CLOUD SECURE ADDENDUM

1. DESCRIPTION OF CLOUD SECURE SERVICES. Fidium will provide Cloud Secure (as applicable, the **"Secure Services"** or **"Services"**) to you as set forth on your order for Secure Services under the Agreement or a separate service order for Secure Services (a **"Service Order"**). Each Service Order will identify the scope of the Services and/or equipment that is the subject of such Service Order.

2. FIDIUM RESPONSIBILITIES.

2.1 Fidium Work. Fidium will perform the work described below:

a. Fidium will assign a qualified Project Manager to be the primary contact for you.
b. A security review meeting will be convened between you and our staff to verify your current security environment, discuss potential security options available from the Secure Services and provide guidance as requested.
c. A separate pre-installation meeting will be convened by you and our staff for review of security settings.
d. Fidium will install and provision the Secure Services, and perform basic testing to verify Secure Service platform operability.
e. If separate network transport has been purchased from Fidium in conjunction with Secure Services, Fidium will coordinate Secure Services with other internal Fidium staff as needed.

2.2 Support Service. Support service is provided to you through a single administrator you identify who will act as a single point of contact with Fidium for all support issues ("**Customer's Administrator**"). Support Service is included with all Secure Services and consists of the following: (i) remote troubleshooting support; (ii) an Extranet website for your use, which you can use to submit and monitor trouble ticket information; and (iii) automated notification and escalation procedure for your trouble tickets. In the case of problems with Secure Services, Customer's Administrator must contact Fidium to open a trouble ticket, and our staff will engage you to investigate the issue as it relates specifically to Secure Services. At the election of Fidium, support may also be provided by Fidium's third-party software vendor. Fidium assumes no responsibility for supporting or assisting in LAN issue resolution, customer-owned or customer–licensed software, customer-owned equipment or issues resulting from third-party network transport services. Fidium support service does not include any advanced security management such as, but not limited to, vulnerability assessments, penetration testing, incident response/resolution, or compliance management.

2.3 Managed Service. Secure Services are a managed service supported by Fidium staff. The Managed Service component of Secure Services will include platform management, including Secure Services upgrades to the platform.

2.3.1 Managed Service—Security Services. Fidium additionally provides verification that the following services are operational:

- Firewall filtering policies, based on the rules provided by you, Network Address Translation (**"NAT"**), if applicable
- De-Militarized Zone (**"DMZ"**) segregating for a customer private LAN handling traffic, based on the policy rules defined by you, if applicable
- Inspection of Intrusion Protection Service/Intrusion Detection Service (**"IPS/IDS"**), if applicable
- URL Filter services are filtering web access based on the rules as defined by you, if applicable
- IP Sec VPN or SSL-VPN (**"Global Protect"**) remote access services Fidium, if applicable. Support will be limited to troubleshooting from the Global Protect application. Fidium will not be responsible for troubleshooting any third-party transport connectivity issues or customer-provided endpoints.
- If you have another managed service from Fidium, such as Managed Router or SD-WAN, the troubleshooting and repair of that service will fall under the Addendum governing such other managed service.

2.3.2. Platform Updates. Fidium will occasionally need to make security, performance and other updates to the Cloud Secure platform. Fidium will make efforts to communicate these changes/updates via a maintenance notification; however, in some cases, the update may take place without a proactive notification as Fidium may choose to perform the update quickly to minimize security exposure to you. Fidium may also choose not to notify you of certain updates. Updates may require downtime of the security service and may also affect the network service uptime/access. Downtime resulting from these updates are not subject to product Performance SLAs.

2.4 Bandwidth. Included with provisioning Secure Services, an Internet connection will be provisioned by Fidium.

2.5 Data Security. Secure Services are intended to improve your security measures, but your use of Secure Services does not guarantee the security of your data, information or network. FIDIUM DISCLAIMS ANY AND ALL REPRESENTATIONS OF WARRANTIES, EXPRESS OR IMPLIED, IN FACT OR BY LAW, STATUTORY OR OTHERWISE, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR USE, AND THAT SECURE SERVICES WILL BE UNINTERRUPTED OR ERROR FREE. YOU AGREE THAT THERE ARE INHERENT RISKS IN INTERNET CONNECTIVITY THAT COULD RESULT IN THE LOSS OF YOUR PRIVACY AND PROPERTY, INCLUDING CONFIDENTIAL INFORMATION. FIDIUM DOES NOT ASSUME, AND YOU HEREBY RELEASE FIDIUM FROM, ANY LIABILITY FOR ANY DAMAGE, THEFT OR LOSS TO YOUR PROPERTY (INCLUDING WITHOUT LIMITATION, DATA) RESULTING FROM THE ACTS OR OMISSIONS OF ANY THIRD PARTY NOT INVOLVED IN PROVISION OF SERVICES, INCLUDING WITHOUT LIMITATION, ANY UNAUTHORIZED PHYSICAL OR NON-PHYSICAL ACCESS (SUCH AS HACKING). Fidium will provision Secure Services according to the standards set forth in the Agreement. In the event of any breach of your data or information, due to any cause, Fidium's liability (and limitations thereof) for such breach, and any failure of Secure Services, is as forth in the Agreement.

3. CUSTOMER RESPONSIBILITIES.

3.1 Coordination. In addition to the responsibilities set forth in the Agreement, you will, at your own expense:

a. Designate a dedicated, knowledgeable representative as Customer's Administrator, such individual being authorized to act on your behalf and to communicate with Fidium regarding Secure Services, Trouble Reports, and service issues. This person should have working knowledge of standard IT infrastructure, equipment, and software and data services.
b. Participate in any required security review meeting.
c. Participate in the pre-implementation to review and approve design, including any change orders.
d. Review and test all security policies set forth in the approved design. CCI staff does not test policies or ensure operability between policies, users, systems, software, applications or your IT environment.

3.2 Cooperation. You will cooperate timely with the following activities: (i) complete assessment interview with Fidium, participate in design meetings and provide prompt response and input to design documentation; (ii) schedule internal resources needed for the scheduled cutover, (iii) designate a primary contact with whom Fidium can interface; and (iv) refrain from making any design change requests from and after the freeze date established by Fidium, which will be at least two (2) weeks prior to the scheduled cutover date. If you make any changes after the freeze date or do not cooperate for cutover on the mutually agreed date, then Fidium may: (i) commence billing for the Secure Services on the scheduled cutover date even if Service has not commenced, and / or (ii) charge additional costs to you, such as overtime charges, caused by such changes or failure to cooperate.

3.3 Notification. You will promptly notify Fidium: (a) of events that may affect the performance of Secure Services; and (b) in advance of, and will pay Fidium's then-standard rates for labor and materials supplied by Fidium as a result of, any: (i) changes at or to the Secure Services point of demarcation or customer Network termination point that may affect Secure Services; and (ii) software or hardware configuration changes proposed to be made to equipment or to your network or third-party supplied equipment used to deliver Secure Services; and (iii) moves, additions, changes or modifications to equipment or network requested by you.

3.4 Support. You are responsible for: (i) giving Fidium an up-to-date list of persons authorized to initiate Trouble Reports on your behalf and access network performance information via web application or other form of communication; (ii) allowing Fidium unblocked access through the network and firewall for all managed devices; (iii) providing one (1) business day advance notice to Fidium of any customer-initiated maintenance such as contact, schedule or network device configuration changes; and (iv) providing technical LAN expertise in certain cases to assist with trouble resolution.

3.5 Communication. You will be responsible for communicating with your own users of Secure Services, and for responding to all service issues and Trouble Reports made by such users.

4. OPERATIONS PROCEDURES. Your operations and use of Secure Services will comply with the Operations Procedures set forth below. You will promptly report to Fidium any interruption or other failure of the Secure Services (**"Trouble Report"**). You will provide to Fidium an escalation list for your personnel upon execution of this Addendum. In the event of a customer-initiated Trouble Report, you will contact Fidium at 1.844.FIDIUMBIZ (1.844.343.4862).

The following information will be exchanged at the time of notification by Fidium or in the event of a customer-initiated Trouble Report:

a. The name and telephone number of the person who is making the Trouble Report.
b. The date and time of the Trouble Report.
c. The specifics relating to the Trouble Report.

Fidium will maintain communication with you throughout resolution of the Trouble Report.

5. SECURE SERVICES PERFORMANCE AND TECHNICAL SPECIFICATIONS. In the event of a Service interruption caused by Fidium's core network(s), Fidium will use commercially-reasonable efforts to restore the affected Service as quickly as possible. Fidium will work in good faith to promptly provide you with a root-cause analysis of any Service level violations.

5.1 Performance Specifications. The Performance Specifications below apply to the following of the Secure Services: Firewall Services, Threat Prevention, Wildfire, Global Protect, and URL Filtering. Availability is a percentage of total time that Secure Services are operative when measured over the respective calendar year. Secure Services are considered unavailable when there has been a complete loss of the security capabilities of Secure Services.

SERVICE	MINIMUM SERVICE AVAILABILITY
Secure Services	At least 99.9% (within the calendar year)

Any issues involving Internet connectivity are subject to the Performance Specifications of Dedicated Internet Services.

5.1.2 Performance Specifications-MPLS or SD-WAN Service. Cloud Secure Services require Fidium's MPLS Service or SD-WAN for connectivity. Refer to the MPLS or SD-WAN Performance Specifications in the appropriate Addendum attached to the Agreement for service standards on latency, packet loss and jitter.

5.1.3 Performance Specifications for security policy changes. Your policy change requests will be worked within one (1) business day of submission of a ticket provided the request contains sufficient information necessary to make the change. Fidium may require additional information from you prior to a policy request being completed. Fidium is not responsible for any business interruptions that may occur as a result of the new policy request. You are responsible for all testing related to the policy change. Fidium will have no liability to you for downtime or security breaches arising either directly or indirectly due to policy changes.

5.1.4 Performance Specifications for change in customer profile. Fidium provisions Secure Services with a standard, customer-default-profile. Customer may request temporary access to administration features that are not made available with the standard, customer-default-profile. Fidium will have no liability for downtime or security breaches arising directly or indirectly due to such access or any changes made by customer to the

Secure Services. Fidium reserves the right to reject or revoke any request for temporary access to Secure Services administration features. Fidium reserves the right to bill for labor charges should you make any administration change that fails and/or causes disruption whereby you require Fidium to aid in resolving the administration change you made.

5.2 General Exclusions. In addition to exclusions provided in Section 4.1 and the Agreement, Fidium will have no liability to you for downtime caused directly or indirectly by:

5.2.1 Secure Services administration settings configured by you or customer-approved administration settings configured on behalf of you by Fidium;

5.2.2 Software changes not made or approved by Fidium or its authorized third-party software provider;

5.2.3 Hardware configuration changes not made or approved by Fidium or its authorized third-party software provider; or

5.2.4 Failure of any components or services not managed by Fidium, including but not limited to hardware, network access, electrical power, or Internet access.

5.3 VPN Connectivity. Fidium is not responsible for the connectivity of any IP Sec or SSL VPN/Global Protect connections that are connecting into Secure Services. Fidium will assist with VPN settings within the Secure Services product; however, Fidium is not responsible for any performance issues related to IP Sec or SSL VPN connectivity.

6. ADDITIONAL TERMS.

6.1 Palo Alto Networks. Fidium hereby notifies you that: (a) Palo Alto Networks (**"PAN"**) is an intended third-party beneficiary of your agreement with Fidium regarding the provision of Secure Services, and (b) all limitations and obligations therein with respect to Fidium are also applicable to PAN. You are responsible for maintaining the confidentiality of your accounts and passwords, as well as all activities that occur under your account. You represent, warrant and covenant to Fidium that: (a) you own or have the legal right and authority, and will continue to own or secure the legal right and authority, to use your equipment and any software you provide; and (b) these terms do not violate any applicable law or agreement to which you are a party and that you will comply with all applicable federal, state and local laws. You are notified about and consent to Fidium providing PAN with certain information regarding your: (i) contact information and (ii) usage of Secure Services, which may be used by Fidium and PAN for their commercial purposes, but not for resale or disclosure to third parties. With respect to any software provided by Fidium for your use in connection with Secure Services, you agree to abide by PAN's End User License Agreement described in Attachment A.

6.2 PHI. If you will use the Secure Services in connection with Protected Health Information (as defined by applicable law, **"PHI"**), Fidium requires a Business Associate Agreement (**"BAA"**) or Sub-Business Associate Agreement with you as needed to comply with the Health Insurance Portability and Accountability Act that will require that you acknowledge that: (i) you will encrypt all PHI in accordance with commercially-reasonable encryption techniques consistent with the guidelines promulgated by the Department of Health and Human Services, and (ii) Fidium is neither responsible for knowing what type of information may be created, stored, used or managed by you in connection with Secure Services, nor for knowing or investigating which laws may or may not apply to such information.

5.3 Customer's Assessment. You agree that you: (i) have conducted an assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of your information to be created, transmitted, stored, used or maintained in connection with Secure Services; (ii) have conducted an assessment of the capabilities and viability of Secure Services as it relates to your needs; (iii) has determined that Secure Services are sufficient for your needs and purposes, and compliance with applicable law; and (iv) Fidium is not responsible for determining whether Secure Services are sufficient for your needs, or compliance with any applicable law.

CLOUD SECURE ADDENDUM ATTACHMENT A

END USER LICENSE AGREEMENT (**"EULA"**)

PLEASE READ CAREFULLY

THIS EULA IS A LEGAL AGREEMENT BETWEEN YOU, EITHER AS AN INDIVIDUAL, COMPANY OR OTHER LEGAL ENTITY (IN ANY CAPACITY REFERRED TO HEREIN AS **"END USER"**, **"YOU"** or **"YOUR"**) AND (I) PALO ALTO NETWORKS, INC., A DELAWARE CORPORATION WITH OFFICES AT 4401 GREAT AMERICA PARKWAY, SANTA CLARA, CALIFORNIA 95054 UNITED STATES,(II) PALO ALTO NETWORKS (NETHERLANDS) B.V., A COMPANY FORMED UNDER THE LAWS OF THE NETHERLANDS, WITH OFFICES AT OVAL TOWER, DE ENTRÉE 99-197, 5TH FLOOR, 1101 HE AMSTERDAM-ZUIDOOST, OR (III) ANY OTHER PALO ALTO NETWORKS AFFILIATE (COLLECTIVELY, **"PALO ALTO NETWORKS"**).

THIS EULA GOVERNS YOUR USE OF THE PALO ALTO NETWORKS HARDWARE (**"HARDWARE"**), ANY SOFTWARE THAT IS INCLUDED IN THE HARDWARE AND ANY STANDALONE SOFTWARE THAT IS PROVIDED WITHOUT HARDWARE FOR USE ON YOUR HARDWARE INCLUDING VIRTUAL MACHINE (**"VM"**) SOFTWARE OR ENDPOINT SOLUTIONS (**"ENDPOINT"**) (COLLECTIVELY, **"SOFTWARE")**, ANY SOFTWARE-AS-A-SERVICE (**"SaaS"**), SUBSCRIPTION-BASED SERVICES INCLUDING, BUT NOT LIMITED TO, WILDFIRE, GLOBALPROTECT, URL FILTERING, AND THREAT PREVENTION (**"SUBSCRIPTION SERVICES"**), OR A COMBINATION OF THE FOREGOING, ALL COLLECTIVELY REFERRED TO HEREIN AS **"PRODUCTS"**, UNLESS YOU AND PALO ALTO NETWORKS HAVE EXECUTED A SEPARATE EULA IN WRITING, SIGNED BY BOTH PALO ALTO NETWORKS AND YOU WHICH EXPRESSLY SUPERSEDES THIS EULA.

BY OPERATING, DOWNLOADING, INSTALLING, REGISTERING OR OTHERWISE USING THE PRODUCTS, YOU ARE EXPRESSLY AND EXPLICITLY ACKNOWLEDGING AND AGREEING THAT THIS IS A BINDING EULA AND YOU HEREBY AGREE TO THE TERMS OF THIS EULA.

IF YOU DO NOT ACCEPT ALL THE TERMS AND CONDITIONS SET FORTH HEREIN, DO NOT OPERATE, DOWNLOAD, INSTALL, REGISTER OR OTHERWISE USE THIS PRODUCT.

PALO ALTO NETWORKS MAINTENANCE AND SUPPORT SERVICES ARE NOT GOVERNED BY THIS EULA, AND ARE GOVERNED BY A SEPARATE GLOBAL SUPPORT SERVICES TERMS AND CONDITIONS (**"EUSA"**) FOUND AT https://www.paloaltonetworks.com/content/dam/paloaltonetworks-com/en_US/assets/pdf/datasheets/support/global-customer-support-services-terms-conditions.pdf.

1. LICENSE GRANT AND RESTRICTIONS.

1.1 Software License Grant. Subject to the terms and conditions of this EULA, Palo Alto Networks grants to End User a non-exclusive license to: (i) use the Software solely as part of the Hardware with which the Software is delivered, or (ii) in accordance with the published specifications. The Software is solely for End User's internal business purposes unless otherwise agreed to with Palo Alto Networks in a separate written agreement. All other rights in the Software are expressly reserved by Palo Alto Networks.

1.2 Subscription Services Limited Right to Use. Palo Alto Networks grants to End User the limited right to use the Subscription Services solely in connection with the Hardware and/or Software and solely for End User's internal business purposes.

1.3 License Restrictions. End User shall maintain the Products in strict confidence and shall not: (a) except in accordance with Palo Alto Networks license transfer procedure (https://www.paloaltonetworks.com/support/support-policies/secondary-market-policy.html), sell, resell, distribute, transfer, publish, disclose, rent, lend, lease or sublicense the Products, or make the functionality of the Products available to any other party (excluding contractors or other third party providing IT services to Customer) through any means (unless otherwise permitted in writing by Palo Alto Networks as expressly agreed to in a separate Managed Security Services Provider agreement), including, without, limitation, by uploading the Software or Subscription Services to a network or file-sharing service or through any hosting, application services provider, service bureau or other type of services; (b) modify, translate or create derivative works based on the Software or Subscription Services, in whole or in part, or permit or authorize a third party to do so; (c) disassemble, decompile, reverse compile, reverse engineer or otherwise attempt to derive the source code of the Software, in whole or in part, or permit or authorize a third party to do so, except to the extent such activities are expressly permitted by applicable law in the jurisdiction of use notwithstanding this prohibition; (d) disclose, publish or otherwise make publicly available any benchmark, performance or comparison tests that End User runs (or has run on its behalf by a third party) on the Products; (e) duplicate the Software except for making a reasonable number of archival or backup copies, provided that End User reproduces on or in such copies the copyright, trademark and other proprietary notices or markings that appear on the original copy of the Software (if any) as delivered to End User.

1.4 Affiliates. If End User purchases the Product for use by any End User Affiliate (defined below), End User shall: (a) provide each such End User Affiliate with a copy of this EULA; (b) ensure that each such End User Affiliate complies with the terms and conditions therein; and (c) be responsible for any breach of these terms and conditions by any such End User Affiliate. For purposes of this EULA, **"Affiliate"** means any entity that Controls, is Controlled by, or is under common Control with End User or Palo Alto Networks, as applicable, where **"Control"** means ownership, directly or indirectly, of 50% or more of the voting interest of End User or Palo Alto Networks, as applicable.

2. OWNERSHIP. The Software and Subscription Services are licensed, not sold. Palo Alto Networks and its suppliers, as applicable, retain all right, title, interest and ownership of the Software and Subscription Services, including copyrights, patents, trade secret rights, trademarks and any other intellectual property rights therein. End User shall not delete or in any manner alter the copyright, trademark, or other proprietary rights notices or

markings that appear on the Software and Subscription Services or related documentation as delivered to End User. To the extent you provide any suggestions or comments related to the Products to Palo Alto Networks or its authorized third party agent, Palo Alto Networks shall have the right to retain and use any such suggestions or comments in current or future products or services, without your approval or further compensation to you.

3. TERM; TERMINATION; AND EFFECT OF TERMINATION. This EULA is effective until terminated. End User's rights under this EULA will terminate immediately without notice from Palo Alto Networks if End User fails to comply with or breaches any provision of this EULA. End User may terminate this EULA upon written notice to Palo Alto Networks. Upon termination, End User shall destroy all copies of Software and documentation and cease to use any Subscription Services and/or Hardware.

4. WARRANTY, EXCLUSIONS AND DISCLAIMERS.

4.1 Warranty. Palo Alto Networks warrants that, under normal authorized use (a) the Hardware shall be free from defects in material and workmanship for one (1) year from the date of shipment; and (b) the Software will substantially conform to Palo Alto Networks' published specifications for three (3) months from the date of shipment. As End User's sole and exclusive remedy and Palo Alto Networks' and its suppliers' sole and exclusive liability for breach of warranty, Palo Alto Networks shall, at its option and expense, repair or replace the Hardware or correct the Software, as applicable. All warranty claims must be made on or before the expiration of the warranty period specified herein. Replacement Products may consist of new or remanufactured parts that are equivalent to new. All Products that are returned to Palo Alto Networks and replaced become the property of Palo Alto Networks. Palo Alto Networks shall not be responsible for End User's or any third party's software, firmware, information, or memory data contained in, stored on, or integrated with any Product returned to Palo Alto Networks for repair or upon termination, whether under warranty or not. End User will pay the shipping costs for return of Products to Palo Alto Networks. Palo Alto Networks will pay the shipping costs for shipment of repaired or replacement Products back to End User.

4.2 Exclusions. The warranty set forth above shall not apply if the failure of the Product results from or is otherwise attributable to: (i) repair, maintenance or modification of the Product by persons other than Palo Alto Networks-authorized third party; (ii) accident, negligence, abuse or misuse of a Product; (iii) use of the Product other than in accordance with Palo Alto Networks' specifications; (iv) improper installation or site preparation or any failure by End User to comply with environmental and storage requirements for the Product specified by Palo Alto Networks, including, without limitation, temperature or humidity ranges; or (v) causes external to the Product such as, but not limited to, failure of electrical systems, fire or water damage.

4.3 Disclaimers. EXCEPT FOR THE WARRANTIES EXPRESSLY STATED AND AS OTHERWISE PROHIBITED BY APPLICABLE LAW, THE HARDWARE, SOFTWARE AND SUBSCRIPTION SERVICES ARE PROVIDED "AS IS". PALO ALTO NETWORKS AND ITS SUPPLIERS MAKE NO OTHER WARRANTIES AND EXPRESSLY DISCLAIM ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTIES ARISING OUT OF COURSE OF DEALING OR USAGE OF TRADE. PALO ALTO NETWORKS DOES NOT WARRANT THAT (I) THE PRODUCT WILL MEET END USER'S REQUIREMENTS, (II) USE THEREOF SHALL BE UNINTERRUPTED OR ERROR-FREE, OR (III) THE HARDWARE, SOFTWARE OR SUBSCRIPTION SERVICES WILL PROTECT AGAINST ALL POSSIBLE THREATS WHETHER KNOWN OR UNKNOWN.

5. LIMITATION OF LIABILITY. TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, (A) IN NO EVENT SHALL PALO ALTO NETWORKS OR ITS SUPPLIERS BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL, PUNITIVE, EXEMPLARY OR CONSEQUENTIAL DAMAGES OF ANY KIND (INCLUDING BUT NOT LIMITED TO LOSS OF USE, DATA, BUSINESS OR PROFITS, OR FOR THE COST OF PROCURING SUBSTITUTE PRODUCTS, SERVICES OR OTHER GOODS), ARISING OUT OF OR RELATING TO THIS EULA, REGARDLESS OF THE THEORY OF LIABILITY AND WHETHER OR NOT PALO ALTO NETWORKS WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGE OR LOSS; AND (B) IN NO EVENT SHALL PALO ALTO NETWORKS' TOTAL LIABILITY ARISING OUT OF OR RELATING TO THIS EULA, FROM ALL CLAIMS OR CAUSES OF ACTION AND UNDER ALL THEORIES OF LIABILITY, EXCEED THE TOTAL PAYMENTS ACTUALLY MADE TO PALO ALTO NETWORKS FOR THE PRODUCTS DURING THE TWELVE (12) MONTH PERIOD PRIOR TO ANY SUCH CLAIM OR CAUSE OF ACTION. THE FOREGOING LIMITATIONS SHALL NOT APPLY TO LIABILITY ARISING FROM DEATH OR BODILY INJURY. End User agrees that the foregoing limitations of liability constitute a material inducement for Palo Alto Networks to enter into this EULA and that the purchase price and fees charged to End User would be substantially higher without such limitations.

6. INDEMNIFICATION.

6.1 Indemnification and Procedure. Palo Alto Networks will defend, at its expense, any third-party action or suit brought against End User alleging that any Palo Alto Networks Product provided to End User hereunder infringes or misappropriates the third party's patent, copyright, trademark, or trade secret (a **"Claim"**), and Palo Alto Networks will pay any damages awarded in final judgment against End User or agreed to in settlement by Palo Alto Networks that are attributable to any such Claim; provided that End User: (i) promptly notifies Palo Alto Networks in writing of the Claim; (ii) gives Palo Alto Networks sole control of the defense and settlement of the Claim; and (iii) gives Palo Alto Networks, at Palo Alto Networks' expense, all information and assistance reasonably requested for the defense and settlement of the Claim. Palo Alto Networks will not be bound by any settlement or compromise that End User enters into without Palo Alto Networks' prior written consent.

6.2 Remedy. If the Product becomes, or in Palo Alto Networks' opinion is likely to become, the subject of a Claim, then Palo Alto Networks may, at its sole option and expense: (i) procure for End User the right to continue using the Product; (ii) replace or modify the Product to avoid the Claim; or (iii) if options (i) and (ii) cannot be accomplished despite Palo Alto Networks' reasonable efforts, then Palo Alto Networks may accept return of the Product from End User and grant End User credit for the price of the Product as depreciated on a straight-line five (5) year basis, commencing on the date of receipt by End User of such Product.

6.3 Exceptions. Palo Alto Networks' obligations under this section shall not apply to the extent any Claim results from or is based on (a) modifications to the Product made by a party other than Palo Alto Networks or its designee; (b) the combination, operation, or use of the Product with hardware or

software not supplied by Palo Alto Networks, if a Claim would not have occurred but for such combination, operation or use; (c) failure to use the most recent version or release of the Product; (d) Palo Alto Networks' compliance with End User's explicit or written designs, specifications or instructions; or (e) use of the Product that is not in accordance with Palo Alto Networks' published specifications.

THE FOREGOING TERMS STATE PALO ALTO NETWORKS' SOLE AND EXCLUSIVE LIABILITY AND END USER'S SOLE AND EXCLUSIVE REMEDY FOR ANY CLAIMS OF INTELLECTUAL PROPERTY INFRINGEMENT OR MISAPPROPRIATION.

7. END USER DATA. Palo Alto Networks utilizes industry standard practices and policies to maintain administrative, physical and technical safeguards for the protection and security of End User Data (defined below). End User is hereby notified and acknowledges that Palo Alto Networks Products may include interaction and communication with facilities hosted outside of the country where End User purchased or utilizes the Products. End User is further notified and acknowledges that some Subscription Services may allow End User, in its sole discretion, to send data to Palo Alto Networks, where such data may contain personally-identifiable, sensitive, and/or confidential data and information (collectively, **"End User Data"**). End User represents and warrants that End User's use of the Subscription Services and related submission of End User Data complies with all applicable laws, including those related to data privacy, data security, international communication and the exportation of technical, personal or sensitive data. Palo Alto Networks is not a data processor or data collector, and the inclusion of such personally identifying or sensitive data in End User Data is solely incidental to the provision of the Subscription Services. Submission of End User Data to Palo Alto Networks shall be at End User's sole discretion and at its own risk, and Palo Alto Networks assumes no responsibility or liability for receipt of such End User Data. End User Data sent to Palo Alto Networks may be stored by Palo Alto Networks. End User further acknowledges that Palo Alto Networks may anonymize such End User Data to use for statistical purposes and share samples of such anonymized End User Data with other third party security-related researchers, vendors and customers.

8. GENERAL.

8.1 Governing Law. Where Palo Alto Networks, Inc., is the contracting entity, this EULA is governed by and construed in accordance with the laws of the State of California, excluding its conflict of laws principles. Where Palo Alto Network (Netherlands) B.V., is the contracting party, this EULA is governed by and construed in accordance with the laws of the Netherlands, excluding its conflict of laws principles. The United Nations Convention on Contracts for the International Sale of Goods shall not apply to this EULA.

8.2 Compliance with Laws; Export Control. End User shall be solely responsible for its compliance with, and agrees to comply with, all applicable laws in connection with its use of the Product. End User further agrees that it will not engage in any illegal activity in any relevant jurisdiction, and acknowledges that Palo Alto Networks reserves the right to notify its customers or appropriate law enforcement in the event of such illegal activity. End User agrees to comply fully with the U.S. Export Administration Regulations, and any other export laws, restrictions, and regulations to ensure that the Product and any technical data related thereto is not exported or re-exported directly or indirectly in violation of, or used for any purposes prohibited by such laws and regulations.

8.3 Cumulative Remedies. Except as expressly set forth in this EULA, the exercise by either party of any of its remedies will be without prejudice to any other remedies under this EULA or otherwise.

8.4 Notices. All notices shall be in writing and delivered by overnight delivery service or by certified mail sent to the address published on the respective parties' websites or the address specified on the relevant order document (attention: Legal Department), and in each instance will be deemed given upon receipt.

8.5 Waiver and Severability. The failure by either party to enforce any provision of this EULA will not constitute a waiver of future enforcement of that or any other provision. Any waiver, modification or amendment of any provision of this EULA will be effective only if in writing and signed by authorized representatives of both parties. If any provision of this EULA is held to be unenforceable or invalid, that provision will be enforced to the maximum extent possible and the other provisions will remain in full force and effect.

8.6 Entire Agreement. This EULA constitutes the entire agreement between the parties with respect to the subject matter hereof, and supersedes all prior written or oral agreements, understandings and communications between the parties with respect to the subject matter hereof. Any terms or conditions contained in End User's purchase order or other ordering document that are inconsistent with or in addition to the terms and conditions of this EULA are hereby rejected by Palo Alto Networks and will be deemed null.

8.7 U.S. Government End Users. This section applies to United States Government End Users only and does not apply to any other End Users. The Software and its documentation are "commercial computer software" and "commercial computer software documentation," respectively; as such terms are used in FAR 12.212 and DFARS 227.7202. If the Software and its documentation are being acquired by or on behalf of the U.S. Government, then, as provided in FAR 12.212 and DFARS 227.7202-1 through 227.7202-4, as applicable, the U.S. Government's rights in the Software and its documentation shall be as specified in this EULA.

8.8 Open Source Software. The Products may contain or be provided with components subject to the terms and conditions of open source software licenses (**"Open Source Software"**). A list of Open Source Software can be found at https://www.paloaltonetworks.com/company/third-party-software.html.

8.9 End User Records. End User grants to Palo Alto Networks and its independent advisors the right to examine End User's books, records, and accounts during End User's normal business hours to verify compliance with this EULA. In the event such audit discloses non-compliance with this EULA, End User shall promptly pay the appropriate license fees to the relevant party, plus reasonable audit costs.

8.10 Authorization Codes, Grace Periods and Registration. Your Product may require an authorization code for activation for support of Your Product or to access Subscription Services. The authorization codes will be issued at the time of order fulfillment and sent to You via email. The service period will commence in accordance with the grace period policy at https://www.paloaltonetworks.com/support/support-policies/grace-period.html. You are hereby notified that, upon applicable grace period expiration, if any, Palo Alto Networks reserves the right to register Your

Product and activate support services (if purchased) on Your behalf without further notification to You.

8.11 WildFire Related Microsoft Licenses. End User acknowledges that certain WildFire offerings require licenses for certain Microsoft software, including Windows and Office, as described further in the relevant Wildfire documentation. Where Microsoft software is provided with certain WildFire offerings, Palo Alto Networks has procured or otherwise provided the necessary Microsoft licenses for the WildFire offering. End User is hereby notified and acknowledges that Microsoft updates and upgrades (software assurance) are not provided with the WildFire product and must be obtained by End User directly from Microsoft in order for End User to utilize later versions of Microsoft products beyond the versions initially provided with the WildFire offerings.

8.12 Survival. Sections regarding license restrictions, ownership, term and termination, U.S. Government End Users, limitations of liability, and this General section shall survive termination of this EULA.