Appendix E to DIR Contract No. DIR-TSO-2724
Avosys PaaS Access Policy
(For Avosys PaaS - ManagedCube Services)

This Avosys PaaS Access Policy ("**Access Policy**") governs your access to and use of the Avosys Platform as a Services (as defined below) provided to you by Avosys Technology Inc. ("**Avosys**"). It sets out the additional rules, conditions and restrictions that apply to you or the entity you represent ("**Customer"**) for use of the Services.

1.0 <u>Avosys PaaS.</u> Avosys Platform as a Services is a collection of Managed Platform Software Solutions, including Managed Hosting, Managed IT Services and related Technical Services (collectively, "ManagedCube" Services) built on top of inter-connected, highly available computing, storage, networking, security and bandwidth components of leading IaaS, PaaS cloud service providers, such as Amazon Web Services, Microsoft Windows Azure and partnered data centers.

2.0 Data Ownership Rights

2.1 <u>Customer Data.</u> Customer Data shall remain under Customer ownership at all times. Avosys is not, and shall not be entitled to any rights, title or interests to Customer Data.

2.2 <u>Customer Owned Data upon Termination.</u> At the conclusion of this Agreement, upon written request from Customer, Avosys shall deliver to the Customer all Customer Data and afterward retain no copies. Avosys cannot transfer any hosted operating systems and any subscription software licenses.

2.3 <u>Avosys Data Transfer Services.</u> Customer may hire Avosys to provide technical services to assist Customer migration of data to Customer. SECURING ALL NEEDED DATA FROM CUSTOMER'S ACCOUNT PRIOR TO SERVICE TERIMNATION SHALL BE CUSTOMER'S RESPONSIBILITY. CUSTOMER'S DATA, APLICATIONS, CONTENT, DATABASES, CONFIGURATION SETTINGS ARE IRREVOCABLY DELETED AFTER SERVICE TERINATION.

2.4 <u>Avosys Data.</u> Avosys Data shall remain under Avosys ownership at all times. Customer is not, and shall not be entitled to any rights, title or interests to Avosys Data.

2.5 <u>Data Backup and Security.</u> Avosys offers standard backup, information assurance, and data security ("Prescribed Services"). If Customer security and/or backup needs are not met by the Prescribed Services, Customer shall detail such requirements to Avosys in a mutually agreed upon Statement of Work. IF CUSTOMER FAILS TO PROVIDE AVOSYS WITH ADDITIONAL SECURITY AND/OR BACKUP SERVICE REQUIREMENTS, AVOSYS WILL NOT BE RESPONSIBLE FOR CUSTOMERS FAILIURE TO DO SO, NOR FOR THE COST OF RECONSTRUCTING DATA OR LOST DATA, DURING THE PERFORMANCE AND DELVERY OF SERVICES UNDER THIS AGREEMENT.

3.0 Service Commitment and Remedies

3.1 <u>Service Level Commitment</u>. Avosys warrants that it will use best efforts and qualified personnel to provide services set forth in each of the SOWs, consistent with industry standards, built upon the Availability Commitments and Service Level Agreements of underlining IaaS and PaaS components provided by Avosys supplied third party IaaS, PaaS Cloud Service providers.

3.1 <u>Remedies.</u> In the event that Customer experiences any of the service performance issues as a result of Avosys' failure to meet its obligations for Service Descriptions provided in each SOW, Avosys will, upon Customer's request within thirty (30) days after the date of service interruption, credit Customer's account up to fifty (50%) percent of Avosys portion of one (1) month of service fees proportional to severity or duration of failure in that month. Service level credits will be available as negotiated by the Parties and set forth in Statement of Work. Customer's right to receive Service Credit(s) or termination of the Customer's use of Avosys PaaS, will be Customer's exclusive remedy

for any unavailability of Avosys PaaS and third party Service Level Commitment of underlining IaaS and PaaS Cloud Service Provider components. .

3.2 <u>Exceptions.</u> The Service Level Commitment Warranty shall not apply to performance issues (i) that result from an emergency update anytime or scheduled maintenance performed by Avosys for which the customer is provided at least 24 hour notice in advance and does not occur from 8:00am to 6:00pm Monday through Friday, State holidays excepted; or (ii) during Customer implementation period; or (iii) from 10:00PM Friday to 7:00AM Monday, Avosys standard scheduled maintenance time window; or (iv) that result from data backup and restore services; or (v) that resulted from Customer's equipment and/or third party equipment and services (not within the sole control of Avosys); or (vi) that result from Customer's requests outside of scheduled maintenance window; or (vii) Force Majeure as set forth in DIR Contract No. DIR-TSO-2724.

4.0 Customer Responsibility.

4.1 <u>Customer Material.</u> Customer is solely responsible for the development, operation, maintenance, and use of Customer's Materials integrated Avosys PaaS. For example, customer is solely responsible for:

(a) The technical operation of Customer materials managed by Customer, including ensuring that calls made by customer material to any Avosys PaaS are compatible with then-current application program interfaces for that Services;
(b) Compliance of Customer Materials with the Avosys Acceptable Use Policy and the law;
(c) Any claims relating to Customer Materials;
(d) Properly handling and processing notices sent to Customer by any person claiming that Customer Materials violate such person's rights, including notices pursuant to the Digital Millennium Copyright Act;
(e) Any action that Customer permit, assist or facilitate any person or entity to take related to this Access Policy, Customer Materials or use of the Services; and
(f) End Users' use of Customer Materials and the Services and ensuring that End Users comply with Customer obligations under this Access Policy and that the terms of Customer agreement with each End User are consistent with this Access Policy.

4.2 <u>Proprietary Right Restrictions.</u> Customer nor any End User may, or may attempt to, (a) modify, alter, tamper with, repair, or otherwise create derivative works of any software included in the Services (except to the extent software included in the Services are provided to Customer under a separate license that expressly permits the creation of derivative works), (b) reverse engineer, disassemble, or decompile the software included in the Services or apply any other process or procedure to derive the source code of any software included in the Services, or (c) access or use the Services in a way intended to avoid incurring fees or exceeding usage limits or quotas.

5.0 Service Interruption.

5.1 <u>General</u>. Avosys may suspend Customer workload if Customer or an End User's use of the Services (i) violates the terms of this Access Policy (including the Avosys Acceptable Use Policy); (ii) poses a security risk to the Services or any other Avosys customer, (iii) may harm Avosys systems or the systems or Materials of any other Avosys customer; or (iv) may subject us to liability as a result of any of the foregoing. Avosys will provide notice of any suspension as soon as practicable to Customer.

5.2 <u>Scope of Interruption</u>. To the extent practicable, Avosys will (i) suspend Customer's right to access or use only those instances, data, or portions of the Services that caused the suspension, and (ii) limit the suspension to those accounts that caused the suspension. If commercially feasible, access to the Services will be restored once the conditions or circumstances giving rise to the suspension have been removed or corrected.

6.0 Disclaimers

6.1 <u>Avosys Supplied Third Party Material</u>. Customer acknowledges that it has selected the Avosys supplied Third Party Material and may provide support to Customer in relation to those products. Customer acknowledges and agrees that its use and possession of the Avosys Supplied Third Party Material shall be subject to the supplier's end user terms and conditions and supplier's warranty, and Customer agrees to look solely to the supplier with respect to all related, services, warranty, service level agreement, and other related claims.

6.2 <u>Warranty</u>. AVOSYS PROVIDES THE SERVICES ON AN "AS IS" BASIS TO CUSTOMER. AVOSYS AND OUR LICENSORS MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND TO CUSTOMER, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE REGARDING THE SERVICES OR ANY THIRD PARTY MATERIALS, INCLUDING ANY WARRANTY THAT THE SERVICES OR THIRD PARTY MATERIALS WILL BE UNINTERRUPTED, ERROR FREE OR FREE OF HARMFUL COMPONENTS, OR THAT ANY MATERIALS, INCLUDING CUSTOMER MATERIALS OR THE THIRD PARTY MATERIALS, WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED. EXCEPT TO THE EXTENT PROHIBITED BY LAW, AVOSYS AND OUR LICENSORS DISCLAIM ALL WARRANTIES, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR QUIET ENJOYMENT, AND ANY WARRANTIES ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE..

7.0 Limitation of Liability. Indemnification shall be in accordance with Section 8K of Appendix A, DIR Contract No. DIR-TSO-2724.

8.0 Definitions

8.1 "End User" means any individual or entity that directly or indirectly through another user: (a) accesses or uses Customer's Materials; or (b) otherwise accesses or uses the Services through Customer.

8.2 "Hosting" Avosys supplied, owned, managed and metered Cloud Server Systems, Storage Services, Networking Services, Data Transfer Services, Cloud Computing IaaS and PaaS Services for use by its Customer and End Users, rented to Customer on a monthly subscription basis, delivered and built on top of Avosys partnered IaaS, PaaS and SaaS Cloud Services providers.

8.3 "Materials" means software, (including machine images), data, configuration, text, audio, video, images or other content.

8.4 "Subscription Software" Avosys supplied, owned, managed and metered third party software, installed on Avosys hosted, shared or dedicated Customer systems for use by Customer and End Users, rented to Customer on a monthly subscription basis.

8.5 "Third Party" Any person or entity other than Avosys and Customer, including Avosys partnered IaaS and PaaS Cloud Service vendors, suppliers and software manufacturers.

8.6 "Acceptable Use Policy" The Avosys Acceptable Use Policy (v2.14.2014) as described below:
This Acceptable Use Policy (this **"Policy"**) describes prohibited uses of the web services offered by Avosys Technology, Inc. and its affiliates (the "Services") and the website located at http://www.avosys.com (the "Avosys Site"). The examples described in this Policy are not exhaustive.

No Illegal, Harmful, or Offensive Use or Content
Customer may not use, or encourage, promote, facilitate or instruct others to use, the Services or Avosys Site for any illegal, harmful or offensive use, or to transmit, store, display, distribute or otherwise make available content that is illegal, harmful, or offensive.

No Security Violations

Customer may not use the Services to violate the security or integrity of any network, computer or communications system, software application, or network or computing device (each, a "System"). Prohibited activities include:

(a) Unauthorized Access. Accessing or using any System without permission, including attempting to probe, scan, or test the vulnerability of a System or to breach any security or authentication measures used by a System.
(b) Interception. Monitoring of data or traffic on a System without permission.
(c) Falsification of Origin. Forging TCP-IP packet headers, e-mail headers, or any part of a message describing its origin or route. This prohibition does not include the use of aliases or anonymous remailers.

No Network Abuse

Customer may not make network connections to any users, hosts, or networks unless Customer has permission to communicate with them. Prohibited activities include:

(a) Monitoring or Crawling. Monitoring or crawling of a System that impairs or disrupts the System being monitored or crawled.
(b) Denial of Service (DoS). Inundating a target with communications requests so the target either cannot respond to legitimate traffic or responds so slowly that it becomes ineffective.
(c) Intentional Interference. Interfering with the proper functioning of any System, including any deliberate attempt to overload a system by mail bombing, news bombing, broadcast attacks, or flooding techniques.
(d) Operation of Certain Network Services. Operating network services like open proxies, open mail relays, or open recursive domain name servers.
(e) Avoiding System Restrictions. Using manual or electronic means to avoid any use limitations placed on a System, such as access and storage restrictions.

No E-Mail or Other Message Abuse

Customer will not distribute, publish, send, or facilitate the sending of unsolicited mass e-mail or other messages, promotions, advertising, or solicitations (like "spam"), including commercial advertising and informational announcements. Customer will not alter or obscure mail headers or assume a sender's identity without the sender's explicit permission. Customer will not collect replies to messages sent from another internet service provider if those messages violate this Policy or the acceptable use policy of that provider.

Reporting of Violations of this Policy

If Customer becomes aware of any violation of this Policy, Customer will immediately notify Avosys and provide Avosys with assistance, as requested, to stop or remedy the violation. To report any violation of this Policy, please email abuse@avosys.comhttp://aws.amazon.com/contact-us/report-abuse/

Appendix F to DIR Contract No. DIR-TSO-2724
AWS Access Policy – State

(For State / Local Public entities utilizing this DIR contract)

This AWS Access Policy ("**Access Policy**") governs your access to and use of the Services (as defined below) of Amazon Web Services, Inc. ("**AWS**") provided to you by your systems integrator, reseller, or services provider ("**Provider**"). It sets out the additional rules, conditions and restrictions that apply to you or the entity you represent ("**you**") for use of the Services. In this Access Policy, "**we**", "**us**", or "**our**" means AWS and any of its affiliates. Please see Section 10 for definitions of capitalized terms.

1. Use of the Services.

1.1 <u>Generally.</u> You are provided access to the Services by your Provider. Your use of and access to the Services are governed by the agreement between you and Provider. This Access Policy supplements the terms of such agreement and may updated by us from time to time. AWS Service Level Agreements do not apply to your use of the Services. Your continued access to and use of the Services is conditioned on your compliance with all laws, rules, regulations, policies and instructions applicable to your use of the Services, including the Policies.

1.2 <u>Account Keys.</u> Provider may provide you with AWS account keys which will allow you to directly access the Services via Provider's account(s). We are not responsible for any activities that occur under these account keys, regardless of whether the activities are undertaken by you, Provider or a third party (including your employees, contractors or agents) and we are also not responsible for unauthorized access to the account.

1.3 <u>Third Party Materials.</u> Through the use of Provider's AWS account(s), you may have access to Third Party Materials, such as software applications provided by third parties, which are made available directly to you by other companies or individuals under separate terms and conditions, including separate fees and charges. Your use of any Third Party Materials is at your sole risk.

2. Your Responsibilities

2.1 <u>Your Materials.</u> You are solely responsible for the development, content, operation, maintenance, and use of Your Materials with the Services. For example, you are solely responsible for:

(a) the technical operation of Your Materials, including ensuring that calls you make to any Service are compatible with then-current application program interfaces for that Service;

(b) compliance of Your Materials with the Acceptable Use Policy, the other Policies, and the law;

(c) any claims relating to Your Materials;

(d) properly handling and processing notices sent to you (or any of your affiliates) by any person claiming that Your Materials violate such person's rights, including notices pursuant to the Digital Millennium Copyright Act;

(e) any action that you permit, assist or facilitate any person or entity to take related to this Access Policy, Your Materials or use of the Services; and

(f) End Users' use of Your Materials and the Services and ensuring that End Users comply with your obligations under this Access Policy and that the terms of your agreement with each End User are consistent with this Access Policy.

2.2 <u>Other Security and Backup.</u> You or Provider are solely responsible for properly configuring and using the Services and taking steps to maintain appropriate security, protection and backup of Your Materials, including using encryption technology to protect Your Materials from unauthorized access

and routinely archiving Your Materials.

2.3 <u>End User Violations.</u> If you become aware of any violation of your obligations under this Access Policy by an End User, you will immediately terminate such End User's access to Your Materials and the Services.

3. Service Interruption.

3.1 <u>General</u>. We may suspend the AWS account(s) through which you access the Services immediately if we determine your or an End User's use of the Services (i) violates the terms of this Access Policy (including the Acceptable Use Policy or Service Terms); (ii) poses a security risk to the Services or any other AWS customer, (iii) may harm our systems or the systems or Materials of any other AWS customer; or (iv) may subject us to liability as a result of any of the foregoing. We will provide notice of any suspension as soon as practicable to Provider, who is solely responsible for providing any notices to you under your agreement with them.

3.2 <u>Scope of Interruption</u>. To the extent practicable, we will (i) suspend your right to access or use only those instances, data, or portions of the Services that caused the suspension, and (ii) limit the suspension to those accounts that caused the suspension. If commercially feasible, access to the Services will be restored once the conditions or circumstances giving rise to the suspension have been removed or corrected. Nothing in this Section 3 will operate to limit your rights or remedies otherwise available to you against Provider under your agreement with them or applicable law.

4. Proprietary Rights

4.1 <u>Services.</u> As between you and us, we or our licensors own and reserve all right, title, and interest in and to the Services. You have the right to use the Services solely as a licensee of Provider in accordance with this Access Policy and the agreement between you and Provider. Except as expressly provided in this Section 4, you obtain no rights to the Services, the AWS Materials or any Third Party Materials.

4.2 <u>Materials.</u> As a part of the Services, you may have access to AWS Materials and Third Party Materials, which may be subject to additional terms and conditions (including the Terms of Use and Apache Software License). By using those materials, you are subject to such additional terms. You are solely responsible for securing any necessary approvals for the download and use of such materials.

4.3 <u>Restrictions.</u> Neither you nor any End User may use the Services in any manner or for any purpose other than as expressly permitted by this Access Policy and the agreement between you and Provider. Neither you nor any End User may, or may attempt to, (a) modify, alter, tamper with, repair, or otherwise create derivative works of any software included in the Services (except to the extent software included in the Services are provided to you under a separate license that expressly permits the creation of derivative works), (b) reverse engineer, disassemble, or decompile the software included in the Services or apply any other process or procedure to derive the source code of any software included in the Services, or (c) access or use the Services in a way intended to avoid incurring fees or exceeding usage limits or quotas. All rights and access granted to you with respect to the Services are conditioned on your continued compliance with this Access Policy, and you will immediately discontinue your use of the Services if you cannot comply with this Access Policy. You will not assert, nor will you authorize, assist, or encourage any third party to assert, against us or any of our customers, vendors, business partners, or licensors, any patent infringement or other intellectual property infringement claim regarding any Services or AWS Materials that you have used.

4.4 <u>Suggestions.</u> If you provide any Suggestions to us when using the Services, you hereby grant to AWS and its affiliates a perpetual, irrevocable, non-exclusive, worldwide, royalty-free right and license to reproduce, distribute, make derivative works based upon, publicly display, publicly perform, make, have made, use, sell, offer for sale, and import the Suggestions, including the right to sublicense such rights through multiple tiers, alone or in combination.

4.5 <u>Government Rights.</u> If you are using the Services on behalf of the government and these terms fail to meet the government's needs or are inconsistent in any respect with federal or state law, you will immediately discontinue your use of the Services (including any AWS Materials).

5. Representations and Warranties. You represent and warrant that (a) you and your End Users' use of the Services (including any use by your employees and personnel) will not violate this Access Policy; (b) you or your licensors own all right, title, and interest in and to Your Materials; (c) Your Materials (including the use, development, design, production, advertising, or marketing of your Materials) or the combination of your Materials with other applications, content or processes, do not and will not violate any applicable laws or infringe or misappropriate any third-party rights; and (d) your use of the Services will not cause harm to any End User.

6. Indemnification. Indemnification shall be in accordance with Section 8A of Appendix A, DIR Contract No. DIR-TSO-2724.

7. Disclaimers. WE PROVIDE THE SERVICES ON AN "AS IS" BASIS TO PROVIDER. WE AND OUR LICENSORS MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND TO YOU, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE REGARDING THE SERVICES OR ANY THIRD PARTY MATERIALS, INCLUDING ANY WARRANTY THAT THE SERVICES OR THIRD PARTY MATERIALS WILL BE UNINTERRUPTED, ERROR FREE OR FREE OF HARMFUL COMPONENTS, OR THAT ANY MATERIALS, INCLUDING YOUR MATERIALS OR THE THIRD PARTY MATERIALS, WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED. EXCEPT TO THE EXTENT PROHIBITED BY LAW, WE AND OUR LICENSORS DISCLAIM ALL WARRANTIES, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR QUIET ENJOYMENT, AND ANY WARRANTIES ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE.

8. Limitations of Liability. Limitation of Liability shall be in accordance with Section 8K of Appendix A, DIR Contract No. DIR-TSO-2724.

9. Miscellaneous.

9.1 <u>Governing Law; Venue.</u> Choice of Law shall be in accordance with Section 3D of DIR Contract No. DIR-TSO-2724.

9.2 <u>Entire Agreement.</u> DIR Contract No. DIR-TSO-2724 and this Access Policy is the entire agreement between you and us regarding the Services, including any materials. It supersedes all prior or contemporaneous representations, understandings, agreements, or communications between you and us, whether written or verbal, regarding the subject matter of this Access Policy. If the terms of this document are inconsistent with the terms contained in your agreement with Provider, the terms contained in this document will control. We will not be bound by, and specifically object to, any term, condition or other provision which is different from or in addition to the provisions of this Access Policy (whether or not it would materially alter it) and which is submitted by you in any order, receipt, acceptance, confirmation, correspondence or other document. In the event of a conflict, the DIR Contract controls.

9.3 <u>Survival.</u> The following provisions will survive any termination of your use of the Services: Sections 2.1, 4, 5, 6, 7, 8, 9 and 10.

10. Definitions.

10.1 <u>Acceptable Use Policy.</u> The AWS Acceptable Use Policy (v11.2.2011) as described below:

This Acceptable Use Policy (this **"Policy"**) describes prohibited uses of the web services offered by Amazon Web Services, Inc. and its affiliates (the "Services") and the website located at http://aws.amazon.com (the "AWS Site"). The examples described in this Policy are not exhaustive. We may modify this Policy at any time by posting a revised version on the AWS Site. By using the

Services or accessing the AWS Site, you agree to the latest version of this Policy. If you violate the Policy or authorize or help others to do so, we may suspend or terminate your use of the Services.

No Illegal, Harmful, or Offensive Use or Content

You may not use, or encourage, promote, facilitate or instruct others to use, the Services or AWS Site for any illegal, harmful or offensive use, or to transmit, store, display, distribute or otherwise make available content that is illegal, harmful, or offensive. Prohibited activities or content include:

(a) Illegal Activities. Any illegal activities, including advertising, transmitting, or otherwise making available gambling sites or services or disseminating, promoting or facilitating child pornography.
(b) Harmful or Fraudulent Activities. Activities that may be harmful to others, our operations or reputation, including offering or disseminating fraudulent goods, services, schemes, or promotions (e.g., make-money-fast schemes, Ponzi and pyramid schemes, phishing, or pharming), or engaging in other deceptive practices.
(c) Infringing Content. Content that infringes or misappropriates the intellectual property or proprietary rights of others.
(d) Offensive Content. Content that is defamatory, obscene, abusive, invasive of privacy, or otherwise objectionable, including content that constitutes child pornography, relates to bestiality, or depicts non-consensual sex acts.
(e) Harmful Content. Content or other computer technology that may damage, interfere with, surreptitiously intercept, or expropriate any system, program, or data, including viruses, Trojan horses, worms, time bombs, or cancelbots.

No Security Violations
You may not use the Services to violate the security or integrity of any network, computer or communications system, software application, or network or computing device (each, a "System"). Prohibited activities include:

(a) Unauthorized Access. Accessing or using any System without permission, including attempting to probe, scan, or test the vulnerability of a System or to breach any security or authentication measures used by a System.
(b) Interception. Monitoring of data or traffic on a System without permission
(c) Falsification of Origin. Forging TCP-IP packet headers, e-mail headers, or any part of a message describing its origin or route. This prohibition does not include the use of aliases or anonymous remailers.

No Network Abuse
You may not make network connections to any users, hosts, or networks unless you have permission to communicate with them. Prohibited activities include:

(a) Monitoring or Crawling. Monitoring or crawling of a System that impairs or disrupts the System being monitored or crawled.
(b) Denial of Service (DoS). Inundating a target with communications requests so the target either cannot respond to legitimate traffic or responds so slowly that it becomes ineffective.
(c) Intentional Interference. Interfering with the proper functioning of any System, including any deliberate attempt to overload a system by mail bombing, news bombing, broadcast attacks, or flooding techniques.
(d) Operation of Certain Network Services. Operating network services like open proxies, open mail relays, or open recursive domain name servers.
(e) Avoiding System Restrictions. Using manual or electronic means to avoid any use limitations placed on a System, such as access and storage restrictions.

No E-Mail or Other Message Abuse
You will not distribute, publish, send, or facilitate the sending of unsolicited mass e-mail or other messages, promotions, advertising, or solicitations (like "spam"), including commercial advertising and informational announcements. You will not alter or obscure mail headers or assume a sender's identity without the sender's explicit permission. You will not collect replies to messages sent from

another internet service provider if those messages violate this Policy or the acceptable use policy of that provider.

Our Monitoring and Enforcement
We reserve the right, but do not assume the obligation, to investigate any violation of this Policy or misuse of the Services or AWS Site. We may:

(a) Investigate violations of this Policy or misuse of the Services or AWS Site; or
(b) Remove, disable access to, or modify any content or resource that violates this Policy or any other agreement we have with you for use of the Services or the AWS Site.

We may report any activity that we suspect violates any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties. Our reporting may include disclosing appropriate customer information. We also may cooperate with appropriate law enforcement agencies, regulators, or other appropriate third parties to help with the investigation and prosecution of illegal conduct by providing network and systems information related to alleged violations of this Policy.

Reporting of Violations of this Policy
If you become aware of any violation of this Policy, you will immediately notify us and provide us with assistance, as requested, to stop or remedy the violation. To report any violation of this Policy, please follow our abuse reporting process.

10.2 AWS Materials. Materials we make available in connection with the Services or on the AWS Site to allow access to and use of the Services, including WSDLs; Documentation; sample code; software libraries; command line tools; and other related technology. AWS Materials does not include the Services.

10.3 AWS Service Level Agreement. All service level agreements that we offer with respect to the Services and post on the AWS Site, as they may be updated by us from time to time.

10.4 AWS Site. http://aws.amazon.com and any successor or related site designated by us.

10.5 Documentation. The developer guides, getting started guides, user guides, quick reference guides, and other technical and operations manuals, instructions and specifications for the Services currently located at http://aws.amazon.com/documentation, as such documentation may be updated by us from time to time.

10.6 End User. Any individual or entity that directly or indirectly through another user: (a) accesses or uses Your Materials; or (b) otherwise accesses or uses the Services through you.

10.7 Materials. Software (including machine images), data, text, audio, video, images or other content.

10.8 Policies. The Acceptable Use Policy, the Terms of Use, the Service Terms, all restrictions described in the AWS Materials and on the AWS Site, and any other policy or terms referenced in or incorporated into this Access Policy.

10.9 Services. Collectively or individually (as applicable), the web services made commercially available by us to Provider for use under this Access Policy, including (as applicable) those web services described in the Service Terms.

10.10 Suggestions. All suggested improvements to the Services or AWS Materials that you provide to us.

10.11 Third Party Materials. Materials made available to you by any third party on the AWS Site or in conjunction with the Services.

10.12 <u>Your Materials.</u> Materials you or any End User (a) run on the Services, (b) cause to interface with the Services, or (c) upload to the Services or otherwise transfer, process, use or store in connection with the Services.

Avosys will review AWS Service Terms and Terms of Use with Customer for approval prior to the execution of a Statement of Work or Service Agreement.

Microsoft Customer License Terms

TERMS AND CONDITIONS REGARDING USE OF MICROSOFT SOFTWARE

This document governs the use of Microsoft software, which may include associated media, printed materials, and "online" or electronic documentation (individually and collectively, "License Products") provided by Avosys Technology, Inc. (hereinafter referred to as "Company") Company does not own the Licensed Products and the use thereof is subject to certain rights and limitations of which Company must inform you. Your right to use the License Products is subject to the terms of your agreement with Company, and to your understanding of, compliance with, and consent to the following terms and conditions, which Company does not have authority to vary, alter or amend.

1) **DEFINITIONS.**

"Client Software" means software that allows a Device to access or utilize the services or functionality provided by Server Software.

"Device" means each of a computer, workstation, terminal, handheld PC, pager, telephone, personal digital assistance, "smart phone" server or other electronic device.

"Server Software" means software that provides services or functionality on a computer acting as a server.

"Software Documentation" means any end user document included with server software.

"Redistribution Software" means the software described in Paragraph 4 ("Use of Redistribution Software") below.

2) **OWNERSHIP OF LICENSED PRODUCTS.** The License Products are license to Company from an affiliate of the Microsoft Corporation (collectively "Microsoft"). All title and intellectual property rights in and to the License Products (and the constituent elements thereof, including but not limited to any images, photographs, animations, video, audio, music, text and "applets" incorporate into the License Products) are owned by Microsoft or its suppliers. The License Products are protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. Your possession, access, or use of the License Products does not transfer any ownership of the Licensed Products or any intellectually property rights to you.

3) **USE OF CLIENT SOFTWARE.** You may use the Client Software installed on your Devices Company online in accordance with the instructions, and only in connection with the services, provided to you by Company. The terms of this document permanently and irrevocably supersede the terms of any Microsoft End User License Agreement that may be presented in electronic form during your use of the Client Software.

4) **USE OF REDISTRIBUTION SOFTWARE.** In connection with the services provided to you by Company, you may have access to certain "sample," redistribution" and/or software development ("SDK") software code and tools (individually and collectively "Redistribution Software"). YOU MAY NOT USE, MODIFY, COPY, AND/OR DISTRIBUTE ANY REDISTRIBUTION SOFTWARE UNLESS YOU EXPRESSLY AGREE TO ANDCOMPLY WITH CERTAIN ADDITIONAL TERMS CONTANTAINED IN THE SERVICES PROVIDER USE RIGHTS ("SPUR") APPLICABLE TO COMPANY, WHICH TERMS MUST BE PROVIDED TO YOU BY COMPANY. Microsoft does not permit you to use and Redistribution Software unless you expressly agree to and comply with such additional terms, as provided to you by Company.

5) **COPIES.** You may not make any copies of the License Product; provided, however, that you may (a) make one copy of Client Software on your Device as expressly authorized by Company; and (b) you

may make copies of certain Redistribution Software in accordance with Paragraph 4 ((Use of Redistribution Software). To the extent allowable under record retention laws and policies, you must erase or destroy all such Client Software and/or Redistribution Software upon termination of cancellation of your agreement with Company, upon notice from Company or upon transfer of your Device to another person or entity, whichever occurs first.

6) LIMITATIONS ON REVERSE ENGINEERING, DECOMPILATION AND DISASSEMBLY. You may not reverse engineer, decompile, or disassemble the License Products, except and only to the extent that applicable law, notwithstanding this limitation, expressly permits such activity.

7) NO RENTAL. You may not rent, lease, lend, pledge, or directly or indirectly transfer or distribute the Licensed Products to any third party.

8) TERMINATION. Terminations will be handled in accordance with Appendix A, Section 9B of DIR Contract No. DIR-TSO-2724.

9) NO WARRANTIES, LIABILITIES OR REMEDIES BY MICROSOFT. ANY WARRANTIES, LIABILITY FOR DAMAGES AND REMEDIES, IF ANY, ARE PROVIDED SOLELY BY COMPANY AND NOT BY MICROSOFT, ITS AFFILIATES OR SUBSIDIARIES.

10) PRODUCT SUPPORT. Any support for the License Products is provided to you by Company and is not provided by Microsoft, its affiliates or subsidiaries.

11) NOT FAULT TOLERANT. THE LICENSED PRODUCTS MAY CONTAIN TECHNOLOGY THAT IS NOT FAULT TOLERANT AND ARE NOT DESIGED, MANUFACTURED, OR INTENDED FOR USE IN ENVIRONMENTS OF APPLICATIONS IN WHICH THE FAILURE OF THE LICENSED PRODUCTS COULD LEAD TO DEATH, PERSONAL INJURY, OR SEVERE PHYSICAL, PROPERTY OR ENVIRONMENTAL DAMAGE.

12) EXPORT RESTRICTIONS. The License Products are of U.S. origin for purposes of U.S. export control laws. You agree to comply with all applicable international and U.S. laws that apply to the License Products, including the U.S. Export Administration Regulations, as well as end-used, end-use and destination restrictions issued by the U.S. and other governments. For additional information, see http://www.microsoft.com/exporting/.