AURORA ENDPOINT DEFENSE
SUPPLEMENTAL PRODUCT TERMS

These Aurora Endpoint Defense 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 Aurora Endpoint Defense solution(s) set forth on an Order Form (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.

BY CLICKING ON THE APPROPRIATE BUTTON WITHIN THE SOLUTION, OR BY INSTALLING, ACCESSING OR USING ANY THE SOLUTION, YOU ARE AGREEING TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, OR IF YOU ARE NOT AUTHORIZED TO ACCEPT THE TERMS AND CONDITIONS OF THIS AGREEMENT ON BEHALF OF CUSTOMER, DO NOT COPY, INSTALL, ACCESS OR USE THE SOLUTION.

1. SOLUTION.

1.1 The Solutions are more fully described in the applicable 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.

1.2 The Solutions may include, to the extent identified on an Order Form, the Software and/or Services and applicable Documentation pertaining to Aurora Endpoint Solutions. "***Services***" means any paid service made available by or on behalf of Arctic Wolf hereunder and identified as an Arctic Wolf service, including Technical Support Services and cloud services made available via the Software, but excluding any Third-Party Items, and set forth on an accepted Order Form. "***Software***" means any Arctic Wolf proprietary enterprise software (and any licensed third-party software embedded therein) in object code form only (and not source code) provided hereunder, including server software, client software, personal computer software and interfaces and Documentation. Any upgrades, updates or modified versions of the Software that may be provided to Customer excludes any Customer or any third party provided: (i) software; (ii) content; (iii) services, including internet connectivity, systems, wireless networks and non-Arctic Wolf websites; and (iv) devices, servers, equipment and other hardware products (collectively, "***Third Party Items***").

1.3 Any Technical Support Services acquired by Customer, including as part of a subscription, may be provided by Arctic Wolf or an Authorized Partner, subject to Customer's agreement directly with such Authorized Partner. To the extent provided by Arctic Wolf, performance of such Technical Support Services are provided subject to: (i) the General Terms, as supplemented by these Supplemental Product Terms; (ii) the Technical Support Services program description found at https://docs.arcticwolf.com/ (or such other site as may be made available by Arctic Wolf from time-to-time), as may be amended by Arctic Wolf and which is incorporated herein by this reference; and (iii) Customer's payment of all applicable fees for the requisite time period and number and type of licenses acquired by Customer pursuant to an accepted Order Form. Customer agrees that it may be required to update Software and/or Third Party Items to continue to access or use the Solution, Third Party Items or portions thereof.

2. DATA; ARCTIC WOLF TECHNOLOGY.

2.1 Data. Data processed by Arctic Wolf in the normal delivery of the Solution includes, depending on the Solution deployed:

2.1.1 Aurora MDR Data. If Aurora Managed Endpoint Defense on Demand or Aurora Endpoint Defense are included in the subscription, Arctic Wolf may process Aurora MDR Data. "***Aurora MDR 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 system log data and any other information provided by you in furtherance of your use of the Solutions and which you may elect to submit to Arctic Wolf through the Solutions, 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. Personal data included in the of data to deliver these Solutions may include IP addresses, first name, last name, username, user unique identifier., but excluding Threat Intelligence Data.

2.1.2 Endpoint Solutions Data. If Aurora Endpoint Defense, Aurora Protect, Aurora Protect Server, or Aurora Protect Mobile are included in the subscription, Arctic Wolf may process Endpoint Solutions Data. ***"Endpoint Solutions Data"*** may include usernames, first name, last name, email address, IP addresses, username unique identifier, user privileges, device name, account status, password status, password age, country code, account type, assigned workstations, failed login attempts, roaming configuration, removable media events (insertion, removal, file copy), script execution events (JScript, VBScript, and VBA macro script, PowerShell), Windows event logs, WMI events, SMS sender ID, SMS message contents and hyperlinks from unknown senders.

2.2 Data Storage. Customer's Confidential Information is stored in Arctic Wolf's third-party service provider data centers selected by Customer and specified within the Unified Portal and may be processed as set forth in the Agreement and Data Processing Addendum.

2.3 Potentially Malicious Code and Anonymous Data.

2.3.1 Transmission of Files. Customer acknowledges that a feature of certain Solutions is to facilitate analysis of files and processes (including portable executable files, meta data, systems files, dll files, binary files, and/or other executable code, including those which may from time to time be embedded in other file types) that exist on, or are being introduced to Customer's devices ("Files") to identify potential or actual malicious code, malware or other intrusive artifacts or processes therein ("Potentially

Malicious Code"). Customer therefore acknowledges and agrees that, in certain configurations, to function optimally, the applicable Solution may transmit Files to servers owned or controlled by Arctic Wolf or may otherwise analyze Files.

2.3.2 Anonymous Data. Arctic Wolf may reduce Potentially Malicious Code to a unique hash, and Arctic Wolf may deconstruct, analyze and catalogue Potentially Malicious Code to determine functionality and potential to cause instability or damage to Customer's devices. Arctic Wolf may also use the unique file hash to identify files on other systems as Potentially Malicious Code and use and distribute the unique file hash to promote awareness, detection and prevention of internet security risks, in which case the unique file hash will be without attribution to Customer, Customers' operations, systems, networks or devices (individually and collectively, "***Anonymous Data***"). Arctic Wolf may also extract, compile, synthesize, and analyze non-personally identifiable data transmitted by Solutions, or information resulting from Customer's use of or access to the Solution, in each case to the extent such data or information only includes Anonymous Data. Customer agrees that Arctic Wolf may use, copy, modify, distribute and display Files, Anonymous Data and Potentially Malicious Code for Arctic Wolf's business purposes, including research, development, enhancement and support of products and services. Without limiting the foregoing, Arctic Wolf will not identify Customer as the source of any Files, Anonymous Data or Potentially Malicious Code.

2.3.3 Risks Regarding Potentially Malicious Code. If the Solution identifies Potentially Malicious Code, certain configurations of the Solution may block Potentially Malicious Code from execution, in which case Customer may either allow execution of the Potentially Malicious Code or quarantine it. Alternatively, Customer may determine that Potentially Malicious Code is acceptable for use on Customer devices and need not be blocked or quarantined. Customer acknowledges that blocking the execution of or quarantining or running Potentially Malicious Code may result in a loss of functionality of Files, applications, or the Customer's devices, and cause other potential harm or loss. CUSTOMER'S DECISION TO BLOCK, QUARANTINE OR ENABLE EXECUTION OF POTENTIALLY MALICIOUS CODE IS AT CUSTOMER'S OWN RISK. CUSTOMER ACKNOWLEDGES THAT ARCTIC WOLF HAS NO CONTROL OVER THE SPECIFIC CONDITIONS UNDER WHICH CUSTOMER USES THE SOLUTION OR ALLOWS OR DISALLOWS POTENTIALLY MALICIOUS CODE TO EXECUTE THE SOLUTION. THE SOLUTIONS DO NOT REPLACE CUSTOMER'S OBLIGATION TO EXERCISE CUSTOMER'S INDEPENDENT JUDGMENT WITH RESPECT TO THE EXISTENCE OR SUITABILITY OF POTENTIALLY MALICIOUS CODE EXISTING ON ITS DEVICES OR THE SECURITY THEREOF.

3. TRIAL LICENSE. If the Solution is provided by Arctic Wolf to Customer for internal testing purposes ("**Trial**"), the license set out above shall be of a limited duration from when the applicable Solution is made available by Arctic Wolf to Customer and may be terminated by Arctic Wolf at any time in its sole discretion ("**Trial Period**") and shall apply solely to the extent necessary to perform the Trial. Notwithstanding anything to the contrary in this Agreement, such license shall automatically terminate upon the expiry of the Trial Period, or earlier if Customer breaches any provision of this Agreement, and subsection 12 (d) of this Agreement shall apply. The Trial Period may be extended or terminated by Arctic Wolf in writing (email sufficient) at any time in its sole discretion.

4. CUSTOMER WARRANTIES. In addition to any warranties set forth in the General Terms:

4.1 CUSTOMER ACKNOWLEDGES AND AGREES THAT WHERE THE SOLUTION IS DESIGNED TO INTEROPERATE WITH OR FACILITATE CUSTOMER'S ACCESS TO THIRD PARTY ITEMS, ARCTIC WOLF HAS NO CONTROL OVER THE FUNCTIONALITY, DELIVERY, USE OR PERFORMANCE OF SUCH THIRD PARTY ITEMS.

4.2 CUSTOMER ACKNOWLEDGES AND WARRANTS THAT CUSTOMER IS SOLELY RESPONSIBLE AND LIABLE FOR: (I) VERIFYING THE ACCURACY AND ADEQUACY OF ANY INPUT, OUTPUT OR ALERT INTO OR FROM THE SOLUTION; OR (II) CUSTOMER'S DECISION TO ALLOW OR MAINTAIN ANY MALWARE OR VULNERABILITY ON OR TO CUSTOMER'S (OR ITS USERS') ENDPOINTS, SYSTEMS OR NETWORKS. TO THE MAXIMUM EXTENT PERMITTED BY LAW, CUSTOMER WAIVES ANY AND ALL CAUSES OF ACTION OR CLAIMS AGAINST ARCTIC WOLF ARISING FROM OR RELATING TO THIS SECTION 4.2.

5. TERMINATION. Except as otherwise required by law and provided that the Solution is no longer in use by Customer, Arctic Wolf will remove, delete, or otherwise destroy all copies of Confidential Information in its possession one hundred-twenty (120) days following expiration or termination. Notwithstanding anything contrary herein, should Customer fail to immediately cease all use of and/or access to the Solution and delete and/or destroy all copies of Software that are in Customer's possession or control, the subscription will not terminate, and Customer shall remain responsible for payment of fees pertaining to the subscription.