Service Description: Context Service Offering Description

The Context Service Offering Description ("**Offering Description**") describes the services comprising the Context Service (the "**Offering**") that Cisco Systems and its affiliates ("**Cisco**") or Cisco Approved Sources will provide to the applicable customer ("**Customer**").
Related Documents. This Service Description should be read in conjunction with the Cisco Universal Cloud Terms at http://www.cisco.com/c/dam/en_us/about/doing_business/legal/docs/universal-cloud-terms.pdf (the "**Agreement**").

Defined Terms. Capitalized terms used in this Service Description and not otherwise defined in the Service Description have the meanings given them in the Agreement. Capitalized terms that are unique to this Service Description are defined in the Glossary of Terms at the end of this document.

Cisco reserves the right to change this Service Description at any time.

1. OVERVIEW

1.1 Summary of Offering

The Context Service is a Cisco cloud-based service that interoperates with release 11.5 and higher of Cisco's Contact Center Express and Contact Center Enterprise solutions. The Service enables the users of the Service to store and associate contextual data with contacts that the user's customers make to user's contact center. The Context Service can support a wide variety of contextual data with the end user determining the contextual data it wants to associated with contacts. Thus, the Offering integrates data from the various ways Customer's customers can interact with Customer's business – such as voice, chat, social media, email and web – to help the agent be better informed and make that service experience more appealing. The service is operated by Cisco in a data center located in the United States.

The Offering is provided to you with the purchase of Cisco Software Support Service ("**SWSS**") for Cisco Contact Center Express or Cisco Contact Center Enterprise release 11.5 and above. Customers must have an active SWSS subscription on one or more of the following Cisco Contact Center product licenses to be entitled to use Context Service:

- Unified CCX agent licenses – all types
- Unified CCE agent licenses – all types
- Unified CVP port licenses
- Packaged CCE agent licenses
- HCS-Contact Center agent licenses

Only those customers with their billing address in a country in which the Offering is available (as set forth in Section 4 below concerning restricted availability) will be able to activate and use the Offering. Support for the Offering is the same support that you receive under your SWSS service contract. The SWSS Service Description is available at on the Cisco Services Descriptions page at the following address: http://www.cisco.com/c/dam/en_us/about/doing_business/docs/cisco-software-support-service.pdf

1.2 Features

- Cisco provided cloud storage of context (included for all Cisco Contact Center Express and Enterprise release 11.5 and above customers with SWSS contracts)
- Out of the box integration from Cisco Contact Center self service, email, and chat components as well as agent desktop.
- Business controlled encryption/security
- Access to third party custom applications via APIs published on Cisco DevNet..

1.3 Excluded Services

The Offering does not provide redundancy.

2. LIMITATIONS, DISCLAIMERS AND NOTICES

Cisco operates a single data center instance of the Offering in the United States. As a result, Customer might experience periods of extended downtime. Cisco makes the Offering available on an "AS IS" and "AS AVAILABLE" basis without any uptime or other service level guarantees. Support is provided under the associated SWSS contract and, thus, subject to the SWSS Service Description.

Customer acknowledges that: (i) Customer's access to and use of the Offering may be suspended for the duration of any unanticipated or unscheduled downtime or unavailability of any portion or all of the Offering for any reason, including as a result of power outages, network connection failure, system failures or other interruptions; and (ii) Cisco shall also be entitled, without any liability to Customer, to suspend access

to any portion or all of the Offering at any time, on a Offering-wide basis: (a) for scheduled downtime to permit us to conduct maintenance or make modifications to any Service; (b) in the event of a denial of service attack or other attack on the Offering or other event that we determine, in our sole discretion, may create a risk to the Offering, to Customer or to any of our other customers if the Offering were not suspended; or (c) in the event that we determine that the Offering is prohibited by any applicable law, regulatory requirement or any other statutory or non-statutory provision or Cisco otherwise determines that it is necessary or prudent to do so for legal or regulatory reasons (collectively, "**Service Suspensions**"). Without limitation, we shall have no liability whatsoever for any damage, liabilities, losses (including any loss of data or profits) or any other consequences that Customer may incur as a result of any Service Suspension. To the extent we are able, we will endeavor to provide Customer with notice of any Service Suspension seven (7) days in advance and to post updates regarding resumption of Offering following any such suspension, but shall have no liability for the manner in which we may do so or if we fail to do so. To the extent we are able, we will endeavor to restore the Offering to Customer as soon as is reasonably practicable following any scheduled downtime permitting us to conduct maintenance or make modifications to the Offering.

3. STORAGE CAPACITY

There is no limit on the amount of data storage provided to Customer. However, Cisco reserves the right to enforce a data storage quota limit or charge for data storage beyond 1 TB. If Cisco elects to enforce a data storage quota limit or charge a fee for a data storage beyone 1 TB, Cisco will update the documentation on Cisco.com and will enforce the policy for the customer at their next SWSS billing cycle. Customer is responsible for checking the latest policy at their SWSS renewal. Alternatively, Cisco may elect to enforce the policy with 90 days written notice to a customer, independent of SWSS billing cycle. If Customer elects not to pay the fee, then Customer will have the opportunity to back up the data, and Cisco will purge data until data storage usage is within the stated quota.

4. RESTRICTED GEOGRAPHIC AVAILABILITY

The Offering is not available to Cisco customers located in the Russian Federation or the People's Republic of China.

5. OFFERING ACTIVATION

5.1 Activation for SAAS Offering

5.1.1 Overview

To activate the Service, Customer will need a current email address and password. Customer's Cisco Partner will create an account for the customer with Context Service entitlement. Customer will use their email and password to connect their Cisco Contact Center Express or Contact Center Enterprise solutions with Context Service.

5.1.2 Customer Requirements

- *General Information and Reasonable Assistance*. Customer shall supply Cisco with all reasonably requested and reasonably necessary, accurate, complete, and up to date information and assets to allow Cisco to supply the Offering to the Customer. Provide updated and accurate information on Customer's hardware and software environment, networking information, and similar information reasonably required or requested to provide the Services. Customer will reasonably work with Cisco in a timely manner to aid in Cisco's provision of the Offering to Customer by any third party cooperation, documents or approvals required for provision of Cisco's Offering.

- *Issue Triage & Resolution***.** Provide technical resources for the following: capture and provide details of reported issues, aid in replication and triaging issues as reasonably requested by Cisco, aid in testing fixes of issues, confirming issues are not related to End User provided hardware, software, applications, or other sources.

- *Data Backup.* Maintain appropriate protection and backup of End User data and content at all times. Customer assumes full responsibility to back-up and/or otherwise protect all data against loss, damage, or destruction. Customer acknowledges that it has been advised to back-up and/or otherwise protect all data against loss, damage or destruction.

- *Security.*
  - Maintain appropriate security against unauthorized access, use or deletion of End User data. Establish and maintain appropriate security policies within the infrastructure, as well as any operating systems or applications.
  - Customer is responsible for implementing and using strong passwords for accessing Cisco infrastructure and the associated support portal. The following are common guidelines for choosing strong passwords. These are designed to make passwords less easily discovered by intelligent guessing: (i) Include numbers, symbols, upper and lowercase letters in passwords; (ii) Password length should be around 12 to 14 characters; (iii) Avoid any password based on repetition, dictionary words, letter or number sequences, usernames, relative or pet names, or biographical information (e.g., dates, ID numbers, ancestors' names or dates...).
  - Customer must not use the Services to send spam, viruses or malware.
  - Customer is responsible for any catastrophic security events that result from any unauthorized configuration of the Offering components by Customer's personnel. These include, but are not limited to, configuring the Offering components in a manner not prescribed in the Documentation, creating an open relay, changing the network configuration set by Cisco, shutting down Cisco's infrastructure, etc.
  - Customer shall protect their access authorization against third-party access and shall immediately modify the same if a third party may have become aware thereof. Customer shall ensure the access authorization may be used only by that to whom it was assigned.

Cisco shall not be liable if a third party uses or abuses Cisco Offering with the access authorization assigned to the Customer. The Customer shall indemnify and hold Cisco harmless in respect of any damage Cisco may incur as a result from such use or abuse.

- *Compliance Review.* Cisco will have the right, upon reasonable notice, to audit Subscriber's records (including but not limited to the List) during normal business hours to ensure Subscriber's compliance with the above requirements. Cisco will pay the cost of the audit unless it is found that Customer is misusing the Service.

6. OFFERING OPERATIONS

6.1 Support and Escalation Guidelines

Support and escalation is provided as set forth in the associated Service Description for SWSS.

6.2 Maintenance and Updates

- From time to time, Cisco performs scheduled maintenance, to update the servers and software that are used to provide the Service. Cisco will make all notifications for such scheduled maintenance solely via https://status.ciscospark.com/. Notwithstanding the foregoing, Customer acknowledges that Cisco may need to perform emergency maintenance without providing advance notice. Cisco operates a single data center instance of the Offering in the United States. As a result, Customer might experience periods of extended downtime.

- Cisco reserves the right to modify and update the features and functionality of the Services, at no additional cost to Customer. These updates shall include any subsequent release or version of the Services containing functional enhancements, extensions, error corrections or fixes which are generally made available free of charge to customers who have an active SWSS contract for CCE and CCX release 11.5 or later. Updates shall not include any release, option or future product which Cisco licenses separately or which is not included under the applicable level of support.

- Provide all Updates and Releases commercially by Cisco. Cisco will give Customer notice of any material modification or update via http://www.cisco.com/go/contextservice. Cisco will use reasonable efforts to ensure that any modifications or updates do not materially degrade the performance of the Services or Customer's use of the Services. Cisco will ensure that any modifications or updates do not require Customer to incur any material additional cost to continue its use of the Services.

- Cisco will use reasonable efforts to implement modifications or updates in a manner that minimizes the impact on Customer's use of the Services but makes no guarantees that such notice will be provided. Cisco will provide seven (7) days advance notice only when possible.

ANNEX B
Optional Terms for SAAS Offering

1. Privacy/Security

All of the data stored for the Offering is stored only in the United States. The information below describes the types of information we gather and retain. This information can also be found in the Context Service Supplemental Privacy Information statement located at http://www.cisco.com/web/siteassets/legal/privacy_full.html

Cisco Context Service Data Privacy Supplement

Note that this page is a supplement to the Cisco Privacy Statement. In order to understand the data collection and use practices relevant for a particular site or solution, you should read both the Cisco Privacy Statement and any applicable supplement.

Collection and Use of Information

User Definitions

Context Service collects or stores different information depending on the type of user accessing the system. This documents classifies different users as follows:

- You: Administrators of Cisco Contact Centers and Context Service. The intended audience of this document.
- Organization: A customer of Cisco or its partner or affiliates who are licensees of Cisco Contact Center products that store data on Context Service.
- Agent: Employee of an organization.
- Customer: Customer of an organization (your customer). Also known as a “caller.”

Personal and Organizational Information

Registration Information (onboarding): When you (and/or your organization) sign(s) up to use Cisco Context Service (the "Service"), we collect personal information about you, including your name, email address ("Registration Information"), in addition to a password ("Authentication Information"). We also collect the name of your organization and any other details that you provide to us about yourself or your employer.
We use Registration Information to enroll you and your organization in the Service, to notify you about features and updates, to understand how the Service is used, and to make improvements to the Service and other Cisco products and services.

Agent Information

We collect and store information about your agents/employees. We collect and store the name and/or ID of an agent as defined in Cisco UCCE or Cisco UCCX. And we collect and store any other information about your agents that you provide to us.

Host and Usage Information

Our servers automatically record certain information when you, your employees, and your customers use the Service, including IP address, user agent identifier, operating system type and version, and client version ("Host Information"). We also automatically record information about your and your employees’ and customers’ usage of the Service, including actions taken, date and time, frequency, duration, quantity, quality, network connectivity, and performance information related to logins, clicks, and other feature usage information ("Usage Information"). We use Host Information, error logs generated by the application, and Usage Information to understand how the Service is used, to diagnose problems, to respond to support requests, to conduct analytics and aggregate statistical analysis, and to improve the Service and other Cisco products and services. We also use Host Information to display the status (registration and connection status) of your servers and clients in service management tools. We also use this information to send your servers and clients periodic “pings” to verify their connection status to the service.

Data Categories

We collect and store service related data as directed by your configuration of the service. There are two broad categories of service-related data; fixed-fields, and your custom-defined fields. Cisco provides a default set (base fieldsets) for custom fields. All custom fields are optional and, ultimately, you decide which data is stored in the fields (either Cisco-defined and/or organization-defined fields). Fields and Fieldsets generally contain information about your customers.

Fixed Fields

Certain fields are fixed and are used to store meta-data about the customer or their activities. These are populated by the service, such as date time, agent identifier, authorization workgroups, custom field schema, etc. Meta-data for a customer activity may include, but not limited to, the media type of the interaction (for example, “voice” or “email”), current state of the interaction (for example “closed”), authorization associated with the interaction, and any “tags” that you apply to the interaction. This meta-data is stored as plain text, but transported over an encrypted layer (HTTPS).

Custom Fields

All custom fields are assigned to one of three privacy categories:

- Personally Identifiable Information (PII) - information that can be personally linked with an individual. PII is always stored and transported (end-to-end and transport encryption) in an encrypted format. Examples include name, email, postal address, phone, age, DOB, etc.
- Non-PII Encrypted - information that cannot be linked to an individual, but is still considered confidential. Non-PII Encrypted is always stored and transported in an encrypted format.
- Unencrypted - Information which is not PII and not confidential. It is stored as plain text, but transported over an encrypted layer (HTTPS).

Cisco provides several default fields as template into which you can store data. You select which fields you want to use to store data. All fields are optional. The Cisco defined fields cover the most common fields used in a contact center, such as customer name, address, phone number, email, notes, activity link, etc.
You and your organization can create additional custom “fields” to store data for your customer’s activities by defining a field name, privacy classification, and data type for the field. These field definitions are grouped into sets and become your organizations custom data schema.
We collect and store details about the data schema that you create to store context data. We collect the names of fields, their privacy level, their data type, and how they are grouped into fieldsets.

Securing Your Information

The Service uses different kinds of encryption to protect different kinds of data in transit and in storage.
End-to-end encryption is used to protect encrypted custom fields that you share on the Service. Just prior to sending a message from your client, it is encrypted on your device locally. Messages remain encrypted until other authorized users retrieves them on their device, where they are decrypted locally on that device.
Transport encryption (also known as HTTPS) is used to protect all connections to and from the Service. When you register for the Service, store or retrieve data, connect with third-party services or applications via Cisco provided SDKs, we always use transport encryption.
As described above, custom fields are stored on our servers based on their field definition. The field definition determines if the field is stored encrypted or unencrypted. Authentication Information is encrypted in storage; Registration Information, Host Information, and Usage Information is not.

Use of Cookies and Other Web Technologies

When you, your employees, and customers use the Service in a web browser, we use cookies, local storage, and other browser storage technologies to ensure that you can stay logged into the Service until you choose to log out and to improve the performance of the Service. These technologies may store Registration Information, Host Information, and/or Usage Information. Cookies are always sent using transport encryption.

Sharing Your Information

We do not share your or your customer information with third parties without your permission.

Other

When you use the Service, you are subject to the Cisco SaaS Terms of Service.