MANAGED DETECTION AND RESPONSE
SUPPLEMENTAL PRODUCT TERMS

These Managed Detection and Response Supplemental Product Terms ("***Supplemental Product Terms***") is an addendum to, supplements, and is made part of the General Terms located at https://arcticwolf.com/terms/general-terms/ (or such other similarly executed General Terms or negotiated Solutions Agreement) in place between the parties (the "***General Terms***") (the Supplemental Product Terms and General Terms collectively referred to herein as the "***Agreement***") and, subject to the terms herein, governs Customer's use of the Managed Detection and Response solution (the "***Solution***"). These Supplemental Product Terms apply to the extent Customer has subscribed to the Solution either as a standalone offering or as part of Customer's subscription to other Products. Any capitalized terms not otherwise defined herein have the same meanings as those noted in the General Terms. If there is any conflict between these Supplemental Product Terms and the General Terms, then these Supplemental Product Terms shall control.

1. SOLUTION.

1.1 The Solution may be licensed separately or as part of a Security Operations Bundle as more fully described at https://arcticwolf.com/terms/bundles-tiers/ (each a "Bundle"). The Solution includes the following Components:

Component	
Software	The object form of any software, including any operating system software included in the Equipment, and add-ons offering enhanced features and functionality made generally available to Arctic Wolf customers from time-to-time
Equipment	Virtual network appliances (vSensor) or physical sensors (Sensor)
Services	Support, onboarding services, and services provided by Security Services, and Cyber Resilience Assessment ("***CRA***")[1]
Platform	One (1) vSensor 100 series Unlimited data ingestion Access to the Unified Portal (formerly called Customer Portal) Use of the Arctic Wolf Agent ITSM Ticketing Integrations (if elected by Customer) 90-day Log Retention (unless another retention period is purchased by Customer and set forth on an Order Form)

1.2 The Solution and its Components are more fully described in the MDR Product Description located at https://docs.arcticwolf.com/ (the "***Product Description***") and incorporated herein by reference. Any capitalized terms not otherwise defined in these Supplemental Product Terms or the General Terms shall have the definition in the Product Description.

2. DATA; ARCTIC WOLF TECHNOLOGY.

2.1 Data. Data processed by Arctic Wolf in the delivery of the Solution includes:

2.1.1 Solutions Data. "***Solutions Data***" means the operational system log data and any other information provided by Customer in furtherance of its use of the Solution and which Customer may elect to submit to Arctic Wolf using the Solution, including, but not limited to operational values, event logs, and network data such as flow, HTTPS, TLS, DNS metadata, cursory inventory data, operating systems and versions, users and groups from Active Directory, system level inventory, event data, and network vulnerability data, but excluding Threat Intelligence Data.

2.1.2 Customer acknowledges and agrees that Arctic Wolf, in the performance of the Solution, may use a GeoIP service (i.e., a method of locating a computer terminal's geographic location by identifying that terminal's internet protocol ("IP") address) to report the location of Customer's IP address.

2.2 Data Storage. Customer's Confidential Information is stored in Arctic Wolf's third-party service provider data centers specified by the Platform location included on Customer's Order Form (or within the General Terms, if identified) and may be processed as set forth in the Agreement and Data Processing Addendum.

2.3 Data Transmission. Customer's Data will be transmitted to Arctic Wolf via a secure tunnel in compliance with the requirements of Arctic Wolf's then-current SOC2 Type II Report and ISO27001 certification.

3. **TERMINATION.** Except as otherwise required by law, Arctic Wolf will remove, delete, or otherwise destroy all copies of Confidential Information in its possession upon the earlier of the following: (i) the return of the Equipment, if applicable, to Arctic Wolf, or (ii) one hundred-twenty (120) days following expiration or termination. Notwithstanding anything contrary in this Agreement, should Customer fail to return any Equipment within ninety (90) days following discontinuation of use of the Equipment or termination or expiration of this Agreement, Customer will be liable for the replacement cost of the Equipment, which shall be due and owing upon receipt of the invoice from Arctic Wolf or the Authorized Partner, and Arctic Wolf shall have no liability to Customer for a breach of Data included on such unreturned Equipment and Customer shall be liable for any breach of the Arctic Wolf Technology contained within such unreturned Equipment.

4. **MICROSOFT US GOVERNMENT COMMUNITY AND HIGH US GOVERNMENT COMMUNITY ENVIRONMENT MONITORING.** In the event Arctic Wolf monitors applications for Customer within the Microsoft US Government Community

[1] CRA is available subject to the terms of the Cyber JumpStart Portal Supplemental Product Terms located at https://arcticwolf.com/terms/.

environment or US Government Community High environment (each a “GCC environment”) as part of the delivery of the Solutions, Customer understands and agrees as follows:

4.1 Arctic Wolf is not FedRAMP compliant.

4.2 Only Arctic Wolf supported and integrated applications will be monitored in the GCC environment.

4.3 Solutions Data (i) may be accessed by Arctic Wolf, its Affiliates, and any third-party providers, from locations outside the United States, and (ii) may be accessed by persons who are not United States citizens.

4.4 Arctic Wolf does not require access to or delivery of Customer’s Controlled Unclassified Information (“CUI”) and in the event information classified as CUI is provided, Arctic Wolf may immediately cease ingestion of Customer Solutions Data without further liability to Customer.

4.5 Arctic Wolf will provide reasonable cooperation to Customer in the event of a data breach involving Solutions Data including, but not limited to assistance in responding to any government or regulatory inquiries.

4.6 Certain Microsoft log sources may be in beta and, consequently, Arctic Wolf makes no representations as to the delivery of the Solutions related to any such beta Microsoft log sources.

4.7 Customer will immediately notify Arctic Wolf of non-consent or any change in consent and any monitoring of Customer’s GCC environment will immediately cease without further liability to Arctic Wolf.