and remediation activities are limited to the actions defined in agreed Playbooks (typically, automated containment, escalation to Customer resolver groups, or initiation of Customer's incident response plan). Customer remains responsible for the remediation of any identified vulnerabilities unless separately agreed.

1.4.2 Penetration testing or vulnerability scanning activities.

1.4.3 Any audit or compliance assessments of relevant security controls or related attestations; any expert testimony or litigation support services, such as (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); and

(e) activity which Accenture reasonably determines is likely to breach applicable law or infringe the rights of a third party, of which Accenture will notify Verizon if it determines that it cannot perform such activities.

1.5 **License.** Accenture grants Customer a non-exclusive, non-transferable, non-sublicensable license to use and receive the benefit of the MXDR Services for the Service Commitment and solely for Customer's internal business purposes. Specifically, Customer may:

1.5.1 Access and use dashboards and MXDR Portal as made available by Accenture; and otherwise receive the benefit of the Services without direct access to the SIEM Platform or SOAR Platform.

1.6 **MXDR CyberHub License**

CyberHub License. Accenture grants to Customer a non-exclusive, non-transferable right to install and use the CyberHub on the Customer hardware or virtual infrastructure (as further specified in the CyberHub Deployment Guide), and additionally, the right to make a single uninstalled copy of the CyberHub for archival purposes which Customer may use and install for disaster-recovery purposes (i.e., where the primary installation of the CyberHub becomes unavailable for use) **("License")**. For the avoidance of doubt, Open-Source Software included in the CyberHub is not licensed under the terms of the CyberHub 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 Customer's use of the Open Source Software is subject to the terms of each such applicable Open Source Software license(s). Customer's rights to the CyberHub shall automatically end upon the expiration or earlier termination of the Service Commitment at which time, Customer shall immediately stop using and destroy all copies of the CyberHub.

Internal Use Only. Customer's access and use of the MXDR Services, and/or the CyberHub during the Service Commitment is on a limited, non-exclusive, non-transferable basis, solely for Customer's internal business purposes and strictly in accordance with the terms of this Schedule and the Customer Agreement, including without limitation: (i) use of the MXDR Services up to the amount for which Customer purchased such MXDR Services (as specified in the Order). Customer's Affiliate Entities may use the MXDR Services: (a) solely for Customer and/or Customer's Affiliate Entities' internal business purpose; (b) up to the amount for which Customer purchased the applicable MXDR Service; and (c) in accordance with the Agreement. Customer assumes full responsibility for all actions in connection with such use of the applicable MXDR Service by Customer's Affiliate Entities. Customer may use ACI as may be provided to it by Accenture solely for the purposes of management and protection of its networks, systems and assets.

Customer will not remove any confidentiality, copyright or other markings from any ACI or transfer or distribute ACI or any portion thereof to third parties. ACI is Accenture's Confidential Information and is provided on an "AS IS', "WHERE IS" AND "AS AVAILABLE" basis.

Restrictions. Customer 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 CyberHub, unless permitted by applicable law for interoperability purposes; (ii) access or use the MXDR Services and/or the CyberHub 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 CyberHub to any third party except as permitted by the Agreement; or (iv) export the MXDR Services and/or the CyberHub in contravention of any applicable or export laws and regulations.

1.7 **MXDR Services related information.** Customer acknowledges and agrees that Accenture shall retain, use and analyze information derived from Customer'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.

1.8 **Intellectual Property.** Customer acknowledges and agrees that the MXDR Services, ACI, Use Case and Playbook Library, CyberHub 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. Customer will not assert any rights in Accenture's intellectual property or data, including limitations provided in FAR 12.212 and DFAR Section 227-7202.

1.9 **Responsibility Matrix.** Accenture will use the SIEM & SOAR Platforms to monitor for indicators of malicious activity, qualify, triage and prioritize security events, and will perform containment and escalation activities all according to agreed Use Cases and Playbooks as described in the responsibility matrices below.

1.9.1 **24x7 Monitoring Services**

Activity	Accenture	Verizon	Customer
Threat Detection, Investigation and Response			
24x7 monitoring and triage of IT security alerts (enrichment, log analysis, false positive suppression)	X		
Provide input on finalizing false positive			X
Security Incident identification, categorization & prioritization	X		
Escalate Customer identified security incidents	X		
Provide remediation recommendations where applicable	X		
Execute incident containment through SOAR based on preauthorized scenarios	X		
Incident management and containment or escalation in accordance with agreed Playbooks	X		
Categorize, document, measure and report Security Incidents	X		
Provide feedback (e.g., report false positives) on incident reports			X
Incident resolution (implementation of corrective actions)			X
Continuous retro-hunts for threats with an Intelligence driven TTP based approach	X		
Provide support and guidance on Customer's end to-end security case management focusing on Customer specific context and processes	X		

SOC Point of Contact			
Provide authorized Customer contacts to MXDR Service team for coordination of device onboarding activities		X	
Provide list of authorized Verizon contacts permitted to access Customer environment within MXDR platform		X	
Approve list of provided Verizon contacts permitted to access Customer environment within MXDR platform			X
Monitor the quality of SOC Services and take action or provide guidance as necessary	X		
Coordination Customer / Customer device onboarding to the Accenture MXDR platform	X		
Confirm authorized/expected activities impacting security monitoring			X
Authorize activation of Customer incident response team			X
Provide input and feedback (e.g., processes / procedures / key owners) required by SOC team to design Customer specific Playbooks			X

1.9.2 **Platform Support Services**

Activity	Accenture	Verizon	Customer
SIEM / SOAR Engineering			
Monitor availability and performance of the Chronicle / Chronicle SOAR platforms using health checks, and follow up with corrective actions or escalations in case of unavailability or low performance	X		
Manage Chronicle / Chronicle SOAR access and administration	X		
Manage authorized users of MXDR Portal, SIEM, and SOAR platforms for Customer	X		
Roll out vendor supplied major and minor software upgrades to the Accenture SIEM and SOAR Platforms	X		
Use Case development and tuning for threat detections	X		

Chronicle SOAR integration and content development	X		
Develop, deploy, test, monitor and optimize Playbooks	X		
Use Case optimization	X		
Provide necessary access to Customer network and systems			X
Provisioning of Linux / Windows virtual or physical machines for installation of the CyberHub and remote agents			X
Installation of the CyberHub and remote agents			X
Configuration of the CyberHub and remote agents	X		
OS Management for Forwarders and remote agents (Linux / Windows virtual or physical machines) (includes health and capacity monitoring, patching, backup & restore according to Customer's standards)			X
On-site diagnoses and remediation of Forwarders / remote agents where remote support is not sufficient			X
Provide technical information for each device to be onboarded to the SIEM Platform			X
Configuration of each device to provide correct logging to Forwarders			X
Forwarders and remote agents application maintenance			X
Accenture SIEM and SOAR Platform configuration changes for onboarding	X		
Validation of correct device logging once connected to the Forwarder	X		
Log source / device health tracking	X		
Notify Customer of device logging / health outages	X		
Provide Asset details within MXDR Portal			X

1.10 **Collection and Processing of Customer MXDR Personal Data**

1.10.1 Customer acknowledges that in providing the MXDR Services, Accenture may, on behalf of Customer, collect, process and store certain information relating to an identified or identifiable natural person, as provided by the applicable Data Protection Laws **("MXDR Personal Data")**. The: (i) subject matter and

duration of the processing; (ii) nature and purpose of the processing; and (iii) type of MXDR Personal Data and categories of data subjects shall be as specified in Attachment 1 to the Schedule, the Service Transparency Notice **("Transparency Notice")**.

1.10.2 Customer authorizes Accenture to engage the Accenture Affiliate Entities and the third-party Sub-processors detailed in the applicable subprocessor list in the Transparency Notice to process MXDR Personal Data in the delivery of the MXDR Service.

1.10.3 Customer acknowledges and agrees that it acts as a data controller for the processing of such MXDR Personal Data and Accenture acts as a data processor under applicable Data Protection Laws. In certain cases, as further specified in the Transparency Notice, Accenture may also collect and process certain MXDR Personal Data as a **"Controller"**. Each party will comply with the requirements of the Data Protection Laws as applicable to such party with respect to the processing of MXDR Personal Data.

1.10.4 Customer will ensure that it has and will maintain during the provision of the MXDR Services, all necessary rights (including lawful legal basis (as applicable)) and permissions to provide the MXDR Personal Data to Accenture for the processing to be performed in relation to the Service, and that Customer has provided all necessary notices, as required under the relevant Data Protection Laws in relation to the processing of the MXDR Personal Data.

1.10.5 Accenture agrees that it will: (i) only use the MXDR Personal Data to the extent that is necessary and proportionate to perform the MXDR Services, and in accordance with Customer's instructions, and only for duration of the MXDR Services; (ii) implement appropriate technical and organizational security measures to safeguard MXDR Personal Data, as specified in Accenture's Data Safeguards **("Data Safeguards")** published by Accenture at www.accenture.com/client-data-safeguards (or successor URL), with respect to which, Customer has satisfied itself that the Data Safeguards provide a level of security appropriate to the risk in respect of any processing of MXDR Personal Data; (iii) provide assistance as reasonably requested by Customer with respect to Customer's obligations under applicable Data Protection Laws (e.g. responding to requests by individuals, providing notice of breaches, consulting with regulators); (iv) make available information as reasonably requested by Customer to demonstrate Accenture's compliance with its obligations under this clause; and (v) return or destroy (at End Customer's direction) such MXDR Personal Data upon request of Customer or termination of the MXDR Services, to the extent that any MXDR Personal Data is retained by Accenture in performing the MXDR Services, as specified in the Transparency Notice.

1.10.6 For the purposes of delivering the MXDR Services, MXDR Personal Data may be transferred outside the country where MXDR Personal Data originates from. Destination countries might not be recognized by an adequacy decision under the applicable Data Protection Laws. Accordingly, in order to protect MXDR Personal Data being transferred to such countries in connection with the delivery of the MXDR Services, Accenture adopts the transfer mechanism(s) as specified in the Transparency Notice.

1.10.7 The following shall apply to the extent that the California Consumer Privacy Act **("CCPA")** and/or the California Privacy Rights Act **("CPRA")** applies. Accenture shall: (i) not sell or share any MXDR Personal Data (as defined by CCPA and CPRA); (ii) not retain, use or disclose any such MXDR Personal Data for any purpose other than business purposes specified in accordance with this Schedule; or (iii) not retain, use or disclose such MXDR Personal Data outside the direct business relationship between Accenture and Customer, as set forth in this Schedule, unless otherwise required by law; (iv) not process outside the specified business purpose; (v) provide the same level of privacy protection required by the applicable obligations under CPRA for MXDR Personal Data received by Accenture; (v) not combine personal information of opted out individuals from the Customer with different sources or with data collected from its own interaction with consumer; (vii) notify the business if it can no longer meet its obligations under CPRA and will work with the business to take appropriate steps with regard to the MXDR Personal Data. Customer agrees that execution of the applicable Order shall be deemed to constitute any certification that is required under applicable Data Protection Laws to the restrictions on sale, retention, use, or disclosure of MXDR Personal Data.

2. **Updates to the MXDR Services**
Accenture may update any of the MXDR Services from time to time, provided the updates do not result in a material reduction of the functionality, performance, availability, or security of such MXDR Services. Additionally, Accenture may make changes to the MXDR Service as required to comply with applicable law or to address a material security risk.

3. **Service Levels**
Subject always to Customer meeting its responsibilities as specified in the **'Customer Responsibilities'** section, the following service levels (each a **"Service Level"** and collectively the **"Service Levels"**) shall apply to the MXDR Services.

	Category	Security Incident Priority	Time	Expected Service Level	Description
1	**Traige Activation Time Incident Response**	Priority 1	15 min	95%	Accenture will start triaging Security Alerts reported by the SIEM Platform within the agreed timeframe. This is to provide assurance that Security Alerts are analyzed in a timely fashion consistent with their priority levels. Note: ● Initial Case priority is equal to the highest severity of all aggregated Security Alerts ● If Case priority is increased before Triage activation, due to automated enrichment/orientation or aggregation of higher severity Alerts, the shorter SLA will apply calculated from the time priority is increased, but no longer than the original SLA. ● Security Alerts triggered after Triage activation do not affect this SLA.
		Priority 2	15 mins		
		Priority 3	4 hours		
		Priority 4	8 hours		
2	**High Priority Initial Notification Time**	Priority 1	30 mins	95%	Upon identifying a high priority Security Incident, Accenture will notify the Customer of an on-going investigation. This is to provide assurance that Customer security responders are receiving a timely initial warning for high priority Security Incidents. Note: If priority is incremented during Triage, the shorter SLA will apply calculated from the time priority is increased, but no longer than the original SLA.
		Priority 2	45 mins		
3	**Containment or Escalation / Notification Time**	Priority 1	2 hours	95%	If a Case is classified as a Security Incident, once the investigation is complete, Accenture triggers mutually agreed pre-authorized containment actions (where applicable) or notifies the Customer with appropriate details within the agreed timeframe. This is to provide assurance that Incidents are managed in a
		Priority 2	4 hours		
		Priority 3	24 hours		
		Priority 4	72 hours		

					timely fashion consistent with their urgency and impact. This SLA is calculated according to the priority established during the investigation phase. Note: If priority is incremented during Investigation, the shorter SLA will apply calculated from the time priority is increased, but no longer than the original SLA
4	**MXDR Platform Availability**	N/A	N/A	99.9%	MXDR Portal, Customer-facing APIs and log ingestion availability excluding scheduled maintenance.

4. **Priority Definitions for Security Incidents:**

PRIORITY LEVEL	DESCRIPTION	EXAMPLES
Priority 1 (P1) – Critical	● Business Process and System functionality have been severely impacted or halted. ● System(s) or system data are rendered unsafe, inoperable, or compromised which includes data confidentiality, integrity, and availability partially or totally loss, privacy breach, recovery of the system not possible or time taken to recover is unpredictable.	Ransomware attack, DDoS attack
Priority 2 (P2) – High	● Business Process and system functionality have been seriously affected. ● System and/or system data are exposed to loss (Confidentiality), compromise (Integrity), or interruption (Availability) and time to recovery is predictable.	Successful unauthorized logins
Priority 3 (P3) – Medium	● Business process or system functionality may be moderately affected. ● A threat may exist against systems or system data, but no information was exfiltrated, changed, deleted, or otherwise compromised. These Incidents does not require an immediate response but requires additional investigation.	An exploitation attempt against a non-critical asset with no other indicator of compromise

Priority 4 (P4) – Low	● System and/or System data are not at risk. ● No effect to the organization's ability to provide all services to all users. ● These Incidents are useful for trend analysis and understanding applicable enhancements, if any, according to Defense in Depth approach.	An unsuccessful drive-by download attack blocked by security measure in place (e.g., as malicious File Download blocked by the network security appliance or removed / execution blocked by endpoint protection such as EDR / antivirus)

5. **Customer Responsibilities**
In addition to any obligations and requirements specified in the Order, the following is a non- exhaustive list of Customer obligations and responsibilities (collectively **"Customer Responsibilities"**) necessary for Accenture to deliver the MXDR Services and for Customer to access and use of the MXDR Services. Accordingly, Customer acknowledges and agrees that: (i) Accenture's ability to perform the MXDR Services during the Service Commitment is subject to Customer meeting all Customer Responsibilities during the Service Commitment; 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 Customer's act or omission inconsistent with the Customer 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 Service Commitment nor be deemed a breach of the Customer Agreement:

5.1 **Consent and Authorization Customer:** (i) explicitly confirms to Accenture that it has obtained all applicable consents and authority for Accenture to deliver the MXDR Services; (ii) gives Accenture explicit permission to perform the MXDR Services and to access and process any and all Customer data related to the MXDR Services; (iii) represents that such access and processing by Accenture does not violate any applicable law or any obligation Customer owes to a third party. Customer shall fully indemnify and hold harmless Accenture for any claims by any third parties related to the MXDR Services.

5.2 **CyberHub Installation.** Customer shall be solely responsible for successfully installing the CyberHub on Customer hardware or virtual infrastructure (as specified in the CyberHub Deployment Guide) and establishing the necessary network access to allow the delivery center(s) to remotely manage the CyberHub, and to allow the CyberHub to collect, compress, encrypt, and send event log data to the delivery center(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, Customer agrees to make any necessary changes to the configuration of the Device(s), as requested by Accenture, to conform with the supported format. Customer must provide all required hardware or virtual infrastructure necessary for the CyberHub and enable access to such hardware or virtual infrastructure by Accenture (as specified in the CyberHub Deployment Guide). Customer must configure their Devices to export event data in English. No other languages are supported for event data at this time.

5.3 **Reasonable Assistance.** Customer 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, Customer must provide Accenture remote access to the Device(s) and necessary administrative credentials to enable Accenture to perform the MXDR Services.

5.4 **Performance Standard.** The MXDR Services are provided as one element of the Customer's overall security control framework. Accenture will provide the MXDR Services with due care and skill, but notwithstanding anything to the contrary in the Customer Agreement, Customer acknowledges that the Services are not guaranteed to: (i) detect or identify all security or network threats to, or vulnerabilities of

Customer's networks or other facilities, assets, or operations; (ii) prevent all intrusions into or any damage to Customer's networks or other facilities, assets, or operations; or (iii) return control of Customer or third party systems where unauthorized access or control has occurred.

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

5.6 **Customer Outage.** Customer 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.

5.7 **Device Maintenance & Management.** Customer shall be solely responsible for: (i) maintaining its current maintenance and technical support contracts with Customer 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-FS; (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 Customer requires Accenture's assistance for remediation or resolution activities.

5.8 **Recommendations.** Customer 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.

5.9 **Reporting.** Customer 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 Customer is subject to in one or more territories in which Customer operates. Accordingly, Customer shall remain solely responsible for all such reporting requirements and Accenture shall have no liability in this regard whatsoever.

6. **Definitions**

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

"Affiliate Entity" 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 Affiliate Entities.

"Customer" shall mean the company or legal entity named in the Order.

"Customer's System" shall mean (as applicable) Customer'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.

"CyberHub" shall mean Accenture's log collection platform which is provided by Accenture and installed by Customer on virtual infrastructure. Further details on the CyberHub and Customer infrastructure

requirements can be found in the CyberHub deployment guide distributed by Customer's MxDR Service Delivery Lead (**"CyberHub Deployment Guide"**).

"Data Protection Laws" means all applicable data protection and privacy Laws that apply to the processing of personal data under this Agreement, including, as applicable, General Data Protection Regulation 2016/679 ("GDPR"), Federal Data Protection Act of 19 June 1992 (Switzerland), UK Data Protection Act 2018 (DPA 2018) and UK General Data Protection Regulation ("UK GDPR"), and any US state or federal laws or regulations pertaining to the collection, use, disclosure, security or protection of personal data, or to security breach notification, e.g., California Consumer Privacy Act of 2018 ("CCPA") as amended by the California Privacy Rights Act of 2020 ("CPRA").

"Device(s)" shall mean endpoint(s), security device(s) and/or product(s) owned or licensed by the Customer, that is specified in the Supported Product List – Full Stack (SPL-FS) and that receives MXDR Services e.g., servers, workstations, network firewalls, intrusion detection sensors, cloud-based applications and products.

"Forwarder" means a device or agent that collects data and sends it to another device. For example, an agent that collects data on a Customer server and forwards that data over the network to the CyberHub.

"List – Full Stack" or **"SPL-FS"** shall mean Accenture's list of supported products for the MxDR Services, which is available on the MxDR Portal.

"MxDR Portal" shall mean Accenture's web portal through which Customer may access and use the MXDR Services and which is made available by Accenture to Customer for use during the Service Commitment.

"MxDR Service Delivery Lead" shall mean Accenture's point of contact available to Customer 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.

"Playbook" means the agreed containment and escalation actions to be followed in response to an identified security event and may include automated containment activities using the SOAR Platform capabilities.

"Security Alert" shall mean a notification or warning generated by a monitored Device or by the SIEM Platform when a Security Event is detected, indicating the likely occurrence of one or more Security Events.

"Security Case" or **"Case"** shall mean a case created in the SIEM or SOAR Platform in response to one or more Security Alerts. A Security Case may be generated automatically by policies or analytics, or manually by the SOC analyst.

"Security Event" shall mean any observable activity or occurrence in a monitored Customer environment with potential security implications to the system or its environment. A Security Event may indicate a Security Incident is occurring.

"Security Incident" shall mean a Security Case that has been validated and found to show evidence of suspicious, malicious, or unauthorized activities that may jeopardize the confidentiality, integrity, or availability of a system or the data the system processes, stores, or transmits.

"SOC Infrastructure" shall mean individually or collectively, the SIEM Platform, SOAR Platform, MxDR Portal, CyberHub Accenture's Security Operations Center(s), data storage, SOC(s) log analysis processing, the MxDR Portal, and SOC(s) / Customer communication methods (i.e. phone, email, the MxDR Portal).

"Use Case" means the configurations used by the SIEM Platform to detect relevant security events from data sources.

"Use Case and Playbook Library" means Accenture's pre-existing library of Use Cases and Playbooks, used to accelerate configuration of the SOC Infrastructure.

ATTACHMENT 1 -TRANSPARENCY NOTICE -
ACCENTURE MXDR SERVICE – FULL STACK
Revision Date: December 1, 2023

This Transparency Notice describes how Accenture's **MXDR Service** collects and processes personal data.

MXDR SERVICE – OVERVIEW

The MXDR Service is a managed security service comprising: a multi-tenant instance of Google Chronicle SIEM and SOAR, native threat intelligence, log ingestion from supported Customer devices, security monitoring, SIEM & SOAR platform maintenance, and may include access to an MXDR Service online portal.

Further information about the MXDR Service is included in the customer's Agreement and Schedule.

PERSONAL DATA, COLLECTION & PROCESSING

DATA PRIVACY – ROLES OF ACCENTURE AND CUSTOMER. With respect to personal data that Accenture is required to process to deliver the MXDR Service, the Customer acts as the **'Controller'**, and Accenture acts as a **'Processor'**, as further detailed in the section **'Collection & Processing –Customer-Controlled Personal Data'** below.

Accenture also collects and processes personal data as a **"Controller"** (e.g., in order to provide Customer with access and use of the MXDR Service online portal), as further detailed in the section **'Collection & Processing – Accenture-Controlled Personal Data'** below.

COLLECTION & PROCESSING –CUSTOMER-CONTROLLED PERSONAL DATA. The following table details the personal data that Accenture collects, processes and stores on behalf of a Customer, the applicable data subjects and the nature and purpose of processing.

NOTE: Accenture has no control over the content of the personal data processed by Accenture in delivering the MXDR Service on behalf of a Customer:

CATEGORY	PERSONAL DATA	DATA SUBJECTS	NATURE AND PURPOSE
Authentication Data*	● User ID ● Password ● Personal data contained in control questions and other information necessary to verify identity when accessing and/or using the MXDR Service online portal.	Individual(s) appointed by a Customer to access and use the MXDR Service online portal.	Personal data stored and processed by Accenture through the MXDR Service online portal to enable Customer authorized personnel to use and access the MXDR Service and the MXDR Service online portal in accordance with the Agreement.

Customer Care Data*	● Title ● Name ● Business E-mail ● Address ● Telephone Number ● Business Address. ● Personal data contained in a Customers request for support through chat, email, voicemail, SMS/MMS (NOTE: Personal data may include Security Data (see below) processed by Accenture in connection with the provision of MXDR Service, as may be required for Customer to detail its request and for Accenture to action such request for support e.g., location data, network activity data, authentication data).	Individual(s) appointed by a Customer to access and use the MXDR Service online portal and to interact with Accenture during the delivery of the MXDR Service. Customers personnel, customers, suppliers, and any persons interacting electronically in or with Customer's networks.	Personal data stored and processed by Accenture, including through the MXDR Service online portal, in order to provide technical support to Customers during their use of MXDR Service.
Security Data* (Monitored Data)	● Personal Data contained in security events and activity logs e.g., IP Address, Email Address MAC Address, Host, Usernames, Device IDs and similar Unique Identifiers, Event ID, Process ID, Machine ID, WAP and/or Web Logs Files, Browsing Logs, Session Logs, Location Data (device and network locale).	Customer's personnel, customers, suppliers, and any persons interacting electronically in or with Customer's networks.	Personal data that is part of network diagrams and can be part of the security logs transmitted by the Customer's monitored device(s) to the log collection platform (LCP) managed by Accenture to perform the MXDR Service, in accordance with the Agreement. Once collected by the LCP, such Security Data is stored and remotely accessed by MXDR delivery resources as necessary for analysis/investigation purposes, anytime a security alert is triggered.
Security Data* (Triage, Investigation, Escalation, and Containment using an	● Personal data contained in artifacts subject to an investigation that is stored within Customer	Customer's personnel, customers, suppliers, and any persons interacting	Personal data that may be contained in Customers' artifact(s) that is subject to investigation and

EDR tool, if applicable)	environment and accessed by Accenture Analysts in conducting an investigation e.g., Individual Identifiers and Characteristics, Financial Information, and/or Special Categories of Data.	electronically in or with Customer's networks. **NOTE: The personal data referenced may be gathered as part of an investigation, however, such personal data is only used if relevant to the investigation and is otherwise ignored.**	viewed by Accenture Analysts during an investigation.

***NOTE: The personal data indicated above is NOT expected to include Special Categories of personal data.**

COLLECTION & PROCESSING - ACCENTURE-CONTROLLED PERSONAL DATA. In order for Accenture to deliver the MXDR Service (e.g., in order to provide a Customer with access and use of the MXDR Service online portal), Accenture collects and processes Customer provided business contact information (such as name, title, business mailing addresses, email address, or phone number) and certain additional personal data related to individuals designated by a Customer as contacts for the MXDR Service and users of the MXDR Service online portal. The rights and obligations of Accenture and the Customer with respect to the processing of Accenture-controlled personal data are (unless otherwise agreed by Accenture) specified in the Privacy Statement published by Accenture at www.accenture.com/us-en/support/security/security-legal-terms.

DURATION OF PROCESSING

DURATION OF PROCESSING OF -CUSTOMER-CONTROLLED PERSONAL DATA. Customer-controlled personal data will be retained by Accenture for the duration of a Customer's subscription to the MXDR Service. Following the expiration or earlier termination of a Customer's subscription to the MXDR Service, or at an Customer's request, Accenture will (and will require that its Sub-processors) promptly and securely delete (or return to the Customer) all personal data (including existing copies), unless otherwise required or permitted by applicable laws. Unless otherwise agreed, Accenture will comply with a Customer's deletion instruction as soon as reasonably practicable and within a maximum period of 180 days.

DURATION OF PROCESSING OF ACCENTURE-CONTROLLED PERSONAL DATA. Accenture controlled personal data will be processed and retained by Accenture in accordance to the personal data retention schedule included in the Privacy Statement published by Accenture at www.accenture.com/us-en/support/security/security-legal-terms

SUBPROCESSSOR LIST -
ACCENTURE MXDR SERVICE – FULL STACK
Revision Date: December 1, 2023

MANAGED DETECTION & RESPONSE SERVICES. Accenture engages data processor(s) ("Subprocessor(s)") to support the delivery of Accenture's Managed Extended Detection & Response Services **("MXDR Service")**.

ACCENTURE AFFILIATE SUBPROCESSOR(S). Accenture engages one or more of the affiliates listed below as a Subprocessor(s) with respect to the MXDR Service, and any additional locations as described in the Order Confirmation or Statement of Work:

Delivery – Staffing Locations – US Customers

MXDR Services for Customers headquartered in the United States will be provided by one or more of the following Accenture affiliates in the following jurisdictions:

ACCENTURE AFFILIATE	COUNTRY	FULL STACK GLOBAL
Accenture Solutions Pvt. Ltd	India	Global SOC 24x7x365
Accenture Inc (Philippines)	Philippines	Global SOC 24x7x365
Accenture Services, s.r.o	Czech Republic	Global SOC 24x7x365
Accenture Outsourcing Services SA	Spain	Global SOC 24x7x365
Tecnilogica Ecosistemas SA	Spain	Global SOC 24x7x365
Accenture SL	Spain	Global SOC 24x7x365
Accenture do Brasil Ltda	Brazil	Global SOC 24x7x365
Accenture Technology Solutions S.A de CV	Mexico	Global SOC 24x7x365
Accenture SC ATC	Mexico	Global SOC 24x7x365
Accenture LLP	USA	Service Delivery Lead (business hours)

Delivery – Staffing Locations – International Customers

MXDR Services for Customers headquartered in Australia, United Kingdom, Germany, Japan, France, Netherlands, Switzerland, Finland, Norway, Italy, Belgium, Ireland, Sweden, Spain, Luxembourg, Austria and Denmark and other agreed-upon countries will be provided by one or more of the following Accenture affiliates in the following jurisdictions:

ACCENTURE AFFILIATE	COUNTRY	FULL STACK GLOBAL

Accenture Solutions Pvt. Ltd	India	Global SOC 24x7x365
Accenture Inc (Philippines)	Philippines	Global SOC 24x7x365
Accenture Services, s.r.o	Czech Republic	Global SOC 24x7x365
Accenture Outsourcing Services SA	Spain	Global SOC 24x7x365
Tecnilogica Ecosistemas SA	Spain	Global SOC 24x7x365
Accenture SL	Spain	Global SOC 24x7x365
Accenture do Brasil Ltda	Brazil	Global SOC 24x7x365
Accenture Technology Solutions S.A de CV	Mexico	Global SOC 24x7x365
Accenture SC ATC	Mexico	Global SOC 24x7x365
Accenture LLP	USA	Service Delivery Lead (business hours)
Accenture S.R.L. Argentina	Argentina	Service Delivery Lead (business hours)
Accenture Australia Pty Limited	Australia	Service Delivery Lead (business hours)
Accenture SpA	Italy	Service Delivery Lead (business hours)
Accenture Technology Solutions Srl	Italy	Service Delivery Lead (business hours)
Accenture Japan Ltd	Japan	Service Delivery Lead (business hours)
Accenture Pte Ltd	Singapore	Service Delivery Lead (business hours)
Accenture Solutions Co. Ltd	Thailand	Service Delivery Lead (business hours)
Accenture (UK) Limited	United Kingdom	Service Delivery Lead (business hours)

Technical Platform Support

Technical platform support will be provided by the following Accenture affiliates from the following jurisdictions. Technical support roles will not ordinarily require access to personal data, but may have access to incidental personal data:

ACCENTURE AFFILIATE	COUNTRY	TECHNICAL SUPPORT PROVIDED DELIVERY OPTIONS

Accenture Australia Pty Limited	Australia	MXDR Platform Support
Accenture, Inc.	Canada	MXDR Platform Support
Accenture Solutions Pvt. Ltd	India	MXDR and ServiceNow Platform Support
Accenture Inc (Philippines)	Philippines	MXDR and ServiceNow Platform Support
Accenture Outsourcing Services SA	Spain	MXDR Platform Support
Tecnilogica Ecosistemas SA	Spain	MXDR Platform Support
Accenture SL	Spain	MXDR Platform Support
Accenture (UK) Limited	United Kingdom	MXDR Platform Support
Accenture LLP	USA	MXDR and ServiceNow Platform Support

THIRD PARTY SUBPROCESSOR(S). Accenture currently uses the following third-party Subprocessor(s) to provide certain services, as detailed in the table below, necessary to deliver MXDR Service. Prior to engaging any third-party Subprocessor(s), Accenture performs due diligence to evaluate a Subprocessor(s)' privacy, security and confidentiality practices, and executes an agreement implementing its applicable obligations with each Subprocessor(s), including Standard Contractual Clauses to cover any international data transfer as required under applicable data protection laws.

<table>
<tr><th>THIRD PARTY SUBPROCESSOR(S)</th><th colspan="2">SERVICES PROVIDED AND RELATED PURPOSE</th><th>COUNTRY / REGION WHERE DATA IS STORED</th></tr>
<tr><td rowspan="4">Google LLC, its relevant affiliates, including Chronicle LLC; Cyarx, Inc t/a Siemplify; and Mandiant, Inc., and their respective subprocessors as may be updated by Google at the links below:

Subprocessors for Google SecOps services: www.cloud.google.com/terms/secops/subprocessors

Subprocessors for Google Cloud Platform: www.cloud.google.com/terms/subprocessors</td><td>Google Cloud Platform</td><td>Cloud and infrastructure hosting services for the SIEM & SOAR platforms and CyberHub.</td><td rowspan="4">USA
EU: Belgium, Netherlands, Finland
Singapore (asia-southeast1)
UK (europe-west2)
Australia (australiasoutheast1)
Japan (asia-northeast1)
India (asia-south1)</td></tr>
<tr><td>Chronicle SIEM</td><td>SIEM platform (including security event data ingested in the course of the services).</td></tr>
<tr><td>Chronicle SOAR</td><td>SOAR platform</td></tr>
<tr><td>Google AI tools (Vertex AI, Gemini, etc.)</td><td>Google's proprietary foundation models or LLMs may be used during an engagement as part of regular service delivery. Such capability may</td></tr>
</table>

		necessitate including personal data in the prompts.	
Okta, Inc. and the following subprocessors as may be updated by Okta at: www.okta.com/trustandcompliance/#subprocessorinformation	Authentication service (used to authenticate users accessing the MXDR Service online portal).		USA EU
Microsoft Corporation, and its subprocessors as may be updated by Microsoft at: www.servicetrust.microsoft.com/DocumentPage/badc200c 02ab-43d9-b092-ed9b93b9b4a8	Entra ID	Authentication service (used to authenticate users accessing the MXDR Service online portal).	The closest region available based on Customer location (available regions are listed at: www.azure.microsoft.com/enus/explore/globalinfrastructure/dataresidency/#overview)h
	Azure Open AI	Azure Open AI service may be used during an engagement as part of regular service delivery. Such capability may necessitate including personal data in the prompts.	
Amazon Web Services, Inc. and its subprocessors as may be updated by AWS at: www.aws.amazon.com/compliance/sub-processors/	Amazon Bedrock may be used during an engagement as part of regular service delivery. Such capability may necessitate including personal data in the prompts.	The closest region available based on Customer location (available regions are listed at: www.docs.aws.amazon.com/bedrock/latest/userguide/bedrockregions.html	
ServiceNow, Inc. and the following subprocessors as may be updated by ServiceNow, Inc at: www.servicenow.com/content/dam/servicenow assets/public/en-us/doctype/legal/servicenow-subprocessors.pdf	Cloud based tool integrated with the MXDR platform to support Customer communications and facilitate service delivery.	Netherlands, Ireland	