



## DYNASYS CLOUD PROGRAM DOCUMENT

This Cloud Program Document establishes terms and conditions for Cloud Services ordered by Customer and provided by Vendor under an Order Document executed under a Cloud Services Agreement. Terms not otherwise defined herein shall have the meanings set forth in the Cloud Services Agreement.

### Cloud Services

General Terms	
<b>Subscription Terms</b>	<p>Upon Vendor’s acceptance of Customer’s order under an Order Document Vendor shall make the Cloud Applications available to Customer on a subscription basis and provide the other Cloud Services as described herein. Customer’s usage of the Cloud Applications shall be limited to the subscription levels set forth in the Order Document. Customer shall not acquire any further rights in or to the Cloud Applications and Customer’s right to access to the Cloud Applications shall cease upon termination of the Order Document. Customer shall not be provided with a copy of the Cloud Applications.</p> <p>The user metrics applicable to subscription to the Cloud Services are defined as follows:  <u>Administrator</u> shall mean a Named User that may set up, model, administer the Software and run batches. The Administrator is a Planner, however, an Administrator is not authorized to use the Software for planning purposes in the “production” platform as a Planner (i.e. an Administrator may not perform planning tasks using the Software).  <u>Collaborative User</u> shall mean a Named User authorized to view and modify existing data. The Collaborative User may also add references, make changes to horizons and import or export data.  <u>Named User</u> shall mean each individual or process that is authorized to access the Cloud Applications.  <u>Planner</u> shall mean a Named User that can perform planning activities using the Software. In particular, a planner may perform special calculations (sales forecasts, plan calculations, DRP, etc.), program supplementary calculations or rule bases, add references, make changes to horizons, etc.), program supplementary calculations or rule bases, add references, make changes to horizons, etc.  <u>Planning Site</u> shall mean the physical site, named in a Order Document, for which planning is performed supported by the Software.  <u>Product Division</u> shall mean a family of the Customer’s products, designated in the Order Document.  <u>Viewer</u> shall mean a Named User who is only authorized to view existing data.</p> <p>Customer’s use of the Cloud Applications shall be subject to the following restrictions. Customer shall:</p> <ul style="list-style-type: none"> <li>• only use the Cloud Applications for its own business purposes.</li> <li>• restrict usage of the Cloud Applications to the purchased subscription levels.</li> <li>• use unique logon IDs for individuals, devices and processes (i.e. logon IDs shall not be shared).</li> <li>• not use any method, software or technology which hides or understates the actual number of users accessing the Cloud Applications (e.g. by circumventing the Cloud Applications log-on process).</li> <li>• not provide access to the Cloud Applications to third parties, except as explicitly permitted herein.</li> </ul>

	<ul style="list-style-type: none"> <li>not use the Cloud Applications for timesharing, rental or service bureau purposes.</li> </ul> <p>Customer may permit a third party to access the Cloud Applications only if such third party forms part of the Customer’s supply chain (i.e. the third party is a supplier or a customer of the Customer) and provided that such access is limited to the benefit of Customer. Customer shall be responsible for compliance with the terms of this Agreement by any third party granted access to the Cloud Applications by Customer.</p> <p>Customer shall appoint and maintain a “Super User” who shall function as the contact for support issues. Customer may appoint a replacement Super User for situations in which the Super User is not available. Super User means a member of Customer’s personnel who participates or has participated actively with Vendor in the implementation of the Cloud Applications. The Super User must have expertise on the Customer’s business processes and shall form the link between Vendor and Customer. The Super User is required to have completed all required training modules (Super User cycle) and to have all required knowledge of the Customer’s information systems.</p>
<b>Version Management</b>	<p>At the commencement of the Cloud Services the latest generally-available versions of the Cloud Applications shall be deployed unless otherwise agreed. Thereafter, Vendor shall in its discretion apply new versions, bug fixes, service packs and other updates in accordance with Vendor’s standard operating procedures, <u>provided, however</u>, that (1) Vendor shall give reasonable advance notice and obtain Customer’s consent prior to applying any such update; and (2) Customer may withhold consent if Customer reasonably believes that applying such update shall cause material disruption to Customer’s business. In the event Customer withholds consent then Vendor shall not be responsible for any changes in software or system performance resulting from not applying such update. Notwithstanding the foregoing, Vendor may immediately shut down all environments if Customer withholds consent to an update and the absence of such update causes, in Vendor’s reasonable opinion, material risk to the security of Vendor’s systems.</p>
<b>Environments</b>	<p>As part of the Cloud Services, Vendor will provide one production environment and, on request, up to two non-production environments. Vendor may provide additional environments for additional fees. The service levels outlined in this Program Document apply to the production environment only (i.e. only to the environment that contains Customer’s live data).</p>
<b>Environment availability commitment</b>	<p>Vendor warrants the availability of the production environment for 99.5% (ninety nine and five tenths percent) of the Scheduled Hours of Operation during Go-Live status. This availability commitment does not apply to either Build status or Transition status.</p> <p>Environment availability statuses are defined as follows:</p> <ul style="list-style-type: none"> <li>Build – the initial status, during which the environment is being built prior to release to Customer.</li> <li>Transition – after the completion of the Build status, during which the environment is configured prior to Go-Live.</li> <li>Go-Live – the status following the first production use of the environment per the scheduled Go-Live date mutually agreed by Vendor and Customer.</li> </ul>
<b>Scheduled Hours of Operation</b>	<p>The Scheduled Hours of Operation are defined as 24/7 (Monday through Sunday during 24 hours each day), minus Planned Maintenance Windows and minus the daily restart of the DSCP services. A Planned Maintenance Window is a period during which the Cloud Services will be unavailable, downtime not to exceed eight (8) hours.</p> <p>Planned Maintenance Windows shall be announced in advance to Customer, the exact times to be agreed by parties and documented in writing.</p> <p>Information on Planned Maintenance Windows is available within the Customer’s online collaborative share location or will be communicated in writing (by email or otherwise).</p>

<b>Measuring availability</b>	<p>Unavailability of the production environment is measured over a calendar month and is based on total outage time incurred by the Customer. Environment unavailability will exist when the environment is unable to transmit Internet Protocol data packets to the Vendor designated point of presence. Environment unavailability is measured until the time Vendor determines that the affected service is again able to transmit and receive data.</p> <p>Customers are responsible for the connection between their sites (and users) and the Vendor data center. The Cloud Services rely on an Internet Protocol connection. If the connection is slowed or becomes unavailable, the Cloud Applications may become unresponsive or unusable. Inadequate performance by network connections and/or computer infrastructure not under Vendor's control is not covered by Vendor's environment availability commitment.</p>
<b>Service credits and conditions</b>	<p>If Vendor fails to meet this environment availability commitment for any calendar month and Customer provides Vendor with a written request within thirty (30) days of the last day of the month in which such failure occurred, Vendor will provide a service credit to Customer's account that may be applied against subsequent invoices equal to the fee for one (1) day of Cloud Services (excluding taxes, pass-through charges, credits, installation or other one-time charges) for each cumulative hour of unavailability or failure during the applicable month, exceeding 0.5% (five tenths of one percent) of the time, up to a maximum of the total Cloud Services fees charged by Vendor to Customer for such month.</p> <p>Service credits will not be available to Customer in cases where the environment is unavailable as a result of (a) the acts or omissions of Customer or its employees, contractors, agents or end-users; (b) the failure, malfunction, or limitation of throughput of equipment, network, software, applications or systems (including web services, ODBC and ftp locations) not owned or directly controlled by Vendor; (c) circumstances or causes beyond the control of Vendor, including, without limitation, events of force majeure and third-party attacks on the environment (such as ping and denial of service attacks); or (d) scheduled outages such as outages during Planned Maintenance Windows. Such credits will be granted only if Customer provides Vendor with all requested information in an expeditious manner and affords Vendor full cooperation to make necessary repairs, maintenance, testing, etc.</p> <p>THIS SECTION SETS FORTH CUSTOMER'S SOLE AND EXCLUSIVE REMEDY FOR SERVICE INTERRUPTIONS, SERVICE RESPONSE ISSUES AND/OR SERVICE DEFICIENCIES OF ANY KIND WHATSOEVER.</p>
<b>Disk Space</b>	<p>The Cloud Services include transaction data storage disk space for each environment in the amount of (A) 1.25 Gb for each Named User subscribed to by Customer plus (B) 1.25 Gb for every 4 Limited Named Users subscribed to by Customer.</p>
<b>Backup</b>	<ul style="list-style-type: none"> <li>• Data to be backed up: all installed Vendor Application and database associated with the production and test environments. Backup of development environment shall require additional fees.</li> <li>• Backup Schedule: incremental backup daily; full backup weekly.</li> <li>• Backup Storage: daily and weekly backups are replicated to off-site digital storage.</li> <li>• Backup Retention Schedule: incremental backups are retained for 3 weeks then are overwritten. Full backups are retained for 13 weeks.</li> <li>• Restoring Files: Customer may request restoration of data by opening a Vendor support ticket. Restore will be performed to the environment specified by the customer.</li> </ul>
<b>Environment and database refreshes</b>	<p>On Customer's request, Vendor shall refresh each of the test and development environments once per calendar month.</p>

	On Customer's request, Vendor shall refresh the database twice per calendar month.
<b>Disaster Recovery</b>	<p><u>Vendor responsibilities</u></p> <ul style="list-style-type: none"> <li>• A "Disaster" is defined as an unrecoverable event at the Vendor data center or Vendor network provider that causes the Customer's production environment at the primary site to be unavailable for (8) hours or more.</li> <li>• Vendor shall make the determination of when and if a Disaster has occurred. If an event or failure causes unavailability that Vendor determines will continue eight (8) hours or more, then Vendor shall declare a Disaster immediately.</li> <li>• Although the technical setup is designed for immediate up-time in case of a Disaster, Vendor will provide a Recovery Time Objective (RTO) of (8) hours after a Disaster has been declared by Vendor at the main hosting facility.</li> <li>• Although the technical setup is designed for zero data loss, Vendor will provide a Recovery Point Objective (RPO) of one (1) hour from when the unavailability initially occurred.</li> <li>• This service covers only the production environment.</li> <li>• Non production environments will be suspended when disaster recovery is enacted.</li> </ul> <p><u>Customer responsibilities</u></p> <ul style="list-style-type: none"> <li>• Customer must have an operational disaster recovery plan in place prior to implementation.</li> <li>• Customer must commit to review the disaster recovery plan every six months.</li> <li>• Customer must commit to test the disaster recovery plan annually (the Disaster Recovery Offering includes two person days Vendor assistance with testing).</li> <li>• The Customer will be responsible for the connectivity to the Vendor designated point of presence for the disaster recovery center, including network rerouting in the event of a Disaster.</li> <li>• Customer will be responsible for reconfiguring client configurations for connection the Vendor designated point of presence for the disaster recovery center.</li> <li>• A planned outage will be required to revert to the main hosting facility once the cause of the Disaster has been resolved.</li> <li>• Customer will be responsible for enabling and managing any third-party interfaces or third-party products in the event of a Disaster.</li> </ul>

Service Delivery Management ("R" indicates the party responsible)			
Task	Frequency	Vendor	Customer
<b>Delivery Management - On Boarding</b>			
Architecture overviews	One time on boarding activity	R	
Cloud Policies and Procedures reviews	One time on boarding activity	R	
<b>Delivery Management - Client Manager</b>			
Key performance indicators reviews - KPI' available on Vendor's 'My QAD Cloud' portal	As Needed	R	
Coordinated planned application/DBA/Server downtime	As Needed	R	
Process & procedure changes & training	As Needed	R	

Planned and unplanned outage notifications	As Needed	R	
Financial reviews	As Needed	R	
Escalation updates	As Needed	R	
Vendor share community - Vendor share location setup and rollout	As Needed	R	
Provide Vendor share environment forum & documentation	As Needed	R	

System Management ("R" indicates the party responsible)			
Task	Frequency	Vendor	Customer
<b>Database Maintenance and Management</b>			
Database installation	One time on boarding activity	R	
Database & OS backups	Daily	R	
Database restores	2 per Month	R	
Database analysis	Yearly	R	
Database Management & Standard maintenance tasks	As Needed	R	
<b>Application Maintenance and Management</b>			
Printer setup after customer request	As Needed	R	
Local printer troubleshooting	As Needed		R
Print server setup and availability	As Needed		R
Local printer setup and management	As Needed		R
System performance monitoring 24x7	As Needed	R	
Vendor product installation	As Needed	R	
Vendor patch installation (scheduled by Vendor)	As Needed	R	
Vendor Service Pack installation	Annual	R	
Run DB data archive and delete	As Needed		R
All Data loads	As Needed		R
Transition of On Premise Vendor components to Cloud	As Needed		R
<b>Restores</b>			
Provide Restore validation	4 times annually	R	

Infrastructure Management ("R" indicates the party responsible)			
Task	Frequency	Vendor	Customer
<b>Server Maintenance and Management</b>			
Maintain Operating System level security (Provide security according to available procedure)	As Needed	R	

Operating system management	As Needed	R	
Network setup, Site to site VPN, purchase/install Vendor approved networking data circuit	As Needed		R
Additional external security review will be customer responsibility and jointly scheduled before they are performed	As Needed		R

**Support for Environment Infrastructure**

The following support service levels pertain only to the environment infrastructure described above. Service levels pertaining to the operation of the Cloud Applications are set forth in Vendor’s Customer Support Guide.

Vendor will respond to Customer’s request for support upon receipt of Customer’s incident report. When Vendor receives the incident report, Vendor’s support contact will respond to the designated person making the report. Response time goals for the various severity levels are outlined below along with resolution goal targets. These resolution goals are only set as targets to measure quality and provide continuous improvement metrics. Customer shall identify to Vendor up to three (3) individuals who are authorized to submit incident reports. Such individuals shall serve as the point of contact for the incident reports.

Severity level	Description	Vendor Response Goal	Vendor Resolution Goal
<b>0</b>	Highest priority available for cases. Business critical (down system or Cloud Applications not available to more than 1 user) condition in a production environment. No “work around” exists. Requires immediate solution.	Direct connection to support personnel or a response within 30 minutes.	8 hours from time call is answered. Resolution is understood as being provided with a work-around or a permanent solution that eliminates the business critical condition, with 90% of tickets resolved.
<b>1</b>	Critically impacts the customer's business operation. Production is operational (i.e. access to Cloud Applications is possible) or a “work around” exists, but severely restricting production.	2 Hours	2 days from time call is answered. Resolution is understood as being provided with a work-around or a permanent solution that eliminates the condition, with 90% of tickets resolved.
<b>2</b>	General product questions regarding the Cloud Applications. Production or non-production environments.	4 Hours	5 days Resolution is understood as being provided with a work-around or a permanent solution that eliminates the condition, with 80% of tickets resolved.
<b>3</b>	Informational or environment related questions about the Cloud Applications, and / or change requests. Production or non-production environments.	8 Hours	15 days Resolution is understood as being provided with a work-around or a permanent solution that eliminates the condition, with 80% of tickets resolved.

### Standard Support Hours

<b>Definition:</b>	"Standard Support hours" are Monday to Friday for French worked days, from 9.00am to 12.00am and 2.00pm to 5.00pm French time UTC+1. References to Days and Hours take into account the previously described opening hours.
<b>Off Hours Support</b>	Off hours support hours are provided to handle severity 0 cases. Issues of lower severity are deferred to the beginning of the following business day for follow-up. Vendor will make all reasonable efforts to respond to "Off Hours" support calls in the same response time as defined for normal and customary daily operations.

Support for Cloud Applications ("R" indicates the party responsible)			
Task	Frequency	Vendor	Customer
Support for Cloud Applications shall be provided in accordance with Vendor's Customer Support Guide.			
Access to Knowledge Management program; Vendor will make the following items available: <ul style="list-style-type: none"> <li>On-line training on industry and application content where available</li> <li>On-line Qbits; video based training on specific topics within the application where available</li> <li>Mastery tests at end of training discipline</li> </ul>	As Needed	R	
Account review <ul style="list-style-type: none"> <li>Review Support process and tools that are available</li> <li>Review customer's incident metrics</li> </ul>	As Needed	R	
T1 - First point of contact <ul style="list-style-type: none"> <li>Provide basic troubleshooting</li> <li>Determine incident severity</li> <li>Coordinate issue resolution</li> </ul>	As Needed	R	
T2 - Resolves complex issues related to product <ul style="list-style-type: none"> <li>Deliver knowledge to T1</li> <li>Identify process improvements</li> <li>Determine escalation priority</li> <li>Assist in identifying data discrepancies</li> </ul>	As Needed	R	
T3 - Provide bug fixes via service pack, bug fix or workaround	As Needed	R	
Monitoring of open incidents	As Needed	R	
Online incident management and reporting	As Needed	R	
Access to knowledgebase of Vendor and Progress	As Needed	R	
Provide qualified contacts for each business function to interface with Vendor Support	As Needed		R
Provide contact for overall responsibility of support relationship and meet regularly to review service levels and process improvements <ul style="list-style-type: none"> <li>This person will be responsible for coordinating all internal activities related to support requests</li> </ul>	As Needed		R
All business data setup and data standards	As Needed		R
Review documented procedures	As Needed		R

Provide remote access to all supported services and systems via dedicated network site to site connection	As Needed		R
End user assistance in testing of installed ECO's, patches, service packs, or upgrades	As Needed		R
Support incidents entered with required information using Vendor's online help desk ticket system <ul style="list-style-type: none"> <li><a href="http://www.dys.com/en/support/online-support/">http://www.dys.com/en/support/online-support/</a></li> </ul>	As Needed		R
Initial application security core model <ul style="list-style-type: none"> <li>Initial creation of the application security to-be model</li> </ul>	One time activity		R
All end user testing	As Needed		R
Review third-party policies for interface to Cloud environment	As Needed		R
Approval of Planned Maintenance Windows by mutual agreement between Customer and Vendor	As Needed	R	R
Security of local area network and client machines. Responsible for any impact that a breach of local area network or client security may have on the service levels outlined in this document.	As Needed		R
Vendor will have access to Customer's business processes documents or personnel to understand the business implications of a solution	As Needed		R
Escalation process will be defined by both parties and with assigned personnel as escalation points	As Needed	R	R
All requests outside of Severity 0 will be received via the Vendor On-Line Support user interface	As Needed		R
All Severity 0 requests will be called into Vendor's emergency Support line	As Needed		R
Storage of credit card data and PCI (personal credit information) legal compliance are not supported. Customer is responsible for ensuring any required PCI legal compliance	As Needed		R

### Security Procedures

Vendor shall be responsible for establishing and maintaining an information security program related to securing and protecting Customer's data and Customer's customers' data (collectively "Data") that is designed to: (i) ensure the security and confidentiality of the Data; (ii) protect against any anticipated threats or hazards to the security or integrity of Data; (iii) protect against unauthorized access to or use of Data; (iv) ensure the proper disposal of Data; and, (v) ensure that all contractors / subcontractors of Vendor, if any, comply with all of the foregoing.

In addition to the above, and more specifically, Vendor shall meet or exceed industry accepted standards to comply with the following:

#### **A. Personnel Security**

1. Vendor shall perform background checks on all applicable employees prior to employment.
2. Vendor shall remove employee and contractor access rights from Vendor's systems, servers, and networks utilized in the performance of its obligations under this Agreement within twenty-four (24) hours of the termination effective date.
3. Vendor shall maintain a list of users with access to Customer's systems, and will provide a copy of this list



to Customer upon request. Vendor shall notify Customer within a reasonable timeframe when a user no longer requires access, so that Customer may disable their access to Customer's systems.

4. Vendor shall provide security awareness training to its employees at least annually.

#### **B. Physical and Environmental Security**

1. Vendor shall have and implement access control policies and procedures for its facilities and data centers.

2. Vendor's data centers used in the Vendor's performance under this Agreement shall be equipped and configured to assure continuous operation. These data centers shall employ, at a minimum, uninterrupted power supply, redundant backup generators, smoke and heat alarm systems, water sensors, fire suppression systems, air conditioning and humidity controls, and monitoring.

#### **C. Disaster Recovery/Business Continuity**

1. Vendor shall have detailed and documented plans for responding to a disaster, emergency situation, or other unforeseen circumstances that include processes and procedures for resumption of business operations, which shall be tested and reviewed, at least annually.

#### **D. Technical Controls**

##### 1. Access Controls

Vendor shall implement access controls that include the following:

- a) Access that is authorized, unique for each user, authenticated, and assigned with least and minimum necessary privileges, current, and includes inactive time session timeout (at the application level) not to exceed 30 minutes.
- b) Password controls with industry standard password strength and complexity, expiration and history, removal of vendor supplied passwords, and account lockout.
- c) Logical or physical controls to segregate Customer's Data from data from Vendor's other customers.

##### 2. Remote Access

- a) Vendor shall control access from external sources by using password authentication.
- b) Vendor shall follow Customer's remote access procedures when accessing Customer's network. Procedures include but are not limited to the execution of access agreements for each individual requiring access.

##### 3. Network / Security Management

- a) Firewall/router filtering - Vendor shall maintain a network environment that utilizes firewalls to protect all ingress and egress points. Vendor shall house all public or internet facing applications in a DMZ that separates the publicly facing servers from the internal network.
- b) Protection against Malicious Code – Vendor shall implement automated tools to detect, prevent, remove and remedy malicious code on desktops, servers, e-mail and internet access. Servers shall be updated with security patches based on industry accepted standards and criticality. Vendor shall use supported versions of operating systems for which patches are actively deployed.
- c) IDS / IPS – Vendor shall utilize intrusion detection/intrusion prevention (IDS / IPS) systems to monitor activity that occurs across the network, as the parties may agree pursuant to a separate services engagement.
- d) Wireless technology - Vendor shall implement a standard at least as stringent as 802.11i, when utilizing wireless technology to transmit Data or to access systems or Data.

##### 4. System Hardening

- a) Vendor shall implement policies and technical standards to harden operating systems, networks, databases, and web services.

##### 5. Logging

a) Vendor's systems, networks and applications shall maintain audit logs of key events as agreed by the parties (for example, logon attempts, account lockout, account administration and password resets), and retain such logs for 30 days.

b) Vendor shall implement policies and procedures for monitoring security logs on a regular basis.

#### 6. Software Development Life Cycle (SDLC)

a) Vendor shall follow a documented SDLC process that covers software design, development, and improvement. The development/test and production environments shall be physically separated. All development and testing must be performed in a development / test environment. Sensitive production Data shall not be used for testing purposes, unless de-identified.

#### 7. Change Management

a) Vendor shall implement documented change management and problem management processes which require management review and approval. For example, changes to software code shall require management review and approval.

#### 8. Software Security

a) Vendor shall implement secure coding practices, consistent with industry standards, so that software provided or utilized under this Agreement is not vulnerable to known exploits.

### **E. Data Security**

#### 1. Personal Devices

Vendor shall only store or process Data on / in assets owned or leased by Vendor. Except for back-up media, Vendor shall not store Data on storage devices such as flash drives, memory sticks, CDs, or DVDs.

#### 2. Encryption

All Data that is transmitted between Customer and Vendor's data center through a VPN tunnel shall be encrypted. Data that is transmitted via email and support tickets and other means is not encrypted.

### **F. Data Destruction and Retention**

1. Vendor shall implement policies and procedures around the physical destruction or secure deletion of hardcopy and electronic media based on industry accepted standards.

### **G. Incident Response**

1. Vendor shall have a computer security incident response plan that is supported by a cross-functional response and recovery team that are on call 24x7, 365 days a year.

### **H. Audit and Monitoring**

1. Vendor shall supply annual evidence of SSAE16 certification (as available from Vendor's hosting provider) upon Customer's request.

2. Upon reasonable notice to Vendor, Customer shall have the right to review Vendor's processes, controls and results of internal and/or external reviews of processes and controls associated with the contracted service during the term of this Agreement, including immediately at any time after any security incident incurred by Vendor that may impact Data.

## **Transition Services**

Transition Services consists of the following services, as may be ordered by Customer under an Order Document.

**Setup.** Setup services consist of the following deliverables:

- Kickoff meeting to confirm Project Plan and assign resources. Meeting conducted remotely, up to

five hours.

- Provision hardware, install Vendor software, and setup of three cloud environments (one production environment and, on request, up to two non-production environments). Including set up of a maximum of 20 remote printers (additional printers may be added for additional fees) and users, and refresh databases (three per project).
- Provide training to Customer's core project team on Vendor Cloud process and procedures (train the trainer). Training conducted remotely, up to four hours.
- Performance workshops – two remote meetings (pre go-live and post go-live) to determine specific Customer performance requirements and adjusting the environment accordingly.
- Perform unit testing in collaboration with Customer on the test environment and the production environment.
- Provide support for Customer's acceptance testing (maximum 3 person-days).
- Set/verify on-site and off-site backup schedule in collaboration with Customer.
- Post go-live technical support provided by the assigned Cloud On Boarding Specialist, for up to 40 person/hours during the seven calendar days following go-live.

Setup shall be considered complete and accepted upon successful completion of the following:

- Confirmation of connectivity to Cloud environment.
- Confirmation of successful login to the Vendor Applications.

#### **Assumptions and Exclusions to Transition Services:**

- Customer and Vendor shall agree on a Project Plan at the outset of the transition.
- Customer is responsible for overall project management of the project.
- Customer has all required source code to allow for re-compile on Vendor Cloud servers.
- Vendor and Customer will co-develop and agree to the project plan by site prior to engagement.
- Both Customer and Vendor will use all reasonable and good practices related to migrating software including adequate testing and validation, documentation and project status reporting related to costs, migration milestones, etc.
- The Vendor team shall provide support and assistance to the Customer team throughout the Vendor project by performing the above in scope activities.
- Vendor will staff the project appropriately based on the agreed-to project plan and milestones. Should changes in the plan require changes in this staffing, Vendor commits to make the appropriate resources available whenever possible based on approval.
- Customer database has no data integrity issues. Any remedial activities or data cleansing required is the responsibility of the Customer.
- Customer will provide adequate facilities to enable Vendor consultants to perform their work. This includes, at a minimum, working space, meeting rooms, VPN access, phone access and internet access.
- Vendor may perform most activities remotely in order to reduce timeframes and cost.
- Customer shall provide qualified project resources according to the agreed upon resource plan developed during the Planning phase.
- Project teams shall, whenever possible, remain stable for the duration of their migration efforts.
- All decision making shall be done on a timely basis to ensure that key project milestones can be met. Decisions required that are not made within five business days may require a change order.
- Deliverables submitted for sign off but not signed off or returned for correction within five days will be considered approved by Customer.
- The Customer Project Manager shall ensure that the necessary Customer resources are available when needed as defined in project plans and if necessary, shall escalate business issues to the Steering Committee for quick resolution.
- The Vendor Project Manager shall provide support and guidance to the Customer Project Manager throughout the project based on Vendor's experience and expertise in transitions.
- Changes to scope or project timelines will result in agreement from both Vendor and Customer in the

form of a Vendor change order.

- Third-party interfaces and software is considered out of scope.
- Customizations and/or retrofitting of existing customizations are considered out of scope.
- Customer will provide required access to its current Vendor environment and database.
- Customer's current Vendor environment has not been deployed with a split schema.
- Customer will be responsible for all system testing and acceptance, overall project management of Customer activities, and will provide qualified resources to conduct these activities.

## Exclusions and Quoted Requests

The following items are excluded from the scope of this Program Document. This list of excluded items is presented only for clarification and this list does not represent a comprehensive list of all excluded items. Certain of these items may be performed under a separate, chargeable project as may be agreed by the parties.

- Project-related services
- Implementation support for new plant operations (Green field sites, new plant operations, acquisitions, Data Center transitions, etc.)
- Establishing interfaces to internal or third-party applications, and addressing issues caused by such applications.
- On-site support and projects: Integration support between Vendor Enterprise Applications and third-party applications
- On-site training and consulting
- Customizations (functionality or reporting) development or support
- Third-party or home grown application support
- IT support other than what is outlined above in the Cloud Services section
- Code promotions and compiles - Non Standard Vendor Code (Only with Customization Maintenance Agreement)
- Stress testing
- Penetration testing
- Implementation of modules not currently in use, new functionality, or any process improvements/changes
- Data cleansing or fixing of data integrity issues
- Application or business process consulting
- Any required changes to EDI maps, transformations, or EDI e-Commerce
- Form changes
- Changes required due to third-party software
- Retrofits of pre-existing customizations and integration application code
- Third-party product migration

###