No Charge Cloud Agreement

This No Charge Cloud Agreement, the Service Description for IBM Cloud Identity as set forth in Exhibit 1 (SD) and any applicable Transaction Document (TDs) are the complete agreement (Agreement) governing the use of IBM Cloud Identity (Cloud Service) to enable Client to use its features and functionality at no charge. The Cloud Services may include other services IBM provides to enable or configure the Cloud Services. In the event of conflict, the No Charge Cloud Agreement and SD prevail over any applicable TD. Client means the company and its authorized users of the Cloud Services. This No Charge Cloud Service is available only to Clients who do not currently have authorized access to IBM Cloud Identity.

1. Use of Cloud Services

Client is authorized to use the Cloud Services during the No Charge Period. Upon expiration of the No Charge Period for any continued use Client will need to submit an order for the generally available Cloud Services offering. IBM is under no obligation to offer migration capabilities or services.

2. Content and Data Protection

a. Content consists of all data, software, and information that Client or its authorized users provides, authorizes access to, or inputs to the Cloud Service. Use of the Cloud Service will not affect Client's ownership or license rights in such Content. IBM, its affiliates, and contractors of either, may access and use the Content solely for the purpose of providing and managing the Cloud Service. IBM will treat all Content as confidential by not disclosing Content except to IBM employees and contractors and only to the extent necessary to deliver the Cloud Service.

b. Client is responsible for obtaining all necessary rights and permissions to enable, and grants such rights and permissions to, IBM, its affiliates, and contractors of either, to use, provide, store and otherwise process Content in the Cloud Service. This includes Client making necessary disclosures and obtaining consent, if required, before providing individuals' information, including personal or other regulated data in such Content. If any Content could be subject to governmental regulation or may require security measures beyond those specified by IBM for a Cloud Service, Client will not input, provide, or allow such Content unless specifically permitted in the terms of this Agreement or unless IBM has otherwise first agreed in writing to implement additional security and other measures.

c. IBM's Data Security and Privacy Principles for IBM Cloud Services (DSP), at http://www.ibm.com/cloud/data-security, apply for generally available Cloud Service offerings. Specific security features and functions of a Cloud Service may be provided in the Exhibit and TDs. Client is responsible to assess the suitability of each Cloud Service for Client's intended use and Content and to take necessary actions to order, enable, or use available data protection features appropriate for the Content being used with a Cloud Service. By using the Cloud Service, Client accepts responsibility for use of the Cloud Services, and acknowledges that it meets Client's requirements and processing instructions to enable compliance with applicable laws.

d. IBM's Data Processing Addendum at http://ibm.com/dpa (DPA) and applicable DPA Exhibit(s) apply to personal data contained in Content, if and to the extent: i) the European General Data Protection Regulation (EU/2016/679); or ii) other data protection laws identified at http://www.ibm.com/dpa/dpl apply.

e. IBM will return or remove Content from IBM computing resources upon the expiration or cancellation of the Cloud Service, or earlier upon Client's request. IBM may charge for certain activities performed at Client's request (such as delivering Content in a specific format). IBM does not archive Content, however some Content may remain in Cloud Service backup files until expiration of such files as governed by IBM's backup retention practices.

f. Upon request by either party, IBM, Client or affiliates of either, will enter into additional agreements as required by law in the prescribed form for the protection of regulated personal data included in Content.

The parties agree (and will ensure that their respective affiliates agree) that such additional agreements will be subject to the terms of the Agreement.

If the Cloud Services require use of enabling software, descriptions and details of the software and permitted use granted by IBM or third parties will be identified in the Exhibit or TD.

Cloud Services may not be used in any jurisdiction for any unlawful, obscene, offensive or fraudulent Content or activity, such as advocating or causing harm, interfering with or violating the integrity or security of a network or system, evading filters, sending unsolicited, abusive, or deceptive messages, viruses or harmful code, or violating third party rights. If there is a complaint or notice of violation, use may be suspended until resolved, and terminated if not resolved promptly.

3.   Charges, Payments & Taxes

There are no charges for use of the Cloud Services during the No Charge Period, unless specified by IBM or a third party service provider. If any authority imposes a custom, duty, tax (including withholding tax), levy or fee for the import or export, transfer, access or use of the Cloud Services, then Client is responsible to pay any such amount imposed.

4.   Changes

IBM may, in its reasonable discretion, change the terms applicable to the Cloud Services, modify the computing environment, or withdraw its features, in whole or in part by providing notice. Continued use of the Cloud Services is Client's acceptance of any such change. If Client does not accept a change, Client is responsible to discontinue use upon such notice.

5.   Term, Termination, and Suspension

Client may use the Cloud Services for ninety (90) days from account registration ("the No Charge Period"). Client may cancel use of the Cloud Services at any time by notifying IBM. At any time, IBM may, in its sole discretion, extend the No Charge Period.

6.   Liability and Indemnity

IBM's entire liability for all claims related to the Agreement will not exceed the amount of any actual direct damages incurred by Client up to the greater of, U.S. $1,000.00 (or equivalent in local currency) or up to the amounts paid, for the service that is the subject of the claim, regardless of the basis of the claim. IBM will not be liable for special, incidental, exemplary, indirect or economic consequential damages, lost profits, business, value, revenue, goodwill, or anticipated savings. These limitations apply collectively to IBM, its affiliates, contractors, subprocessors, and suppliers.

IBM has no responsibility for claims based on non-IBM products and services, items not provided by IBM, or any violation of law or third party rights caused by Client's Content, materials, designs, or specifications.

7.   Warranties and Disclaimers

Cloud Services are provided without warranties of any kind. IBM does not warrant uninterrupted or error- free operation of the Cloud Services. These warranties are the exclusive warranties from IBM and replace all other warranties, including the implied warranties or conditions of satisfactory quality, merchantability, non-infringement, and fitness for a particular purpose.

8. Governing Laws and Geographic Scope

Each party remains responsible for complying with: i) laws, rules and regulations applicable to its business and Content; and ii) import, export and economic sanction laws and regulations, including defense trade control regime of any jurisdiction, including the International Traffic in Arms Regulations and those of the United States that prohibit or restrict the export, re-export, or transfer of products, technology, services or data, directly or indirectly, to or for certain countries, end uses or end users. Client is responsible for its use of IBM and non-IBM products and services.

Both parties agree to the application of the laws of the State of New York, United States, without regard to conflict of law principles. The rights and obligations of each party are valid only in the country of Client's business address. If Client or any user exports or imports Content or use of any portion of the Cloud Service outside the country of Client's business address, IBM will not serve as the exporter or importer. If any provision of the Agreement is invalid or unenforceable, the remaining provisions remain in full force and effect. Nothing in the Agreement affects statutory rights of consumers that cannot be waived or limited by contract. The United Nations Convention on Contracts for the International Sale of Goods does not apply to transactions under the Agreement.

9. General

IBM and its affiliates, and their contractors and subprocessors, may, wherever they do business, store and otherwise process business contact information (BCI) of Client, its personnel and authorized users, for example, name, business telephone, address, email, and user ID for business dealings with them. Where notice to or consent by the individuals is required for such processing, Client will notify and obtain such consent.

Account Data is information, other than Content and BCI, that Client provides to IBM to enable Client's use of the Cloud Services or that IBM collects using tracking technologies, such as cookies and web beacons, regarding Clients use of a Cloud Service. IBM and its affiliates, its contractors and subprocessors may use Account Data for example to enable product features, administer use, personalize experience, and otherwise support or improve use of the Cloud Service. The IBM Online Privacy Statement at https://www.ibm.com/privacy/details/us/en/ provides additional details.

Neither party may assign the Agreement, in whole or in part, without the prior written consent of the other. Assignment in conjunction with the sale of the portion of IBM's business that includes a service is not restricted.

All notices under the Agreement must be in writing and sent to the business address specified for the Agreement, unless a party designates in writing a different address. The parties consent to the use of electronic means and facsimile transmissions for communications as a signed writing. Any reproduction of the Agreement made by reliable means is considered an original. The Agreement supersedes any course of dealing, discussions or representations between the parties.

IBM may use personnel and resources in locations worldwide, including third party contractors and subprocessors to support the delivery of the Cloud Services. IBM may transfer Content across country borders. A list of countries where Content may be processed for a Cloud Service is available upon request.

No right or cause of action for any third party is created by the Agreement or any transaction under it. Neither party will bring a legal action arising out of or related to the Agreement more than two years after the cause of action arose.

Exhibit 1
Service Description - IBM Cloud Identity

This Service Description describes the Cloud Service.

1.   Cloud Service

IBM Cloud Identity provides Single Sign-On (SSO), multifactor authentication and identity lifecycle controls for internal (employees) user types.

1.1   Offerings

The Client may select from the following available offerings:

1.1.1   IBM Cloud Identity Connect

This Cloud Service delivers Single Sign-On (SSO) and Open ID Connect (OIDC), Authentication as a Service for cloud-based API authorization, an application launchpad, administrator reporting and an analytics dashboard. This Cloud Service connects users to applications using modern standards-based authentication and federation protocols, including hundreds of connectors to common applications. This Cloud Service tightly integrates with the on-premise IBM Security Access Management (ISAM)software program, which is included as enabling software, to provide a solution for Clients to support their line-of-business demands for access management spanning both their on-premise and cloud applications.

1.1.2   IBM Cloud Identity Verify

This Cloud Service provides multi factor authentication for applications protected by Cloud Identity Connect, or via direct API invocation, and for other enforcement points including RADIUS clients, Unix/Linux PAM servers and Windows servers in order to verify their identities when accessing a digital service. This includes mechanisms such as time based (software token) one-time passwords, and push based mobile biometrics authentication powered by IBM Verify. This Cloud Service integrates with the on-premise IBM Security Access Management (ISAM)software program to provide a solution for Clients to support their line-of-business demands for access management spanning both their on-premise and cloud applications. It is available standalone, or to compliment Cloud Identity Connect, Cloud Identity Connect for ISAM and Cloud Identity Essentials.

2.   Data Processing and Protection Data Sheets

IBM's Data Processing Addendum at http://ibm.com/dpa(DPA) and the Data Processing and Protection Data Sheet(s) (referred to as data sheet(s) or DPA Exhibit(s)) in the links below provide additional data protection information for the Cloud Services and its options regarding the types of Content that may be processed, the processing activities involved, the data protection features, and specifics on retention and return of Content. The DPA applies to personal data contained in Content, if and to the extent i) the European General Data Protection Regulation (EU/2016/679) (GDPR); or ii) other data protection laws identified at http://ibm.com/dpa/dplapply.https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=735E5650E26711E69CCD7F0385C6524D

3.   Verification

Client will i) maintain, and provide upon request, records, and system tools output, as reasonably necessary for IBM and its independent auditor to verify Client's compliance with the Agreement, and ii) promptly order and pay for required entitlements at IBM's then current rates and for other charges and liabilities determined as a result of such verification, as IBM specifies in an invoice. These compliance verification obligations remain in effect during the term of the Cloud Service and for two years thereafter.