Managed Security Appliance ("Managed Security") Terms and Conditions

These terms and conditions apply to business clients only.

These product specific terms and conditions, along with the accompanying Master Service Agreement and Business Service Agreement, supplement and compose the entirety of the contract between the parties.

VENYU's Managed Security Appliance ("Managed Security") service **includes** the following:

- Pre-implementation analysis of Client's infrastructure and systems environment to determine and document Client's configuration requirements and preferences.
- Optional pre-implementation consulting to determine best-practices strategy, if applicable.
- Professional installation by trained Provider technicians or contractors.
- Post installation testing and acceptance.
- Single security context running on a single firewall appliance dedicated to the Client. Service is limited by whatever constraints the underlying physical appliance and corresponding software may have.
- Features of the product may include the following:
    - Web Filtering
    - Intrusion Prevention System (IPS)
    - Secure Sockets Layer (SSL)/Virtual Private Network (VPN)
    - Site to Site VPN
    - 2 Factor Authentication
    - Domain Name System (DNS) Filtering
- Diagnosis, troubleshooting, and repair of issues with the security appliance and features. IF CLIENT MAKES CHANGES TO THE SECURITY APPLIANCE AND/OR CONFIGURED FEATURES THAT RESULT IN SYSTEM ISSUES, CLIENT WILL BE BILLED FOR ADMINISTRATIVE SERVICES FOR DIAGNOSIS, TROUBLESHOOTING, AND REPAIR OF ISSUES RESULTING FROM SUCH CHANGES.
- Standard system reports on detected events which will be provided to Clients on a periodic basis. Upon Client request, custom reports can be developed and provided to Client. Custom report development time may be billed as administrative services.
- Periodic upgrades to the security appliance in accordance with manufacturer's recommendations.

VENYU's Managed Security service **excludes** the following:

- Internet access, power, cabling, cooling, and appropriate network connectivity that is needed for the Managed Security services provided by VENYU to operate properly.
- Support and troubleshooting on Client owned servers, desktop computers, laptops, workstations, printers, copiers, fax machines, or other networked devices for issues not related to VENYU Managed Security services.
- Application support for client owned/operated applications.
- Anti-virus software, malware detection, or other end-point security related software.

ADMINISTRATIVE SERVICES: Additional hours for administration services are billed at one hundred seventy-five dollars ($175) per hour, unless otherwise noted. Administrative services are billed in fifteen (15) minute increments with no minimums. Client will be billed for reasonable and customary related travel expenses that may be incurred as part of the services provided by Provider.

THIRD PARTY SOFTWARE UPGRADES: VENYU shall upgrade the third-party software necessary to provide Managed Security services. Client may refuse to allow VENYU to upgrade this third-party software in the event that Client's existing third party software supplier does not authorize such upgrade, provided, however, VENYU HEREBY DISCLAIMS ANY AND ALL LIABILITY OR HARM ASSOCIATED WITH ANY FAILURE OF ANY SERVICES, SOFTWARE,

HARDWARE OR ANY OTHER FAILURE RELATED, DIRECTLY OR INDIRECTLY, TO THE FAILURE OF CLIENT TO UPGRADE VENYU OR THIRD PARTY SOFTWARE IN A TIMELY MANNER.

Title, Control, Use and Risk of Loss of CPE

TITLE. The services and all such related materials are for Client's legitimate business use only.

CLIENT PREMISE EQUIPMENT (CPE). Title to and/or ownership of any CPE provided to Client by Provider and/or its licensors under a rental option shall remain with Provider or such licensors as appropriate. Client agrees not to tamper with, modify, make error corrections, or otherwise alter any CPE provided to Client under a lease or rental option, nor permit third parties not authorized by Provider or the CPE vendor to do the same. All such leased or rented CPE must be returned to Provider upon termination of the Services for any reason. Client must contact Provider within thirty (30) days of such termination (unless contacted earlier by Provider) to schedule pickup of CPE, or Client shall be deemed to have purchased such CPE and shall be invoiced for the replacement cost of such CPE.

CONTROL AND USE OF CPE. Client agrees that it shall be bound by any vendor specific license terms and conditions related to any CPE. Where required by a vendor(s), such license terms shall be located in the Third Party Software Policy located on VENYU.com (https://www.venyu.com/terms-conditions) or successor site that is identified by VENYU, and made a part of the Agreement through this reference. Client acknowledges receipt of any such applicable license terms and its responsibility to comply with the terms and assumes all liability for compliance with such terms, including but not limited to, (a) informing all Client end-users of the terms of the license terms; (b) monitoring use of the CPE to ensure compliance with the terms thereof; and (c) maintaining the distribution and security of any user identification and/or passwords necessary to access any CPE. Provider disclaims all liability to vendors for breaches of such license terms by Client.

Client agrees not to reverse engineer, de-compile, disassemble, translate, modify, alter or change the Services, the CPE, or any component of either, or otherwise obtain or attempt to obtain any technology (including encryption technology) or source code for any hardware or software that may be provided with the services or CPE. Client acknowledges that the hardware and software provided under this Exhibit or utilized with the services provided under these terms and conditions may be subject to third party license terms, and/or U.S. export laws and regulations and that any transfer (whether directly or by products incorporating the technology) must be authorized under those laws and regulations. Client agrees not to copy, sell, assign, transfer, sublicense, export or distribute any hardware, software, documentation or other materials that Provider may provide related to the services. Title to such software, and all related technical know-how and intellectual property rights therein are and shall remain the exclusive property of Provider and/or its suppliers. Client shall not take any action to jeopardize, limit or interfere in any manner with Provider and its supplier's ownership of and rights with respect to any licensed software.

RISK OF LOSS OF CPE. Risk of loss of CPE or damage to any CPE, provided to Client on a rental basis as an integral part of Provider Managed Security service and is assumed by Client, except when such damage is caused solely by Provider in the installation or maintenance of such CPE. Provider retains title and all rights to such CPE.

DISCLAIMER OF WARRANTIES, LIMITATIONS OF LIABILITY AND EXCLUSIVE REMEDY

CLIENT ACKNOWLEDGES THAT DATA TRANSMISSION SECURITY SERVICES SUCH AS THOSE PROVIDED VIA MANAGED SECURITY SERVICES ARE NOT FOOLPROOF AND, THEREFORE, ARE NOT GUARANTEED. IN ADDITION TO THE DISCLAIMERS AND LIMITATIONS SET FORTH IN THESE TERMS, NEITHER PROVIDER NOR ITS SUPPLIERS WILL BE LIABLE FOR ANY DAMAGES (INCLUDING, WITHOUT LIMITATION, ANY LOSS OR DAMAGE TO DATA) RELATING TO OR ARISING FROM THE USE OF THE SERVICES PROVIDED HEREUNDER.

CLIENT UNDERSTANDS AND AGREES THAT PROVIDER IS PROVIDING SERVICES, AND ANY RELATED HARDWARE, SOFTWARE AND DOCUMENTATION TO CLIENT AND CLIENT HEREBY WAIVES ANY LIABILITY AGAINST PROVIDER AND AGREES TO HOLD PROVIDER HARMLESS FROM ANY AND ALL LIABILITY ARISING FROM LOSS OR DAMAGE DUE TO DELAY OF SERVICE COMMENCEMENT OR INABILITY TO PROVIDE THE SERVICE, FAILURE OF ALL OR PART OF THE SERVICE, INCLUDING ANY BETA SERVICE, OR ANY RELATED SERVICE PROVIDED HEREUNDER.

PROVIDER PROVIDES, AND CLIENT HEREBY ACCEPTS, ANY PROVIDER OR THIRD PARTY HARDWARE OR SOFTWARE PROVIDED TO OR USED BY CLIENT IN CONNECTION WITH THE SERVICES "AS IS" WITH NO EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS OF ANY KIND, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY, TITLE, NON-INFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE. NOTHING HEREIN SHALL BE INTERPRETED TO ENHANCE OR CREATE ANY WARRANTY WITH RESPECT TO ANY THIRD PARTY SOFTWARE OR HARDWARE. PROVIDER DISCLAIMS ANY AND ALL LIABILITY ARISING OUT OF THE DELIVERY, INSTALLATION, SUPPORT OR USE OF ANY SOFTWARE OR HARDWARE. PROVIDER ASSUMES NO OBLIGATION TO CORRECT ERRORS IN ANY SOFTWARE OR HARDWARE. CLIENT UNDERSTANDS AND ACCEPTS ALL RESPONSIBILITY FOR ANY SOFTWARE OR HARDWARE MEETING CLIENT'S REQUIREMENTS OR EXPECTATIONS.

NEITHER PROVIDER NOR ANY OTHER PARTY MAKES ANY WARRANTIES EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. PROVIDER'S LIABILITY IN CONNECTION WITH THIS AGREEMENT FOR MANAGED SECURITY APPLIANCE SERVICES, WHETHER IN CONTRACT, TORT OR OTHERWISE, SHALL NOT EXCEED THE TOTAL NET PAYMENTS PAYABLE BY CLIENT FOR THE APPLICABLE SERVICE UNDER THE APPLICABLE BUSINESS SERVICE AGREEMENT DURING THE TWELVE (12) MONTHS PRECEDING THE MONTH IN WHICH THE DAMAGE OCCURRED. IN NO EVENT SHALL PROVIDER OR ANY OF ITS LICENSORS BE LIABLE FOR ANY INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES OF ANY KIND.

Provider is NOT responsible for:

a. Determining all required configuration settings for the Managed Security appliance and/or Managed Security features. This should be completed by the Client prior to service installation through a Statement of Work or acceptance by client of default Managed Security appliance configurations. For any required configuration changes and/or updates after the initial service installation, Client should communicate those updates through a support case.
b. Ensuring the configuration of and/or performance of Client's secondary two factor authentication system.
c. Ensuring that Client's applications are performing properly across the VPN.
d. Latency across the VPN.
e. The applications within the Client's LAN or traversing the VPN.
f. Opening trouble tickets for remote access end users.
g. Resolving incompatibilities between Client infrastructure and the Managed Security services.
h. Ensuring that Managed Security services provided to Client comply with Clients' compliance related obligations under any rules, regulations, applicable laws or similar requirements. VENYU may, upon Client request, provide documentation to assist Client in its compliance related obligations.
i. Diagnosing, troubleshooting, and/or remediating any Managed Security appliance issues arising out of configuration changes executed by Client users' accounts on the Managed Security appliance.

Client is responsible for:

a. Designating a technical point of contact to work with Provider to lend support for a successful implementation and ongoing support.
b. Providing Provider with all required infrastructure and system information and feature configuration selections to successfully complete the initial assessment as a basis for the service implementation. Client may incur a charge for any information omitted during the assessment, whether intentional or accidental, that requires additional Provider services.
c. Cooperating in scheduling installations as required by Provider personnel.
d. Authorizing any and all modifications, updates, additions/deletions, etc. to the Managed Security services through a support case submitted by an authorized contact in the client portal.
e. IT support and troubleshooting on Client owned servers and workstations. Client may request assistance from VENYU which will be billed as administrative services.
f. Configuration, management, maintenance, and support of any equipment not expressly provided by Provider for use with the Managed Security services.
g. The performance of its applications across the network.

h. Requesting password resets through a support case submitted in the client portal.
i. Requesting user additions, deletions, and/or changes through a support case submitted in the client portal, as applicable.
j. Providing Provider the necessary physical and logical user access to perform services and adding Provider to Client's distribution list to allow Provider to receive notifications related to provided services.
k. Maintaining an updated list in the client portal of authorized Client users including the Authorizing Officer, Technical Contact, and Billing Contact.
l. Communicating any issues promptly to VENYU.
m. Notifying VENYU, through a support case submitted in the client portal, of any critical changes made by Client to the Managed Security services.
n. Notifying VENYU, through a support case submitted in the client portal, of any critical changes in the non-managed Client environment that may impact the services provided by Provider.
o. Ensuring the communication services and equipment used to connect to the VENYU services are reliable. Client agrees to provide a technical environment for the required access to and use of the services. This environment must meet the standard system requirements as determined by VENYU from time to time.
p. Ensuring Client's technical environment complies with the minimum requirements specified in the installation notes for the services provided to Client including, but not limited to bandwidth availability, system I/O and processor speed. VENYU shall have no obligation to provide any services to Client if Client has failed to maintain the minimum technology standards required as noted in the installation notes of the software.