Managed Detection and Response
Solution Terms

This Managed Detection and Response – Solution Terms ("***Solutions Terms***") describes the Managed Detection and Response Solution (the "***Solution***"). The Solution, if purchased by Customer as evidenced by Customer's election on an Order Form, will be provided in accordance with the terms set forth herein and the Solutions Agreement (the "***Solutions Agreement***") made by and between Customer and Arctic Wolf Networks, Inc. ("Arctic Wolf"). Any capitalized terms not otherwise defined herein shall have the meaning set forth in the Solutions Agreement.

Solution. 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") and 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 appliances or physical sensors
Services	Support, onboarding services, and services provided by Security Services, all as described herein, and Cyber Resilience Assessment ("***CRA***")
Platform	One (1) vSensor 100 series Unlimited data ingestion Access to the 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)

The Solution is delivered by the Security Services team which is comprised of two (2) teams: (1) the Concierge Security™ Team ("***CST***"), and (2) the Security Operations Center ("***SOC***").

Specific features and functionality provided as part of the Solution include:

- collection of Solutions Data and Points of Contact Information, including Customer's system logs, from Customer's systems using Equipment,
- analysis by Arctic Wolf Security Services of both Equipment and log data through the correlation of Solutions Data with threat and vulnerability information,
- scanning of Customer's internal and external systems,
- escalation of Security Incidents (as defined below) in need of attention by Customer as set forth herein,
- advisory recommendations intended to improve Customer's security robustness,
- calculation of Customer's Security Score, as more fully described below,
- Access to additional modules, if licensed by Customer as reflected on an Order Form (as more fully described below)[1],
- Response Actions[2] (as more fully described below),
- Cyber Resilience Assessment ("***CRA***") subject to the terms set forth at https://arcticwolf.com/terms/cyber-jumpstart-portal-subscription-agreement/, and
- regular summary Executive Dashboard reports, as described herein and the Documentation.

NOTE: The performance of the Solution, including specifically, notification of Emergencies or Security Incidents, as defined below, will not commence until after initial deployment is complete. The performance of (i) remediation services for Security Incidents (as defined below), (ii) the re-imaging of Customer's systems, or (iii) change of policy settings is outside the scope of the Solution.

Data Transfer. Any Equipment provided by Arctic Wolf to Customer is physically or virtually deployed to monitor Customer's system traffic. Such system traffic is augmented with additional sources of log data, as required, to deliver the Solution. Except as otherwise set forth in the Solutions Agreement, all such system traffic information is deemed Solutions Data. Essential log sources will be determined by Customer and Arctic Wolf during the onboarding process following the Order Form Effective Date.

Any Solutions Data and Points of Contact Information will be securely transmitted to Arctic Wolf in accordance with the Agreement. The Solution operates redundantly with Customer's High Availability (HA) specifications to minimize potential service interruptions. Hosting providers used by Arctic Wolf to deliver the Solution may experience service interruptions and service outages outside the control of Arctic Wolf. If such a hosting provider issues an outage notice that could materially impact delivery of the Solutions, Arctic Wolf will use commercially reasonable efforts to promptly notify Customer about the outage and communicate the planned recovery time provided by the hosting provider.

Solutions Data and Points of Contact Information may include personal or confidential information. Customer will provide any such personal or confidential information in accordance with the terms of the Solutions Agreement.

[1] Existing Arctic Wolf MDR Customers may be, subject to authorization by Arctic Wolf, eligible to license Log Search capabilities only. In such event, Log Search will be included on an Order Form.
[2] Response Actions were formerly referred to as Host Containment Actions.

Data Retention. Arctic Wolf will store Solutions Data and Points of Contact Information for the Data Retention period specified in Customer's then-current Order Form. Solutions Data and Points of Contact Information may be returned to Customer in accordance with the terms of the Solutions Agreement.

Data Storage. Arctic Wolf will store raw Solutions Data and Points of Contact Information in the platform location set forth on an Order Form.

Updates & Upgrades. Automated maintenance and update cycles to the Equipment will be performed remotely by Arctic Wolf Security Services. Arctic Wolf will provide any services related to the replacement or upgrades of the Equipment. Any costs related to such Equipment replacement or upgrades will be in accordance with the Solutions Agreement.

Security Incidents. The CST supporting Customer is available 8:00 am to 5:00 pm (based on the time zone within which the CST is located), Monday through Friday (excluding holidays) and will provide Concierge Security™ Tier support in accordance with the Concierge Security™ Tier selected by Customer, as applicable. The SOC is available 24 hours a day, 7 days a week, including holidays. Customer may schedule specific activities with their CST, in accordance with Customer's Concierge Security™ Tier, as applicable, by contacting the Arctic Wolf SOC at security@arcticwolf.com. Arctic Wolf Security Services will acknowledge any schedule request submitted by Customer to security@arcticwolf.com within one (1) hour of receipt of such request. Arctic Wolf Security Services will provide an estimate of response time determined by scope, size, and urgency.

Arctic Wolf Security Services will notify and escalate to Customer any Security Incidents, the definition of which will be agreed upon by Customer and its CST during the Subscription Term after transition from the deployment team, discovered by Arctic Wolf within two (2) hours of Arctic Wolf's discovery of such Security Incident. Arctic Wolf standard Security Incident notification process is through a ticket to the Customer; however, Arctic Wolf and Customer may agree to alternate notification processes. Security Incident notifications will include a description of the Security Incident, the level of exposure, and a suggested remediation strategy. Customer is responsible for implementing, in its sole discretion, any remediation strategies identified by Arctic Wolf. Customer may request validation by Arctic Wolf that any such implemented remediation strategies are working as expected.

Emergencies. Following transition from the deployment team to the CST, Customer and the CST will agree on and document which Security Incidents will be defined as an ***"Emergency"***. Emergencies will typically include the discovery of ransomware and other alerts that could cause degradation/outage to Customer's infrastructure security. Arctic Wolf will escalate Emergencies to Customer within thirty (30) minutes of Arctic Wolf's discovery of the Emergency.

Any Emergency identified by Customer can be escalated to Arctic Wolf's Security Services by calling: 1-888-272-8429, option 2 or by calling the toll-free number based on the location from which you are calling found at https://arcticwolf.com/toll-free/. Customer must describe the Emergency in the initial call and Arctic Wolf will respond within 5 minutes. In addition, with respect to any urgent inquiries, Customer may contact Arctic Wolf's Security Services by calling: 1-888-272-8429, option 2 or using the applicable toll-free number for the location from which Customer is located as set forth at https://arcticwolf.com/toll-free/.

Ticketing Integration (included in the Platform component of the Solutions). At Customer's election and based on configurations and permissions collected from Customer, Arctic Wolf may employ an integration to transfer data into and out of Customer's third-party ticketing system, provided Arctic Wolf supports integrations to such systems.

Scans. On a monthly basis, Arctic Wolf will use the Solution to conduct external vulnerability assessment scans of Customer's environment. As part of these scans, vulnerability and exploit information will be normalized and correlated with other data sources to determine Customer's Security Score and prioritization of any identified remediation strategies. Arctic Wolf will deliver to Customer a summary security report that includes Security Incident and Emergency notification activities on a monthly and quarterly basis.

Coverage Score (fka Configuration Score or Security Score). Customer's Coverage Score is provided as part of the Solution for illustrative and informational purposes only and may be used by Customer for internal benchmarking. The Coverage Score is based on certain information related to the results of the Solution within Customer's environment and is compiled using the Solutions Data made available to Arctic Wolf in conjunction with its delivery of the Solution. Customer's Coverage Score will be communicated in Customer's summary reports in addition to being available on Customer's online Executive Dashboard. Customers may elect to compare their Coverage Score against industry averages from organizations in the same industry vertical to assess how Customer is performing against industry norms.

Response Actions. Arctic Wolf may, if agreed with Customer, using commercially reasonable efforts, perform response actions, including application/removal of host containment, enable/disable user accounts, block URLs, modify deny lists and iprules, retrieve files, kill processes, and run files or scripts, as described below (collectively, "***Response Actions***"), provided that Customer has deployed the Arctic Wolf Agent, such other agreed upon third party agents, and/or configured the appropriate integrations. In the event Customer has deployed multiple agents, including the Arctic Wolf Agent, within its environment, Arctic Wolf will attempt to contain first using the Arctic Wolf Agent. Based on (i) information provided by Customer to its CST following initial deployment, (ii) a mutually agreed upon response and escalation process set forth in Customer's onboarding document, as updated upon agreement by Customer and its CST during the Subscription Term, and (iii) Arctic Wolf is provided appropriate access to applicable third party security applications, if any, within Customer's environment, the Security Services team may remotely isolate a Customer endpoint device(s), network appliance, or user account that shows evidence of compromise or other suspicious activity. When the Security Services team identifies certain indicators of attack on an endpoint, network device, or user account, the Response Action will be initiated systematically, in accordance with the agreed upon response and escalation process, and subject to the requirements set forth herein, to rapidly quarantine the suspected compromised system or account.

The indicators of attack that may drive Response Actions include those relating to ransomware (and other types of advanced malware), malicious command-and-control (C2) activity, or active data exfiltration attempts.

The endpoints, network, or user accounts participating in the Response Actions will receive a notification and the Response Actions will be detailed in an incident ticket. If using the Arctic Wolf Agent, the Customer Portal will display the Customer endpoints that are currently in a contained state. Security Services team is available to Customer to answer questions or provide detailed information on any endpoints, network, and/or user accounts participating in the Response Action.

Pre-requisites for Response Actions –

Customer must:

- Complete a checklist in partnership with its CST, which will include further definition, including but not limited to the scenarios where Arctic Wolf will and will not perform Response Actions including specific information regarding which endpoints/servers, network appliances, and/or user accounts where Response Actions will and will not be performed, the times of day for Response Actions to occur, notification and escalation preferences related to Response Actions (If parties have not defined the Response Actions pertaining to Customer endpoints, network, and/or user accounts, Arctic Wolf will take Response Actions in accordance with Arctic Wolf's standard response and containment policy);
- Provide Arctic Wolf with technical permissions to allow Arctic Wolf to perform Response Actions within Customer's environment (Customer understands that should Arctic Wolf have invalid access or is blocked from initiating Response Actions, Arctic Wolf will be unable to provide the agreed upon Response Actions);
- Implement appropriate internal procedures and oversight to the extent Customer utilizes the configuration of workflows and processes, including but not limited to Response Actions and other similar functionalities; and
- Enable software or services, in Customer's discretion, to permit necessary visibility into Customer's environment to perform Response Actions.

Active Directory Deception. If licensed and implemented by Customer either as a standalone or bundled feature within the Solution, Customer may deploy Active Directory Deception ("AD Deception"). With AD Deception, Customer creates, configures, and maintains Active Directory decoy account(s) intended to act as a deception trap within Customer's network.

The Active Directory decoy account is not intended to participate in normal business activities and should not log-in to Customer's system. The Active Directory decoy account is intended to provide a high-fidelity mechanism for detecting abnormal activity yielding no false positives. If a decoy account is deployed by Customer, Customer is responsible for creating, configuring, and maintaining the decoy account. The naming of the decoy account should follow Customer's account naming conventions. Arctic Wolf will provide reasonable guidance and assistance to Customer in the configuration of such decoy accounts. Customer will provide Arctic Wolf details of the decoy account to Arctic Wolf for monitoring. Customer understands that any changes to the decoy account configurations may impact the security of Customer's environment.

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 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:

1. Arctic Wolf is not FedRAMP compliant.
2. Only Arctic Wolf supported and integrated applications will be monitored in the GCC environment.
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. 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;
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;
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; and
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.

Additional Modules.

- **Cloud Detection and Response ("CDR").** Customers may license CDR for Amazon Web Services (AWS), Microsoft Azure, and any such other cloud IaaS and SaaS environments that Arctic Wolf may agree to monitor. Customer's election to license such CDR feature will be set forth on an Order Form. If licensed as part of the Solution, Arctic Wolf will provide detection and response for the respective IaaS and SaaS environments as described herein. Arctic Wolf is not responsible for any software and/or application changes made by the cloud IaaS and SaaS providers which affect or impair the CDR feature.

- **Data Explorer**. Customer may elect to license the Data Explorer feature. Should Customer subscribe to such feature, Data Explorer will be included on an Order Form. Data Explorer allows Customer to access historical data for quick, ad-hoc investigations and self-service reporting. Customer may identify and remediate risk in Customer's environment and may take appropriate actions when needed depending on results. Data Explorer includes (i) access to the prior ten (10) days of event and analyzed data, and (ii) Log Search[3] which permits Customer to query its retained Solutions Data in 30-day increments.

[3] Legacy customers licensing Log Search are entitled to Log Search only.

- **Data Explorer – Lite**. Customers licensing MDR as part of a Bundle will receive Data Explorer - Lite which includes access to the prior three (3) days of event data.

  For purposes of Data Explorer and Data Explorer-Lite, analyzed data includes parsed, normalized, and enriched data processed by the Arctic Wolf platform, however, not all logs ingested by Arctic Wolf will be parsed, normalized, or enriched. Event data is a collection of analyzed observations Arctic Wolf finds to be interesting from a security standpoint.

- **Application and SaaS Integrations.** Customers may license application and SaaS integrations as may be offered by Arctic Wolf. Customer's election to license such integration will be set forth on an Order Form. If licensed as part of the Solution, Arctic Wolf will provide detection and response for the respective integrated environments as described herein. Arctic Wolf is not responsible for any software and/or application changes made by the third-party application provider which affect or impair the integration with such third-party application.