

**Appendix E to DIR Contract No. DIR-TSO-4090
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 Avosys PaaS. 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 Customer Data. 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 Customer Owned Data upon Termination. 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 Avosys Data Transfer Services. 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 TERMINATION SHALL BE CUSTOMER'S RESPONSIBILITY. CUSTOMER'S DATA, APPLICATIONS, CONTENT, DATABASES, CONFIGURATION SETTINGS ARE IRREVOCABLY DELETED AFTER SERVICE TERMINATION.

2.4 Avosys Data. 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 Data Backup and Security. 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 CUSTOMER'S FAILURE TO DO SO, NOR FOR THE COST OF RECONSTRUCTING DATA OR LOST DATA, DURING THE PERFORMANCE AND DELIVERY OF SERVICES UNDER THIS AGREEMENT.

3.0 Service Commitment and Remedies

3.1 Service Level Commitment. 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.

3.2 Remedies. 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. .

3.3 Exceptions. 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-4090.

4. Customer Responsibility.

4.1 Customer Material. 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 Proprietary Right Restrictions. 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. Service Interruption.

5.1 General. 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 Scope of Interruption. 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. Disclaimers

6.1 Avosys Supplied Third Party Material. 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 Warranty. 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..

6.3 Limitation of Liability. Indemnification shall be in accordance with Section 9K of Appendix A, DIR Contract No. DIR-TSO-4090.

7.0 Definitions

7.1 "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.

7.2 "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.

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

7.4 "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.

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

7.6 "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.

7.7 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.

7.8 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.

7.9 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.

7.10 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.

7.11 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.com