Symantec O_3™ Service Description

I. Introduction.

Symantec O_3 service is a cloud-based security platform designed to help protect enterprise cloud applications and cloud infrastructures. Symantec O_3's vision is to combine access control, information protection and compliance control in a single security solution, allowing enterprise customers to extend their internal security policies to public and private cloud services. Symantec O_3 includes Access Control and Compliance Control functionalities:

A. Access Control

Symantec O_3 helps enable strong authentication, single-sign-on and access control across all external SaaS and internal Web applications. The Symantec O_3 Gateway enables enterprises to standardize on a single authentication source and security policy. Corporate user stores such as Microsoft Active Directory, LDAP, and RDBMS databases are supported. The solution also supports strong authentication. Customers can control which cloud applications an employee may access by defining access policies that the service will automatically enforce.

B. Cloud Audits and Compliance

Symantec O_3 Gateway records important security events to create audit trails that can then be fed to a log management and SIEM solution. Event correlation across both internal and external IT resources becomes possible to help provide complete threat visibility and intelligence.

Symantec O_3 has two primary architectural components:

1. Symantec O_3 Intelligence Center

The Symantec O_3 Intelligence Center is a Web-based administration console. IT administrators log into the Symantec O_3 Intelligence Center to define authentication and access policies for their end users (employees or external users). This console is a multi-tenant SaaS application hosted by Symantec inside Symantec's own secure network infrastructure.

2. Symantec O_3 Gateway

The Symantec O_3 Gateway is a virtual software appliance. Once deployed, it is responsible for enforcing the policies defined by the customer in the O_3 Intelligence Center. End users log into the Gateway, through a Web application running on the Gateway called Symantec O_3 Web portal, to connect to SaaS and intranet Web applications. Once the user is successfully authenticated to the portal, the portal will display a list of SaaS and intranet Web applications the user is authorized to access, based on previously-defined policies. When the user attempts access to one of the authorized applications, the Gateway will connect to the application on the user's behalf, thus providing a single-sign-on service for the user. In the meantime, the Gateway will act as a policy enforcement point that controls access between the users and the SaaS applications based on policies defined by the enterprise customer within the Intelligence Center.

Customers may choose to host the Gateway virtual appliance, or alternatively, they may choose to have the virtual Gateways hosted by Symantec. In either case, Symantec will provide management services (as described in section II.A.iii below) for these virtual appliances once they are deployed.

Authentication at the Web portal is achieved through integration between the Gateway and the customer's existing user store such as their LDAP, AD, or RDBMS. Additionally, the Symantec O_3 Web portal can support external Identity Providers (IdPs) via SAML, OpenID, and Integrated Windows Authentication (IWA).

Integration between the Gateway and SaaS and intranet Web applications is accomplished with a suite of Application Connectors included with the Symantec O_3 service. These connectors enable application-specific integration from the Gateway to the application. The service also includes an Application Connector Wizard, which uses heuristics technology to attempt integration with an application not initially supported by Symantec. Symantec also offers professional services to help customers integrate the Symantec O_3 service with their custom applications.

Synchronization of security policies between the O_3 Intelligence Center and the O_3 Gateway is achieved through a permanent VPN network connection from the Gateway to the O_3 Intelligence Center to enable defined policies and their updates to be published to the Gateway.

II. Symantec O_3 Service Roles and Responsibilities.

A. Symantec as the Managed Service Provider: Symantec, as the service provider, hosts the O_3 Intelligence Center and operates the infrastructure that runs the Intelligence Center for all Symantec O_3 customers. In this role, Symantec provides the following services:

i. Operate the Intelligence Center

The Symantec O_3 Intelligence Center is a multi-tenant Web-based application that enables customers to define access policies to SaaS and intranet Web applications for their users. It is also the application where customers can configure their specific instances of O_3 Gateways. Symantec will host this application and run the infrastructure behind the application from Symantec's data center.

ii. Host the Symantec O_3 Gateway (optional)

The Symantec O_3 Gateway is a virtual software appliance responsible for enforcing application access policies defined by the customer in the Intelligence Center. Symantec will provide hosting services for the O_3 Gateway if customers choose for Symantec to do so.

iii. Manage all O_3 Gateways

Regardless of whether the customer hosts its own O_3 Gateway or opts to have Symantec host the Gateway, Symantec will provide the following management services for the O_3 Gateway virtual appliance: monitoring of the appliance's connectivity to the Intelligence Center, and the appliance's general health.

iv. Operate the Symantec Validation and ID Protection (VIP) Service (optional)

Symantec O_3 may include integration with the Symantec VIP Service that delivers cloud-based strong authentication that combines something you know (*e.g.*, a username and password) with something you have (a credential such as a card, token, or mobile phone). VIP helps to protect networks, applications, and data against unauthorized access as part of a comprehensive information protection program.

B. The Enterprise Customer, as recipient of the Symantec O_3 Service: An enterprise customer means any entity that has purchased the Symantec O_3 service. For each customer, two types of employees are significant to the deployment of Symantec O_3-IT administrators and end users.

i. IT Administrators

A customer's IT administrators access the O_3 Intelligence Center to define employee access policies to SaaS and internal Web applications. The IT administrators will also use the Intelligence Center to configure the customer's O_3 Gateways.

ii. End Users

Users are individuals that the enterprise customer has granted access to the Symantec O_3 Web portal that runs on the O_3 Gateway. Users rely on the O_3 Web portal to log into SaaS and intranet Web applications.

C. SaaS Application Provider: SaaS application providers are third parties that provide SaaS application services to the customer, where the customer wishes to use the Symantec O_3 service to manage and control access to such SaaS application by its users.

D. Third-Party Identity Provider: Third-party identity providers, at customer's option, may provide authentication services to the customer through the O_3 Web portal. Normally, the O_3 Gateway delegates authentication to the customer's own user store, such as the customer's own Active Directory, LDAP, or RDBMS. However, customers may elect to use an external identity provider to authenticate users to the O_3 Web portal, which supports such an option.

E. Third-Party Cloud Platform Provider: Customers may utilize third-party cloud platform providers to host the O_3 Gateway using the provider's infrastructure service.

III. Symantec O_3 Service Components.

Service components for Symantec O_3 include:

i. Symantec O_3 Intelligence Center: As described in section I above.

ii. Symantec O_3 Gateway: As described in section I above.

iii. Symantec O_3 Pre-production Instance (Optional): The optional pre-production instance provides customers an instance of the Symantec O_3 service on Symantec's pre-production network for testing purposes. Customers can leverage the pre-production instance to stage new deployment to a limited set of users, assess the stability

of the new development before rolling out to the rest of their user base. For the pre-production instance, Symantec will host the O_3 Intelligence Center and the O_3 Gateway; customers may not host the pre-production instance themselves nor utilize third-party providers.

iv. Managed DNS Provider (Optional): If a customer chooses for Symantec to host its O_3 Gateway, Symantec will assign DNS names to the O_3 Gateways. Symantec will also by default provide a managed DNS service for these domain names and issue SSL digital certificates for use with such domains.

v. Symantec VIP Service : As described in Section II above. Symantec O_3 may include a limited-use subscription to the Symantec VIP Service so Symantec O_3 customers may use VIP to add strong authentication to web based applications accessed through the Symantec O_3 Gateway. Use of Symantec VIP outside of the Symantec O_3 Gateway requires a full subscription to the Symantec VIP Service.

IV. Symantec O_3 Software Components.

Software components for Symantec O_3 include:

i. Customer-hosted O_3 Gateway (Optional): A customer has the option to host its own O_3 Gateway virtual appliance. In this case, Customer deploys the virtual appliance either in its own corporate data center, or with a third-party cloud platform provider. Symantec will make O_3 Gateway appliances available in the following formats:

- VMWare Virtual Image
- KVM Virtual Image
- Amazon Machine Image (AMI)

ii. Symantec O_3 Identity Link (Optional): The Symantec O_3 Identity Link is an optional software package used to enable connectivity across network firewalls between the O_3 Gateway and a customer's user store such as AD/LDAP. If needed, a customer may download this software from the O_3 Intelligence Center and install it within their corporate network.

iii. Symantec O_3 IWA Connector (Optional): The Symantec O_3 IWA Connector is an optional software package used to enable Integrated Windows Authentication (IWA) to the O_3 Web portal. IWA enables a customer's user, who has already logged into their corporate Windows machine, to access the O_3 Web portal without being challenged to enter their user name and password again. If needed, the customer may download the IWA Connector and install it within their corporate network.

iv. Symantec O_3 Keychain Tool (Optional): The Symantec O_3 Keychain Tool is an optional Java software program that enables a customer's IT administrator to bulk-upload user credentials for a SaaS application. This functionality is useful if the IT administrator does not want users to access a SaaS application using their own usernames and passwords.

v. APIs (Optional): The Symantec O_3 service makes available the following APIs to help enable customers to further customize their deployment:

- The O_3 Custom Portal API enables customers to create a custom Web portal for their users to access SaaS and internal Web applications. This API may be used to customize the look and feel of the Web portal, or enhance the authentication mechanism at the portal such as adding risk-based authentication.
- The O_3 Web Services User Store API enables customers to delegate authentication at the O_3 Web portal to any user store that conforms to this API, beyond the currently-supported LDAP/AD and RDMS-based user stores.
- The O_3 Gateway API is a REST-based Web services interface that can be used to manage an O_3 Gateway. The interface provides access to O_3 Gateway configuration data, including applications, user stores, identity providers and authorization rules. The O_3 Gateway API also supports the ability to query and manage runtime information, including sessions, users, and user profiles.

vi. Documentation: Symantec will make available online relevant service documentation as they become available.

V. Symantec O_3 Audit Trails.

In the Symantec O_3 Gateway, user authentication events occurring through the O_3 Web portal are logged, as are user access to SaaS and intranet Web applications. Such logs are stored in the Gateway in flat-file format that can be rotated with a configurable rotation policy. The logs can also be pushed to a network-based syslog server, Amazon S3 service, or Secure FTP site. Customer shall archive the logs according to its requirements and internal policies.

VI. Symantec O_3 Service Updates.

i. Service Software Updates: As new versions of the O_3 service software are made generally available (GA), Symantec will announce to its customer base the GA date, and will deploy the new version on the pre-production service first. After successful roll-out on the pre-production service, Symantec will leverage the next scheduled maintenance window to update the new version on its production environment. Symantec will give customers advance notice via email of the date and nature of such update, which will include updates to both the O_3 Intelligence Center, as well as to the Symantec-managed O_3 Gateways. For customer-hosted Gateways, customers will have the ability to manually set a configuration attribute in the O_3 Intelligence Center to delay such update for their deployment for no longer than two maintenance cycles.

ii. Application Connector Updates: From time to time, new Application Connectors or updates to existing Application Connectors will be developed and made available to customers. Such updates are automatically deployed to each customer's O_3 Gateways within 24 hours of GA.

iii. Pre-production Service: Software updates will be deployed automatically to the pre-production service within one week of GA.

VII. Symantec O_3 Technical Support Services.

i. Purchase of the Symantec O_3 service includes Symantec technical support as described in the certificate confirming customer's purchase of the O_3 service. Symantec technical support is provided and performed subject to Symantec's then-current terms, policies and processes ("Support Terms"). All references to "Software" in the Support Terms shall be deemed references to the O_3 service, as applicable, provided, however, that any terms or deliverables in the Support Terms specific to software only shall not apply to support for the Symantec O_3 service.

ii. Customer's technical assistance may be limited if customer is using or working on an application that is not identified by Symantec as a "supported application" or if customer is using an implementation of Symantec O_3 service that was not installed or configured using Symantec processes.

iii. Symantec Technical Support personnel may need to access customer's O_3 Intelligence Center and Gateway using a Symantec-managed account, to examine customer's O_3 deployment configurations in order to fulfill their support obligations.

VIII. Symantec O_3 Service Performance SLA.

Purchase of the Symantec O_3 service includes the following service performance commitments:

i. Service Availability definitions:

a. *Up Time Measurement*: Up Time is calculated on a rolling 90-day basis as a percentage equal to (a) the total number of minutes in any such 90-day period that Symantec's systems are available and capable of receiving and processing data from customers, divided by (b) the total number of minutes in such period.

b. *Up Time Percentage*: Symantec's Up Time percentage through such 90-day period shall be no less than 99.5%.

ii. Symantec commits to make the log-in pages for both the Symantec-hosted O_3 Intelligence Center and O_3 Gateway accessible to customers pursuant to the Service Availability level set forth above, subject to the exceptions below.

iii. Exceptions: For purposes of calculating the Service Availability, the services shall not be considered unavailable, even if it is not actually accessible to an individual user, if due to: (i) downtime during regular maintenance windows published by Symantec; (ii) downtime during non-regular maintenance windows that are communicated to customers in writing (including by email) at least seventy-two hours in advance; (iii) acts or omissions of customer or third parties, including but not limited to individual applications and application adapters; (iv) customer's internet connectivity; (v) internet traffic problems not under Symantec's reasonable control; (vi) customer's failure to meet minimum hardware and/or software requirements set forth in the agreement, if any; (vii) customer's infrastructure or other equipment; (viii) any hardware, software, service or other equipment used by an individual user to access the services; or (ix) failure of services provided by customer (or a third party under contract to provide services to customer) that are incorporated into the O_3 Services in the absence of any fault attributable to Symantec.

The service performance commitment set forth above shall not apply to pre-production environments.

IX. Symantec O_3 Deployment.

A. Delivery Details

1. Scope of Deployment. Any Symantec O_3 deployment tasks ("Deployment") not specifically written below are out of scope. Symantec will provide a one-time standard setup of a Symantec O_3 deployment, using one of four architectures defined in Appendices A, B, C and D below (each, a "Standard Implementation"). The deployment will be divided into 5 phases as described below.

Phase 1 – Information Gathering

This phase will begin with Symantec sending Customer the Symantec O_3 Deployment Questionnaires. The questionnaires explain the requirements of Customer's network and applications, information needed to configure the Symantec O_3 service, and provides details on how to gather the information to fill out the questionnaires. The completed questionnaires are required to prepare for a successful Symantec O_3 deployment.

Symantec Responsibilities:	Provide Deployment Questionnaires. Assist customer and answer questions in completing the questionnaires.
Customer Responsibilities:	Complete and return Deployment Questionnaires.
Deliverable:	This phase is complete when the completed questionnaires are returned to Symantec.

Phase 2 – Pre-Deployment

With information provided in the Deployment Questionnaires Symantec will generate a network solution diagram. Once complete, a joint review with Symantec and Customer will be conducted.

Customer will then begin the execution of these requirements, including firewall rules, IP assignment, and DNS creation.

Symantec Responsibilities:	Create network architecture diagram. Assist customer and answer questions while customer configures environment.
Customer Responsibilities:	Begin configuration of network infrastructure: IP assignment, DNS entries, and firewall rules.
Deliverable:	Both parties agree to solution diagram.

Phase 3 – Deployment

Once the solution diagram is agreed to, the O_3 gateway will be prepared for deployment. This includes completing the Virtual Machine (VM) environment preparation and deploying the VM image either at Symantec, on Customer premises or in EC2. Symantec and Customer will work together to conduct any troubleshooting.

Symantec Responsibilities:	Symantec will make the virtual appliance available. Troubleshoot connection to O_3 Intelligence Center Servers
Customer Responsibilities:	Deploy and setup the virtual appliance. Assist in troubleshooting connection to O_3 Intelligence Center Servers.
Deliverable:	This phase completes when the O_3 gateway is connected to the O_3 Intelligence Center servers.

Phase 4 – Configuration & Testing

Now that the O_3 gateway is connected to the Symantec O_3 Intelligence Center, it is ready for the Customer-specific configuration tasks. Symantec will work with Customer to connect the O_3 gateway to the Customer user store and Customer application.

Symantec Responsibilities:	Configure connection to user store and application. Make changes in O_3 Intelligence Center. Assist customer with infrastructure changes required. Lead troubleshooting.
Customer Responsibilities:	Provide infrastructure. Provide information for and contribute to troubleshooting.
Deliverable:	A user from the user store, on a supported platform, can create a session on O_3 gateway and gain access to the agreed upon protected application.

Phase 5 – Knowledge Transfer Hand-off

The final phase is knowledge transfer by Symantec. Administration of the environment in the O_3 Intelligence Center and details on specifics of the Customer environment will be transferred to designated Customer administrator(s). Customer administrator(s) will be instructed on the support request process – web ticket system, email, and phone.

Symantec Responsibilities:	Provide technical training and information on how to access support.
Customer Responsibilities:	All Customer administrators attend training.
Deliverable:	Customer administrator can make simple changes, knows how to request support. Customer signs off on the Project Completion Form

2. Key Dependencies Pre-requisites, assumptions, or dependencies for the Deployment are as follows:

It is agreed that Symantec will:

- Designate a single point of contact as Symantec Project Manager;
- Manage the project with implementation methodology outlined above and supporting documentation;
- Provide timely and knowledgeable support through single point of contact for duration of implementation.

It is agreed that Customer will:

- Designate a single point of contact to act as Customer Project Manager;
- Provide the technical environment including appropriate VM infrastructure, if required;
- Provide all required resources in a timely manner to support Symantec's implementation efforts;
- Promptly advise Symantec of any issues or concerns as project progresses.

Symantec used the following assumptions during development of this Deployment plan. Any changes to these assumptions may affect the price and schedule commitments.

- Customer will provide Symantec access to the business, customer, and technical information and facilities necessary to execute the solution.
- Customer will ensure that appropriate personnel are available to meet with Symantec, as necessary.
- During this effort, Symantec will not be responsible for negotiations with hardware, software, or other vendors, or any other contractual relationship between the Customer and third parties. Symantec, at the request of Customer, will provide input to the Customer regarding optimal product or vendor selection.
- Symantec team members will engage in a knowledge transfer exercise as part of this effort relative to Symantec services, product functionality, similar installations, and techniques.
- Symantec will develop any application code, documentation, and presentations in English.

3. Location and Period of Performance: The Deployment will be performed remotely from a Symantec facility. The period of performance hereunder will commence and end upon mutually agreed upon dates, provided that any Deployment shall be delivered within the twelve (12) months following the effective date of the Symantec O_3 order.

4. Acceptance: Customer will accept or reject the Deployment in writing within five (5) business days from receipt thereof. Acceptance will be based upon completion of the Deployment in accordance with the criteria set forth in this Deployment plan. If Customer does not accept or reject in writing as set forth above, the Deployment will be considered to be accepted by Customer. Customer will clearly state in writing reasons for rejection, if any. Within five (5) business days of any notice of rejection, Symantec will present a corrective plan of action to Customer. Symantec will then make the corrections (and Customer will permit Symantec to make such corrections) and, where applicable, Symantec will re-request for acceptance of the Deployment.

B. Delivery Terms

1. Customer's Responsibilities : Customer agrees to do the following, as applicable, to ensure the successful completion of the Deployment:

   a. Identify a Customer project manager ("Project Manager") to support execution of the Deployment. Customer's Project Manager will: (i) staff and manage Customer personnel to support the project and enforce change control process; (ii) provide Symantec with access, equipment, and other resources needed to support the Deployment; (iii) act as the focal point for resolution of project related issues; (iv) participate in scheduled status checkpoint meetings, and (v) sign the Service Acknowledgement Form, if required.
   b. Identify a Customer project executive ("Project Executive") who has the authority to make decisions for Customer regarding change orders, budget, scope, resources and other project related issues if they cannot be resolved by Customer's Project Manager.
   c. Assign an appropriate number of suitably skilled personnel to work with Symantec, and such personnel shall use reasonable efforts to assist and cooperate with Symantec consistent with the Deployment described herein.
   d. Ensure the applicable systems and personnel (including any applicable executive or project resources) are available and Customer is prepared to receive Deployment-related deliverables on the mutually agreed upon Deployment start date. In the event that Customer is unable or unwilling to allow the Deployment to begin on the mutually agreed upon start date, and Symantec has incurred any portion of the Deployment-related fees in anticipation of commencement, then Customer agrees to pay to Symantec the reasonably incurred fees, constituting no more than the amount equal for the lost time constituting the delay.
   e. Ensure that it has backed up all systems and performed any required maintenance prior to commencement of the Deployment. This shall include, without limitation: (i) servers; (ii) networks; (iii) storage; (iv) power; (v) lighting; (vi) air-conditioning/heating.
   f. Provide licensed copies in the required versions of all software products, including Symantec O_3 software components, to be installed, implemented or used. Payment for license, use and operation of all such software products is the sole responsibility of Customer.
   g. Ensure that the operating systems of all appropriate servers and computers will be at a level supported by the Symantec software products to be used. Customer will ensure that; (i) the storage configuration is a formally qualified configuration for the Symantec O_3 software components to be used, if any; (ii) the technical environment, including the application and database environments, will be kept under change control; and (iii) third parties such as Internet Service Providers have been made aware of any applicable testing that might be carried out by Symantec.

2. Change Order(s): Customer and Symantec may modify the Deployment in accordance with Symantec's standard change order form. Requests for any services not included in the Scope, above, require a separate SOW with fees based on then-current Symantec rates at the time of purchase.

3. Staffing: Symantec reserves the right to assign any suitable skilled resource(s) available during the mutually agreed upon dates of the Deployment. Symantec is not obligated to provide a specific Symantec resource or third party resource for the Deployment. To the extent the applicable agreement governing the Deployment requires written approval by the parties to use third parties in the performance of the Deployment, the parties agree that such approval is hereby provided.

APPENDIX A: Customer-Hosted O_3 gateway on-premise

This section describes the scope of Symantec O_3 Standard Implementation for a Customer-Hosted O_3 gateway within Customer's network as illustrated in Figure A below.

This Standard Implementation includes the successful deployment of One (1) Symantec O_3 gateway virtual appliance (A), located within the Customer's network infrastructure, connected to the Symantec O_3 Intelligence Center (B).

The gateway will be connected to a Customer-designated user store (C), and will be configured to protect up to Five (5) customer-designated applications (D) selected by Customer during the Deployment from the then-current supported application list maintained by Symantec.

The successful completion of the Standard Implementation is described in the "Deliverable" section of Section B, Phase 4 of this document.

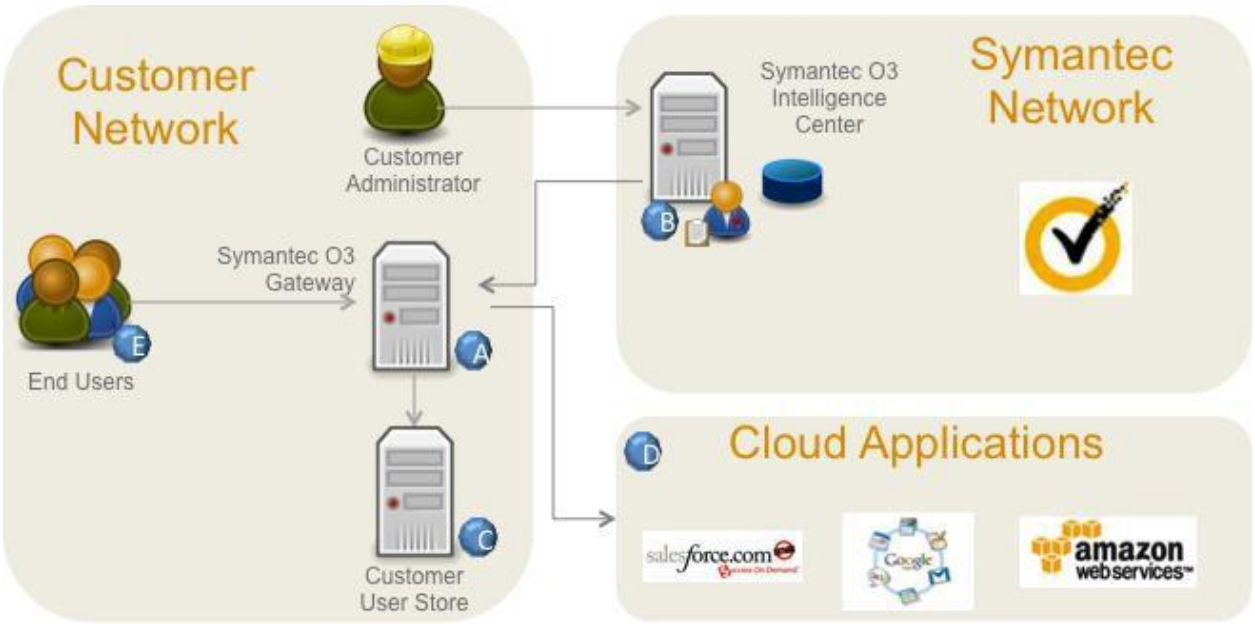

Figure A

APPENDIX B: Customer-Hosted O_3 gateway, Amazon EC2

This section describes the scope of Symantec O_3 Standard Implementation for a Customer-Hosted O_3 gateway within the Amazon EC2 environment, as illustrated in Figure B below.

This Standard Implementation includes the successful deployment of One (1) Symantec O_3 gateway virtual appliance (A), located in Amazon EC2 environment, connected to the Symantec O_3 Intelligence Center (B).

The gateway will be connected to a Customer-designated user store (C), optionally through an network tunnel created by Symantec O_3 Identity Link (F) software, and will be configured to protect up to Five (5) customer-designated applications (D) selected by Customer during the Deployment from the then-current supported application list maintained by Symantec.

Upon successful completion of the Standard Implementation, an end user (E) from the Customer-designated user store (C) can create a session on the O_3 gateway (A), and gain access to the Customer-designated applications (D), as described in the Service Description above.

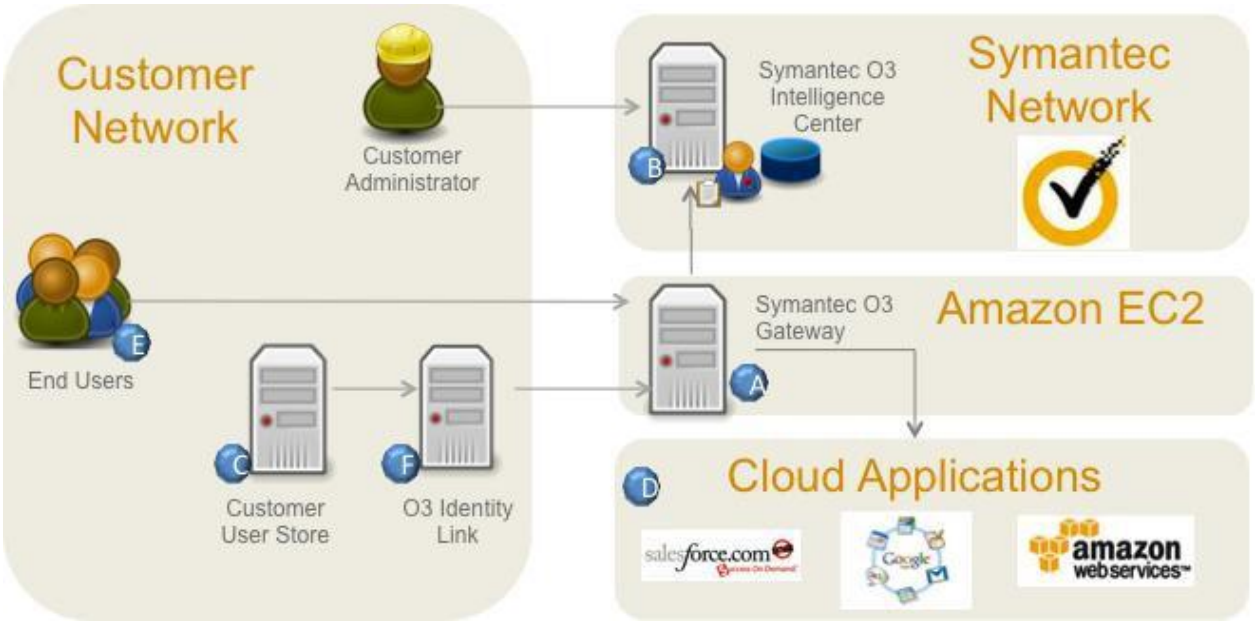

Figure B

APPENDIX C: Symantec-Hosted O_3 gateway

This section describes the scope of Symantec O_3 Standard Implementation for a Symantec-Hosted O_3 gateway within the Symantec network environment, as illustrated in Figure C below.

This Standard Implementation includes the successful deployment of One (1) Symantec O_3 gateway virtual appliance (A), located in Symantec network environment, connected to the Symantec O_3 Intelligence Center (B).

The gateway will be connected to a Customer-designated user store (C), optionally through a network tunnel created by Symantec O_3 Identity Link (F) software, and will be configured to protect up to Five (5) customer-designated applications (D) selected by Customer during the Deployment from the then-current supported application list maintained by Symantec.

Upon successful completion of the Standard Implementation, an end user (E) from the Customer-designated user store (C) can create a session on the O_3 gateway (A), and gain access to the Customer-designated applications (D), as described in the Service Description above.

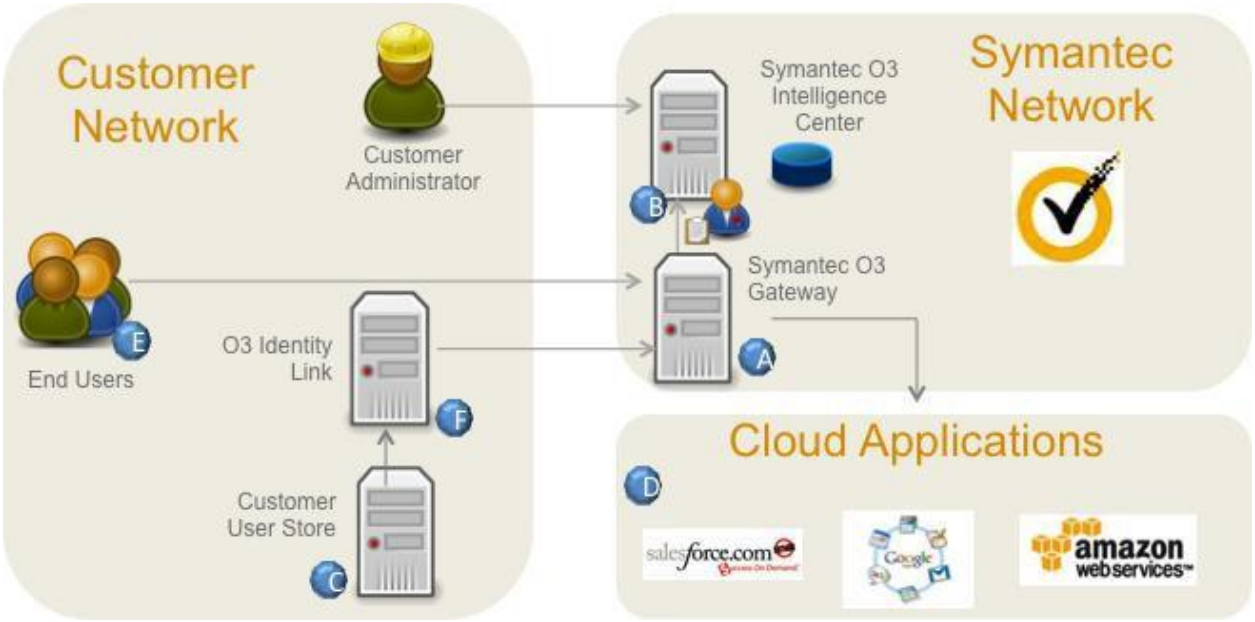

Figure C

APPENDIX D: Symantec-Hosted O_3 gateway (SFDC)

This section describes the scope of Symantec O_3 Standard Implementation for a Symantec-Hosted O_3 gateway within the Symantec network environment, using SalesForce as the user store, as illustrated in Figure D below.

This Standard Implementation includes the successful deployment of One (1) Symantec O_3 gateway virtual appliance (A), located in Symantec network environment, connected to the Symantec O_3 Intelligence Center (B).

The gateway will be connected to the SalesForce user store (C), and will be configured to protect up to Five (5) customer-designated applications (D) selected by Customer during the Deployment from the then-current supported application list maintained by Symantec.

Upon successful completion of the Standard Implementation, an end user (E) from the SalesForce user store (C) can create a session on the O_3 gateway (A), and gain access to the Customer-designated applications (D), as described in the Service Description above.

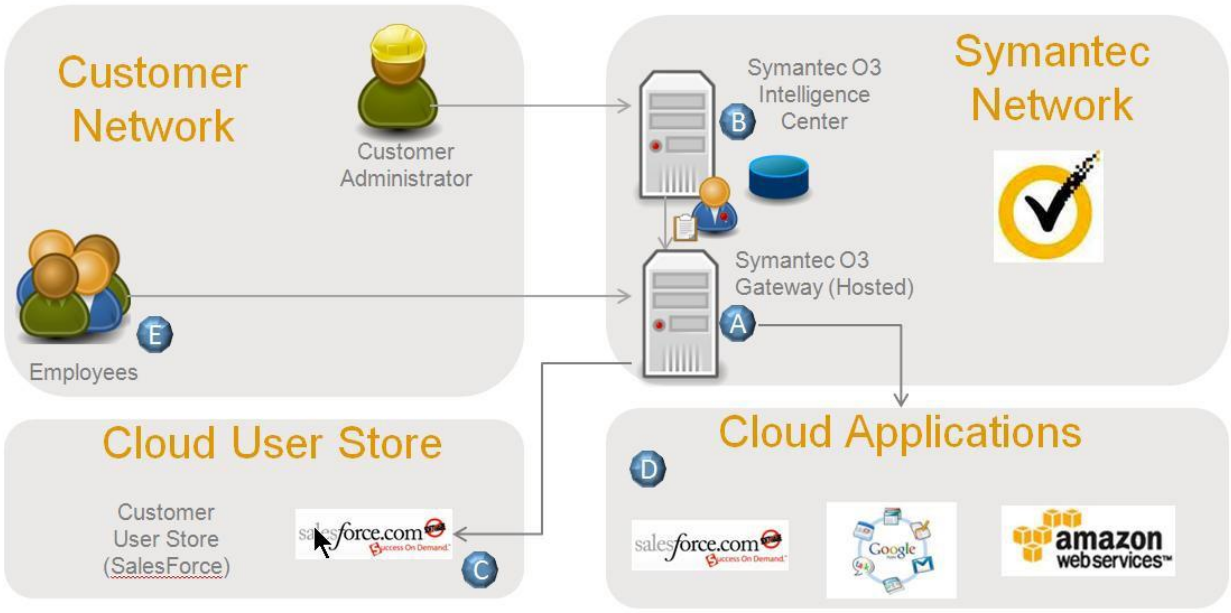

Figure D

SYMANTEC O_3 SERVICE TERMS AND CONDITIONS

1. DEFINITIONS

"Agreement" means the Master Services Agreement or such other agreement entered into between Symantec and Customer under which the order document applicable to this Service Description is issued.

"Customer" means the entity that purchased the O_3 Service, including any agents and/or contractors it authorizes to install and use the service on its behalf.

"Gateway" means O_3 Gateway in the form of a virtual software appliance installed on a virtual machine for use by Customer as part of the Service.

"Services" means the Symantec O_3 solution described in an order document provisioned by Symantec to Customer under the Agreement.

"Software" means, collectively, the O_3 Service software and any Gateway software made available to Customer by Symantec for use in conjunction with the Services.

"Users" means Customer's employees, contractors and external users who are authorized by Customer to use the Services on behalf of Customer.

2. OBLIGATIONS

(a) Service Provisioning. Following completion of the requisite installation, Symantec shall provide Customer with the Services specified in this Service Description in accordance with these terms and conditions throughout the Term of the service.

(b) Symantec O_3 for Salesforce.com. If Customer selects "Symantec-Hosted O_3 gateway (SFDC)" (Appendix D) to rely on user authentication data from salesforce.com (e.g., through Customer's existing Salesforce.com CRM implementation), then the "SFDC Service Agreement" (Exhibit A) shall be incorporated by reference into the Agreement.

(c) Log Data. Customer shall be responsible for all activities that occur under its Gateway User accounts including, but not limited to, implementing the configuration options in line with Customer's internal policies, safeguarding the Software and accompanying systems to protect against unauthorized access to the Service, and retaining any data and/or event logs generated by the Service.

(d) Customer's IT Contractor. Customer may make the Software and the Service accessible to its authorized IT contractors, provided that Customer shall be responsible for such third party's compliance with the terms and conditions of this Agreement, and any breach thereof by such third party shall be deemed to be a breach by Customer.

3. ADDITIONAL TERMS

(a) Privacy. CUSTOMER ACKNOWLEDGES AND AGREES THAT PART OR ALL OF THE SERVICE MAY BE PERFORMED IN THE UNITED STATES OF AMERICA AND/OR IN OTHER JURISDICTIONS WHERE SYMANTEC MAINTAINS A PRESENCE. CUSTOMER IS RESPONSIBLE FOR OBTAINING ALL CONSENTS AND APPROVALS REQUIRED, IF ANY, TO EFFECT THE TRANSFER OF USER DATA OUTSIDE THE UNITED STATES, THE EUROPEAN UNION, AND/OR OTHER COUNTRIES. CUSTOMER FURTHER ACKNOWLEDGES AND AGREES THAT SYMANTEC SHALL NOT BE LIABLE TO CUSTOMER FOR BREACH OF ANY APPLICABLE LEGISLATION OR REGULATION ASSOCIATED WITH SUCH USER DATA TRANSFER.

(b) U.S. Government End Users. If Customer is a branch or agency of the United States Government, the following provision applies. The Service and accompanying Software are comprised of commercial computer software and commercial computer software documentation as such terms are used in 48 C.F.R. 12.212 and are provided to the Government (a) for acquisition by or on behalf of civilian agencies, consistent with the policy set forth in 48 C.F.R. 12.212 or (b) for acquisition by or on behalf of units of the Department of Defense, consistent with the policies set forth in 48 C.F.R. 227.7202-1 and 227.7202-3.

(c) Symantec Validation & ID Protection (VIP) Service. Customer's use of strong authentication that may be included in O_3 Service ("VIP Service"), as further described in this O_3 Service Description, is subject to the following terms and conditions:

(1) the "*VIP Service Description*" published at the following link shall be incorporated by reference into the Agreement to govern the VIP Service: http://www.verisign.com/repository/service_description;

(2) *Symantec O_3 Technical Support Services* and *Symantec O_3 Service Performance SLA* as described herein will be the only technical support services and performance SLA that apply to such VIP Service; and

(3) such VIP Service shall be used only in combination with O_3 Service, and Customer may not use the VIP Service on a stand-alone basis or use or integrate it with any other software or service unless otherwise subscribed to by the customer.

EXHIBIT A - SFDC Service Agreement

"**AppExchange**" means the online directory of on-demand applications that work with the Service, located at http://www.appexchange.com or at any successor websites.

"Org" means a separate set of Your Data and SFDC product customizations held by SFDC in a logically separated database (i.e., a database segregated through password-controlled access).

"**Platform**" means the online, Web-based platform service provided by SFDC to Reseller in connection with Reseller's provision of the Reseller Application to You.

"**Reseller**" means Symantec.

"**Reseller Application**" means Symantec O_3 for Salesforce.

"**SFDC Service**" or "**Service**" means the online, Web-based application and platform service generally made available to the public via http://www.salesforce.com and/or other designated websites, including associated offline components but excluding Third-Party Applications.

"**SFDC**" means salesforce.com.

"**Third-Party Applications**" means online, Web-based applications and offline software products that are provided by third parties, interoperate with the Service, and are identified as third-party applications, including but not limited to those listed on the AppExchange.

"**Users**" means Your employees, representatives, consultants, contractors or agents who are authorized to use the Service subject to the terms of this SFDC Service Agreement as a result of a subscription to the Reseller Application having been purchased for such User, and have been supplied user identifications and passwords by You (or by SFDC or Reseller at Your request).

"**You**" and "**Your**" means the customer entity which has contracted to purchase subscriptions to use the Reseller Application subject to the conditions of this SFDC Service Agreement, together with any other terms required by Reseller.

"**Your Data**" means all electronic data or information submitted by You as and to the extent it resides in the Service.

1. Use of Service.

(a) Each User subscription to the Reseller Application shall entitle one User to use the Platform via the Reseller Application, subject to the terms of this SFDC Service Agreement, together with any other terms required by Reseller. User subscriptions cannot be shared or used by more than one User (but may be reassigned from time to time to new Users who are replacing former Users who have terminated employment with You or otherwise changed job status or function and no longer require use of the Platform). For clarity, Your subscription to use the Platform hereunder does not include a subscription to use the SFDC Service generally or to use it in connection with applications other than the Reseller Application or combined solutions or ISVForce solutions provided by other SFDC resellers. If You wish to use the SFDC Service or any of its functionalities or services other than those included in the Reseller Application, or to create or use additional custom objects beyond those which appear in the Reseller Application in the form that it has been provided to You by Your Reseller, visit www.salesforce.com to contract directly with SFDC for such services. In the event Your access to the Reseller Application provides You with access to the SFDC Service generally or access to any Platform or SFDC Service functionality within it that is in excess to the functionality described in the Reseller Application's user guide, and You have not separately subscribed under a written contract with SFDC for such access, then You agree to not access and use such functionality, and You agree that Your use of such

functionality, or Your creation or use of additional custom objects in the Reseller Application beyond that which appears in the Reseller Application in the form that it has been provided to You by your Reseller, would be a material breach of this Agreement.
For clarity, and without limiting any of the foregoing, Your subscription to the Platform does not include any features and functionalities in excess of, and You shall not use any functionality in connection with Your subscription to the Platform in excess of, the following SFDC features and functionality: (i) Web Services API to create, manage and authenticate Users; (ii) My Domains; (iii) SAML (i.e. Single Sign On); (iv) Identity Provider; (v) Chatter; (vi) Oauth; and (vii) features and functionalities contained in SFDC-released updates to the features and functionalities listed in (i) through (vi).

(b) Notwithstanding any access You may have to the Platform or the SFDC Service via the Reseller Application, Reseller is the sole provider of the Reseller Application and You are entering into a contractual relationship solely with Reseller. In the event that Reseller ceases operations or otherwise ceases or fails to provide the Reseller Application, SFDC has no obligation to provide the Reseller Application or to refund You any fees paid by You to Reseller.

(c) You (i) are responsible for all activities occurring under Your User accounts; (ii) are responsible for the content of all Your Data; (iii) shall use commercially reasonable efforts to prevent unauthorized access to, or use of, the Platform and the SFDC Service, and shall notify Reseller or SFDC promptly of any such unauthorized use You become aware of; and (iv) shall comply with all applicable local, state, federal and foreign laws and regulations in using the Platform and the SFDC Service.

(d) You shall use the Platform and the SFDC Service solely for Your internal business purposes and shall not: (i) license, sublicense, sell, resell, rent, lease, transfer, assign, distribute, time share or otherwise commercially exploit or make the Platform or the SFDC Service available to any third party, other than to Users or as otherwise contemplated by this SFDC Service Agreement; (ii) send spam or otherwise duplicative or unsolicited messages in violation of applicable laws; (iii) send or store infringing, obscene, threatening, libelous, or otherwise unlawful or tortuous material, including material that is harmful to children or violates third party privacy rights; (iv) send or store viruses, worms, time bombs, Trojan horses and other harmful or malicious code, files, scripts, agents or programs; (v) interfere with or disrupt the integrity or performance of the Platform or the SFDC Service or the data contained therein; or (vi) attempt to gain unauthorized access to the Platform or the SFDC Service or its related systems or networks.

(e) You shall not (i) modify, copy or create derivative works based on the Platform or the SFDC Service; (ii) frame or mirror any content forming part of the Platform or the SFDC Service, other than on Your own intranets or otherwise for Your own internal business purposes; (iii) reverse engineer the Platform or the SFDC Service; or (iv) access the Platform or the SFDC Service in order to (A) build a competitive product or service, or (B) copy any ideas, features, functions or graphics of the Platform or the SFDC Service.

2. **Third-Party Providers.** Reseller and other third-party providers, some of which may be listed on pages within SFDC's website and including providers of Third-Party Applications, offer products and services related to the Platform, the SFDC Service, and/or the Reseller Application, including implementation, customization and other consulting services related to customers' use of the Platform and/or the SFDC Service, and applications (both offline and online) that interoperate with the Platform, SFDC Service, and/or the Reseller Application, such as by exchanging data with the Platform, the SFDC Service, and/or the Reseller Application, or by offering additional functionality within the user interface of the Platform, the SFDC Service, and/or the Reseller Application through use of the Platform and/or SFDC Service's application programming interface. SFDC does not warrant any such third-party providers or any of their products or services, including but not limited to the Reseller Application or any other product or service of Reseller, whether or not such products or services are designated by SFDC as "certified," "validated" or otherwise. Any exchange of data or other interaction between You and a third-party provider, including but not limited to the Reseller Application, and any purchase by You of any product or service offered by

such third-party provider, including but not limited to the Reseller Application, is solely between You and such third-party provider. In addition, from time to time, certain additional functionality (not defined as part of the Platform or SFDC Service) may be offered by SFDC or Reseller to You, for an additional fee, on a pass-through or OEM basis pursuant to terms specified by the licensor and agreed to by You in connection with a separate purchase by You of such additional functionality. Your use of any such additional functionality shall be governed by such terms, which shall prevail in the event of any inconsistency with the terms of this SFDC Service Agreement.

3. **Integration with Third-Party Applications.** If You install or enable Third-Party Applications for use with the Platform or SFDC Service, You acknowledge that SFDC may allow providers of those Third-Party Applications to access Your Data as required for the interoperation of such Third Party Applications with the Platform or SFDC Service. SFDC shall not be responsible for any disclosure, modification or deletion of Your Data resulting from any such access by Third-Party Application providers. In addition, the Platform and SFDC Service may contain features designed to interoperate with Third-Party Applications (e.g., Google, Facebook or Twitter applications). To use such features, You may be required to obtain access to such Third-Party Applications from their providers. If the provider of any such Third-Party Application ceases to make the Third-Party Application available for interoperation with the corresponding Platform or SFDC Service features on reasonable terms, SFDC may cease providing such Platform or SFDC Service features without entitling You to any refund, credit, or other compensation.

4. **Proprietary Rights.** Subject to the limited rights expressly granted hereunder, SFDC reserves all rights, title and interest in and to the Platform and the SFDC Service, including all related intellectual property rights. No rights are granted to You hereunder other than as expressly set forth in this SFDC Service Agreement. The Platform and the SFDC Service is deemed SFDC confidential information, and You will not use it or disclose it to any third party except as permitted in this SFDC Service Agreement.

5. **Compelled Disclosure.** If either You or SFDC is compelled by law to disclose confidential information of the other party, it shall provide the other party with prior notice of such compelled disclosure (to the extent legally permitted) and reasonable assistance, at the other party's cost, if the other party wishes to contest the disclosure.

6. **Suggestions.** You agree that SFDC shall have a royalty-free, worldwide, transferable, sublicenseable, irrevocable, perpetual license to use or incorporate into any SFDC products or services any suggestions, enhancement requests, recommendations or other feedback provided by You or Your Users relating to the operation of the Platform and/or the SFDC Service.

7. **Suspension and Termination.** Your use of the Platform and the SFDC Service may be immediately terminated and/or suspended upon notice due to (a) a breach of the terms of this SFDC Service Agreement by You or any User, (b) the termination or expiration of Reseller's agreement with SFDC pursuant to which Reseller is providing the Platform as part of the Reseller Application to You, and/or (c) a breach by Reseller of its obligations to SFDC with respect to the subscriptions it is providing to You in connection with this SFDC Service Agreement. If You use the Reseller Application in combination with a SFDC Service Org other than the Org provisioned solely for use with the Reseller Application (such SFDC Service Org, a "**Shared Org**"), Reseller shall be solely responsible for provisioning the Reseller Application to You. With respect to any Shared Org, You acknowledge and understand that (i) access to such Org, including the Reseller Application used in connection with such Org, may be suspended due to Your non-payment to SFDC or other breach of Your Agreement with SFDC, and (ii) in the event Your relationship with SFDC is terminated as a result of non-payment or other material breach of Your agreement with SFDC, Your Platform subscriptions would also be terminated. In no case will any such termination or suspension give rise to any liability of SFDC to You for a refund or other compensation. SFDC has no obligation to retain Your Data following thirty days after termination of Your final Platform subscription term. You have 30 days from the date of termination of your final Platform subscription term in which to request a copy of Your Data, which will be made available by SFDC to You in a .csv format.

8. **Subscriptions Non-Cancelable**. Subscriptions for the Platform and the SFDC Service are non-cancelable during a subscription term, unless otherwise specified in Your agreement with Reseller.

9. **No Warranty.** SALESFORCE.COM MAKES NO WARRANTIES OF ANY KIND, INCLUDING BUT NOT LIMITED TO WITH RESPECT TO THE PLATFORM, THE SFDC SERVICE, AND/OR THE RESELLER APPLICATION, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE. TO THE MAXIMUM EXTENT PERMITTED BY LAW, SALESFORCE.COM DISCLAIMS ALL CONDITIONS, REPRESENTATIONS AND WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, WITH RESPECT TO RESELLER APPLICATION AND THE SERVICE, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT OF THIRD PARTY RIGHTS.

10. **No Liability.** IN NO EVENT SHALL SFDC HAVE ANY LIABILITY TO YOU OR ANY USER FOR ANY DAMAGES WHATSOEVER, INCLUDING BUT NOT LIMITED TO DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, OR DAMAGES BASED ON LOST PROFITS, HOWEVER CAUSED AND, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, WHETHER OR NOT YOU HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

11. **Further Contact.** SFDC may contact You regarding new Platform and SFDC Service features and offerings.

12. **Third Party Beneficiary.** SFDC shall be a third party beneficiary to the agreement between You and Reseller solely as it relates to this SFDC Service Agreement.