IBM Cloud Service Description: IBM Kenexa Prove It! Add-ons on Cloud

The following is the Service Description for your Order:

1. Cloud Service Description

The following is the Cloud Service offering that you may order. The offering presented in this Service Description is considered an "add-on" offering, so you must subscribe to IBM Kenexa Prove It! before ordering any of the add-ons described in Section 1.1 below. The offerings that you have ordered are specified in your Order Document. For the purpose of this Cloud Service, the Order Document will consist of the Quotation that IBM presents to you and the Proof of Entitlement (PoE) that you will receive from IBM confirming the Cloud Services have been provisioned, notifying you when invoicing will commence, and setting forth the beginning and end date for the term of the Cloud Service.

1.1 IBM Kenexa Prove It! Add-ons on Cloud

IBM Kenexa Prove It! is an online solution that is provided to administer and support IBM Kenexa Skills Assessments and select IBM Kenexa Behavioral Assessments. IBM Kenexa Prove It! provides the following configuration services to customize the Prove It! web site to meet Customer's select requirements:

a. IBM Kenexa Prove It! Custom Web Site

This add-on offering allows you to change colors, logos and content in the Welcome section. There are no changes to the structure, banner or layout of the Welcome site or the rest of the web site.

b. IBM Kenexa Prove It! Corporate Custom Web Site

This add-on offering allows you to change colors, logos, content, banner, and layout in the Welcome section. There are no changes to the structure or layout of the rest of the web site.

2. Security Description

2.1 Security Policies

IBM maintains privacy and security policies that are communicated to IBM employees. IBM requires privacy and security education training to individuals worldwide who support IBM data centers and we maintain a security team that is focused on information security. IBM security policies and standards are reviewed and re-evaluated annually. IBM security incidents are handled in accordance with a comprehensive incident response procedure.

2.2 Access Control

Access to client data is allowed only by authorized IBM support representatives according to principles of segregation of duties. IBM support staff use two–factor authentication to an intermediate "gateway" management host. All connections are encrypted channels when accessing client data. All access to client data and transfer of data into or out of the hosting environment is logged. There is no usage of WIFI within the IBM data centers that support this Cloud Service.

2.3 Service Integrity & Availability

Modifications to operating system resources and application software are governed by IBM's change management process. Changes to firewall rules are also governed by the change management process and are separately reviewed by the IBM security staff before implementation. IBM monitors the data center resources 24x7. Internal and external vulnerability scanning is regularly conducted by authorized administrators and third party vendors to help detect and resolve potential system security exposures. Malware detection (antivirus, intrusion detection, vulnerability scanning, and intrusion prevention) systems are in place throughout all IBM data centers. IBM's data center services support a variety of information delivery protocols for transmission of data over public networks. Examples include HTTPS/SFTP/FTPS/S/MIME and site-to-site VPN. Backup data intended for off-site storage is encrypted prior to transport.

2.4 Activity Logging

IBM maintains logs of its activity for systems, applications, data repositories, middleware and network infrastructure devices that are capable of and configured for logging activity. To minimize the possibility of tampering and to enable central analysis, alerting and reporting, activity logging is done in real-time to central log repositories. Data is signed to prevent tampering. Logs are analyzed in real-time and via periodic analysis reports to look for anomalous behavior. Operations staff is alerted to anomalies and contacts a 24x7 on-call security specialist when needed.

2.5 Physical Security

IBM maintains physical security standards designed to restrict unauthorized physical access to data center resources. Only limited access points exist into the IBM data centers, which are controlled by two-factor authentication and monitored by surveillance cameras. Access is allowed only to authorized staff that have approved access. Operations staff verifies the approval and issues an access badge granting the necessary access. Employees issued such badges must surrender other access badges and can only possess the data center access badge for the duration of their activity. Usage of badges is logged. Non-IBM visitors are registered upon entering on premises and are escorted when they are on the premises. Delivery areas and loading docks and other points where unauthorized persons may enter the premises are controlled and isolated.

2.6 Compliance

IBM certifies its privacy practices annually as consistent with the U.S. Department of Commerce's Safe Harbor Principles: Notice, Choice, Onward Transfer, Access and Accuracy, Security, and Oversight/Enforcement. Industry standard audit SSAE 16 Type (formerly SAS 70), or equivalent, is performed annually in our production data centers. IBM reviews security and privacy-related activities for compliance with IBM's business requirements. Assessments and audits are conducted regularly by IBM to confirm compliance with its information security policies. Workforce security education and awareness training is completed by IBM's employees and vendor employees on an annual basis. Personnel are reminded of their job objectives and their responsibility to meet ethical business conduct, confidentiality, and IBM's security obligations on an annual basis.

3. Entitlement, Billing and Term Information

3.1 Charge Metrics

The Cloud Service offering is sold under the following charge metric as specified in the Order Document:

a. Instance is a unit of measure by which the Cloud Service can be obtained. An Instance is access to a specific configuration of the Cloud Service. Sufficient entitlements must be obtained for each Instance of the Cloud Service made available to access and use during the measurement period specified in the Proof of Entitlement (PoE) or Order Document.

3.2 Charges and Billing

The amount payable for the Cloud Service offerings is specified in the Order Document.

3.2.1 Set-Up

Set-up charges will be specified in the Order Document.

3.2.2 On-Demand

On-Demand options will be invoiced in the month the on-demand option is ordered by you at the rate set forth in the Order Document.