Offer Description: CES, CRES, DMP and APP

This Offer Description (the **"Offer Description"**) describes Cisco Cloud Email Security ("CES"), Cisco Registered Envelope Service ("CRES"), Cisco Domain Protection ("DMP"), and Cisco Advanced Phishing Protection ("APP") (the **"Cloud Service(s)"**). Your subscription is governed by this Offer Description and the Cisco Universal Cloud Agreement located at www.cisco.com/go/uca (or similar terms existing between you and Cisco) (the **"Agreement"**). Capitalized terms used in this Offer Description and/or the Order not otherwise defined herein have the meaning given to them in the Agreement.

Table of Contents

1. Offer Description.

1.1. Cisco Cloud Email Security and Cisco Registered Envelope Service.

CES is a cloud-based email security service that blocks spam and security threats from the Internet and, depending on the features licensed, prevents the accidental or intentional leakage of Your data. CES includes the option to license CRES. CRES helps companies secure their email communications and allows businesses to send encrypted messages via registered envelopes. Other features and functionality are available depending on the licensed features purchased, including anti-spam, intelligent multi-scan anti-spam, anti-virus, outbreak filters, advanced malware protection, safe unsubscribe, image analysis, and data loss prevention.

1.2. Cisco Domain Protection.

DMP for external email helps prevent phishing emails from being sent using a customer domain(s). The DMP service automates the process of implementing the email authentication standard Domain Message Authentication Reporting & Conformance ("DMARC") to better protect employees, customers and suppliers from phishing attacks using a customer domain(s). This protects the customers' brand identity as well as increases email marketing effectiveness by reducing phishing messages from reaching inboxes.

1.3. Cisco Advanced Phishing Protection.

APP stops identity deception based attacks such as social engineering, impostors and business email compromise and provides local email intelligence and advanced machine learning techniques to model trusted email behavior on the internet, within organizations and between individuals. APP's protection integrates machine learning techniques to drive daily model updates, maintaining a real-time understanding of email behavior to stop identity deception.

2. Supplemental Terms and Conditions

2.1. Use Limitations.

Cisco may audit Your usage of CES and if Cisco determines in good faith that You are using CES as an outbound bulk email delivery service, Cisco may require You to purchase additional services or require You to re-architect the email flow to exclude CES from the outbound bulk email flow. The Cloud Services are licensed based on the quantity of Users.

2.2. CES - Capacity Assurance.

Cisco may, in its sole and reasonable discretion and solely to the extent Your account is in good standing, provide additional capacity to handle an increase in spam volumes and inbound email for the number of Users specified on the Order. In such case, Cisco will use commercially reasonable efforts to provide capacity for unforeseen events. Any such additional capacity, if made available, will not exceed 50% of the initial deployed capacity.

The above capacity assurance does not apply to:

- Capacity requirements placed on CES due to misconfigured, ill-formed or performance intensive activities that include but are not limited to body-scanning, or content dictionaries.
- Capacity needs placed on CES resulting from a change in applicable regulatory schemes or business environment.
- Capacity needs placed on CES from non-users including, but not limited to, marketing communications, Your customers, or an email generating program or entity.
- An increase in email volume from marketing campaigns and other application-generated emails.

2.3. DMP - Data Usage Acknowledgement.

In connection with Your use of DMP, You can, at your discretion, publish a DMARC policy via your own DNS infrastructure. This policy instructs email service providers ("ESPs") to send numerical summaries to the Cloud Service about messages which have been processed and which appear to come from Your domains. You may also request that these ESPs send examples of messages failing email authentication to the Cloud Service. Some ESPs provide only redacted message samples containing the sender's email address, the message subject, URLs, and SMTP headers. Other ESPs may send the full content of the messages failing authentication in the failure sample feed, but in such cases the Cloud Service retains only the header information referenced in the preceding sentence above. In most cases, these failure examples originate from fraudulent senders and the URLs and attachments contain malware or link to fraudulent web sites. The details from these failure examples are shared only with You and are retained by the Cloud Service for no more than 14 days, at which time they are deleted following the then current Amazon Web Services best practices. Cisco and/or its applicable subprocessors and subcontractor(s) may use this Customer Data relating to emails that fail authentication ("Authentication Failure Data") in order to provide the Cloud Service

and as otherwise authorized under the Agreement and this Offer Description. Without limiting rights otherwise set forth in the Agreement and this Offer Description, Cisco (and its subprocessor(s)) may compile, aggregate, publish, use and share anonymized summaries of such Authentication Failure Data both during and after the subscription term to determine and report Cloud Service usage patterns, to analyze and report security related issues and trends, and to improve upon and create new products and service offerings. You further acknowledge that, notwithstanding anything to the contrary herein or in the Agreement, Cisco (and its subprocessors and subcontractors involved in the delivery of the Cloud Service) may license and provide such aggregated and anonymized summary data (excluding Your Confidentidal Information and any personally identifiable information (if any is actually received)) to its or their licensees for their internal use in doing the same, both during and after the term of the Agreement. For clarity, no customer Confidential Information will be disclosed, published or shared with any third party. To the extent You may have any rights in or to any Authentication Failure Data, You hereby provide Cisco (and its subprocessors and subcontractors involved in the delivery of the Cloud Service) a perpetual, royalty-free, transferable license to do all of the foregoing. This paragraph will survive the expiration or termination of the Agreement.

2.4. Cisco Threat Content.

If Your use of a Cloud Service requires or permits You to use any Cisco Threat Content, then You (and Your agents acting on your behalf) may only use such Cisco Threat Content for Your use with such Cloud Service and with those third party products or services offerings that Cisco has identified as being compatible. You agree not to provide Cisco Threat Content to a third party.

2.5. Restrictions.

You may use the Cloud Service for Your own internal business purposes and shall not outsource, sublicense, resell, lease, transfer or otherwise allow use of the Cloud Service for the benefit of any third party; except to the extent You are an authorized Cisco service provider whose contract with Cisco authorizes You to utilize Cisco cloud services on behalf of end customers (in which case You may use the Cloud Service only for the benefit of such end customers). You shall not (i) create derivative works based on the Cloud Service, or cause or permit others to; (ii) modify, reverse engineer, translate, disassemble, or decompile the Cloud Service, or cause or permit others to; (iii) access the Cloud Service in order to build a competitive product or service; or (iv) access the Cloud Service in order to infringe or misappropriate any intellectual property included in the Cloud Service. You will promptly notify Cisco of any unauthorized access or use of the Cloud Service.

2.6. Disclaimers.

CISCO DOES NOT REPRESENT OR WARRANT THAT THE CLOUD SERVICES WILL GUARANTEE ABSOLUTE SECURITY DUE TO THE CONTINUAL DEVELOPMENT OF NEW TECHNIQUES FOR INTRUDING UPON AND ATTACKING FILES, NETWORKS AND ENDPOINTS. CISCO DOES NOT REPRESENT OR WARRANT THAT THE CLOUD SERVICES WILL PROTECT ALL YOUR FILES, NETWORK, OR ENDPOINTS FROM ALL MALWARE, VIRUSES OR THIRD PARTY MALICIOUS ATTACKS. CISCO DOES NOT MAKE ANY REPRESENTATIONS OR WARRANTIES REGARDING ANY THIRD PARTY SYSTEM OR SERVICE TO WHICH A CLOUD SERVICE INTEGRATES OR TO ANY ONGOING INTEGRATION SUPPORT. INTEGRATIONS MADE ACCESSIBLE TO YOU THAT ARE NOT A GENERALLY AVAILABLE PRODUCT INCLUDED ON YOUR ORDER ARE PROVIDED ON AN “AS IS” BASIS.

2.7. Integration with Third Party Products.

The Cloud Service may allow you to integrate with third-party products.
Cisco does not support or warrant third-party products and disclaims all responsibility and liability for third-party products used with the Cloud Service, including any responsibility for customer data transferred to such third-party product through Your use of the applicable integration. If You use a third-party product, the terms of use for that third-party product are between You and the provider. Some third-party products may contain tracking technology. Accordingly, it is Your responsibility to read the third party's disclosures, terms of use, and privacy policy before using such third-party products with the Cloud Service.

3. Service Level Agreements.

3.1. CES and CRES.

The following defined terms apply to the CES and CRES service level agreements set forth below in this Section 2.7 (the "Service Level Agreement(s)"):

- **Caught Spam** means Spam that is either quarantined or categorized as a "threat message" in the user interface.
- **Infraction** means a single instance of unavailability in accordance with the specific calculation set forth in the applicable Service Level Agreement. Separate downtime occurrences cannot be aggregated for purposes of determining an Infraction has occurred.
- **Known Virus** means a virus defined solely by the provider of anti-virus software that is used for a specific message or file.
- **Missed Spam** is Spam delivered to an end user's email inbox.
- **Service Credits** mean the amounts set forth in the applicable table in each Service Level Agreement in this Section 2.7.
- **Spam** means unsolicited or unauthorized bulk electronic mail (SMTP only), and excludes unwanted marketing messages that include opt-out provisions.
- **Virus** means a binary or executable code whose purpose is to gather information from the infected host, change or destroy data on the infected host, use inordinate system resources in the form of memory, disk space, CPU cycles or network bandwidth on the infected host, use the infected host to replicate itself to other hosts, or provide control or access to any of the infected host's system resources. A Virus does not include: (1) text messages that use fraudulent claims to deceive the customer, and/or prompt the
  customer to action, (2) a binary or executable code installed or run by the end user that gathers information for sales or marketing purposes, (3) a virus that may be detected and cleaned by other virus scanning products, or (4) an ineffective or inactive virus fragment.

Service Credits Remedy.
The Service Credits available to You under the CES and/or CRES Service Level Agreements are Your sole and exclusive remedy for Cisco's failure to meet the applicable Service Level Aagreement including an Infraction.

CES Uptime Service Level Agreement.
CES will accept connections on Port 25 and process email at least 99.999% of the time during each calendar month, excluding maintenance windows. Uptime is determined by dividing the total number of minutes CES was processing email divided by the number of minutes in that calendar month. A CES downtime must exceed 26 seconds per occurrence for it to be considered an Infraction.

If You experience a downtime Infraction, then subject to the General Exceptions (defined below), You will be entitled to the applicable Service Credit set forth in the table below.

Monthly Service Availability	Service Credit as a % of Monthly Fee
< 99.999%	20%
< 99.0%	40%
< 98.0%	100%

CES Delivery Time Service Level Agreement.
CES will process email messages such that the monthly Average Time in the Work Queue of CES (as shown in the administrator console) will be less than one (1) minute based on a calendar month, provided, that the quantity of email messages above 10MB sent to CES does not exceed 0.01% of all email traffic. "Average Time in the Work Queue" is the amount of time spent processing a message from the point at which the message is accepted via SMTP to the first SMTP delivery attempt from CES.

If You experience a delivery time Infraction, then subject to the General Exceptions, You will be entitled to the applicable Service Credit set forth in the table below.

Monthly Average Delivery Time	**Service Credit as a % of Monthly Fee**
> 1 minute	20%
> 5 minutes	40%
> 10 minutes	100%

CES Anti-Spam Service Level Agreement.
CES will detect and stop at least 99% of all inbound Spam that is routed through CES. This "Spam Catch Rate" is determined by dividing Caught Spam by the sum of the Caught Spam and the number of Missed Spam, during a calendar month. Exception: Marketing emails with opt-out provisions will not be counted as a Missed Spam.

If You experience a Spam Catch Rate Infraction, and subject to the exception above and the General Exceptions, then You will be entitled to the applicable Service Credit set forth in the table below.

Spam Catch Rate During Month	Service Credit as a % of Monthly Fee
< 99%	20%
< 98%	40%
< 95%	100%

CES False Positive Rate Service Level Agreement.
CES will not categorize legitimate inbound email as Spam more than one (1) time per one million (1,000,000) messages processed. This "False Positive Rate" is determined by dividing the number of non-Spam messages misclassified as Spam by the total attempted messages processed during that calendar month.

Exceptions and Conditions:

Email messages from legitimate senders whose IP addresses may be compromised due to an unforeseen event will not be counted towards the False Positive Rate. Cisco will make a determination in good faith based on its system logs, monitoring reports and configuration records for such email senders. In addition, marketing emails with opt-out provisions will not be counted towards the False Positive Rate.

The following conditions also apply to this False Positive Rate Service Level Agreement:

- SenderBase reputation filters must be enabled at default levels or more conservatively,
- You must have the reputation messages per connection multiplier set to the default value;
- You must have IronPort Anti-Spam (IPAS) block settings at the default value or more conservatively;
- You must have IronPort Anti-Spam quarantine enabled with settings at default or more conservatively;
- You must have SenderBase Network Participation enabled;
- You must provide copies of false positive messages to Cisco;
- You must provide the domains covered by CES, the number of mailboxes and the incoming mail report for the last thirty (30) days; and
- You must only enable IPAS for spam scanning to qualify.

Failure to comply with any of the above conditions will eliminate Your right to receive a Service Credit under this this Service Level Agreement.

If You experience a False Positive Rate Infraction, and subject to the exceptions set forth above and the General Exceptions, then You will be entitled to the applicable Service Credit set forth in the table below.

False Positives During a Month	Service Credit as a % of Monthly Fee
> 1 in 1 Million	20%
> 1 in 100 Thousand	40%
> 1 in 1 Thousand	100%

CES Virus Catch Rate Service Level Agreement.
CES will detect and stop one hundred percent (100%) of all Known Viruses that are routed through CES within thirty (30) minutes of when the applicable anti-virus provider releases a signature for the platform (the “Virus Catch Rate”).

Exceptions and Conditions:
Messages that contain a URL to a website hosting malware and Virus attachments that are password protected are not included in the Virus Catch Rate.

The following conditions also apply:

- You must have SenderBase reputation filters enabled at a default level or more aggressively;
- SenderBase Network Participation must be enabled;
- You must provide all samples of missed Viruses to Cisco,
- You must ensure that the message was scanned by the anti-virus engine (e.g. message did not exceed the maximum scanning size limit); and

- You must provide the domains covered by CES, the number of mailboxes and the incoming mail report for the last thirty (30) days.

Failure to comply with any of the above conditions will eliminate Your right to receive a Service Credit.

If You experience a Virus Catch Rate Infraction, and subject the exception set forth above and the General Exceptions, then You will be entitled to the applicable Service Credit set forth in the table below.

Virus Catch Rate During a Month	Service Credit as a % of Monthly Fee
< 100%	20%
< 99%	40%
< 95%	100%

CRES Uptime Service Level Agreement.
CRES will be Operational at least 99.999% of the time during each calendar month, excluding maintenance windows. For the purposes of this section, "Operational" means that You will have access to CRES for the purposes of: (1) encrypting emails; (2) enabling secure envelope recipient actions (e.g. opening, secure reply, secure forward, and/or forwarding to mobile@res.cisco.com); and (3) CRES user account access. CRES uptime is determined by dividing the total number of minutes CRES was Operational divided by the number of minutes in that calendar month. Consequently, an Infraction is a minimum of thirty (30) seconds of CRES downtime. CRES uptime is determined and validated by an industry-recognized third-party monitoring service that performs service-level checks from various locations on the Internet.

Exceptions:
This Service Level Agreement excludes any downtime resulting from Your administrator account access.

Remedy:
If You experiences a downtime Infraction, and subject to the exception above and the General Exceptions, You will be entitled to the applicable Service Credit set forth in the table below.

Monthly Service Availability	Service Credit as a % of Monthly Fee
< 99.999%	20%
< 99.0%	40%
< 98.0%	100%

General Service Level Agreement Conditions.
All remedies for Service Credits referred to in this Section 2.7 above are conditioned upon Your (1) payment of all applicable fees, (2) fulfillment all of Your obligations under the Agreement and this Offer Description, and (3) Your submission of a claim in accordance with the SLA Claim Procedure below. If You have earned a Service Credit but have prepaid for a subscription in full and You do not renew such subscription, then all such earned Service Credits will be forfeited and no refund will be provided.

Service Credits earned will be applied to either (1) the subscription fee for the next subscription term if You have prepaid for the then-current subscription in full, or (2) the next installment payment amount owed if You are paying for the subscription on a monthly, quarterly or annual installment basis.

Service Credits do not apply as a result of CES or CRES not meeting a particular Service Level Agreement due to any of the following ("General Exceptions"):

- Hardware or software upgrades, facility upgrades, or other similar Customer-led network interruptions requested by You;
- A scheduled maintenance period that was announced at least 24 hours in advance;
- Hardware, software or other data center equipment or services not in the control of Cisco or within the scope of CES;
- Hardware or software configuration changes made by You;
- Denial of CES attacks on the installed email security infrastructure or ancillary services such as SenderBase; or
- Events outside of Cisco's reasonable control, including without limitation acts of God, earthquake, labor disputes, industry wide shortages of supplies, actions of governmental entities, riots, war, terrorism, fire, epidemics, or delays of common carriers.

SLA Claim Procedure.
You must submit a claim for a Service Credit within thirty (30) calendar days of the claimed Infraction. Each claim must be supported with evidence from message logs, sample messages, support ticket numbers, ping or trace route data, reporting data or other applicable method for documenting the occurrence and duration of the claimed Infraction. You must certify that (1) no changes or actions initiated by You were responsible for the occurrence resulting in the claimed Infraction, and (2) You did not ignore warnings by Cisco of certain behavior that is responsible for such occurrence—including but not limited to, the presence of a mail loop due to configuration within or external to CES; creating a policy bypass around anti-spam policies in the policy configuration; creating a policy bypass around anti-virus filtering in the configuration; or misconfiguration of an encryption profile or failure to permit upgrade of the PXE-SDK or software version of CES. You must submit all claims for Service Credits via a support ticket. Cisco will evaluate the claim, respond within forty-eight (48) hours regarding the validity of the claim, and, if applicable, provide Service Credits under the applicable remedy section within thirty (30) days following such response.

3.2. DMP and APP.

The following defined terms apply to the service level agreement set forth in this Section 2.8 ("DMP-APP Availability SLA"):

- **Emergency Maintenance** means any time outside of the Scheduled Maintenance Window that Cisco is required to apply urgent patches or fixes, or undertake other urgent maintenance activities.
- **Infraction** is a single instance of unavailability in accordance with the specific calculation set forth in this DMP-APP Availability SLA. Separate downtime occurrences cannot be aggregated for purposes of determining if an Infraction has occurred.
- **Scheduled Maintenance Window** means the window during which weekly scheduled maintenance ("Scheduled Maintenance") of the Cloud Service may be.

The Scheduled Maintenance Window is between the hours of Friday 9:00 p.m. to Saturday 5:00 a.m. Pacific time.

- **Service Availability** means the percentage of total time during which the Cloud Service (including but not limited to the Cloud Service portal) is available to You and operating properly without material degradation of service, excluding up to thirty minutes per month for Scheduled Maintenance and Emergency Maintenance. "Available" in this context means You may log in, view data, create reports, modify settings and similar, and substantially all licensed components, including but not limited to hosted sensors (if applicable) and the Cloud Service portal, are functioning properly.
- **Service Credit** means the percentage of the Calculated Monthly Fees paid that is awarded You for validated claim(s) associated with that portion of the Cloud Service related to breach of this Service Availability SLA during that month (see below for applicable percentages). The "Calculated Monthly Fee" is defined as fees received for Your annual subscription for the Cloud Service divided by 12.

Remedy.
Service Credits are Your sole and exclusive remedy for any failure to achieve the DMP-APP Availability SLA including any Infraction.

All remedies for Service Credits referred to in this Section 2.8 above are conditioned upon Your (1) payment of all applicable fees, (2) fulfillment of all of Your obligations under the Agreement and this Offer Description, and (3) Your submission of a claim in accordance with the SLA Claim Procedure below. If You have earned a Service Credit but have prepaid for a subscription in full and You do not renew such subscription, then all such earned Service Credits will be forfeited and no refund will be provided.

SLA Claim Procedure.
You must submit a claim for a Service Credit within thirty (30) calendar days of the claimed Infraction. Each claim must be supported with evidence from message logs, sample messages, support ticket numbers, ping or trace route data, reporting data or other applicable method for documenting the occurrence and duration of the claimed Infraction. You must certify that (1) no changes or actions initiated by You were responsible for the occurrence resulting in the claimed Infraction, and (2) You did not ignore warnings by Cisco of certain behavior that is responsible for such occurrence. You must submit all claims for Service Credits via a support ticket. Cisco will evaluate the claim, respond as soon as reasonably possible regarding the validity of the claim, and, if applicable, provide Service Credits under the applicable remedy section within thirty (30) days following such response.

Exclusions.
Service Credits do not apply as a result of not meeting the DMP-APP Availability SLA due to any of the following ("General Exceptions"):

- Use of the Cloud Service outside the scope described in the Agreement or this Offer Description.
- Hardware or software upgrades, facility upgrades, or other similar customer-led network interruptions requested by You;
- A Scheduled Maintenance period that was announced at least 24 hours in advance;
- Hardware, software or other data center equipment or services not in the control of Cisco or within the scope of the Cloud Service;

- Hardware or software configuration changes made by You or Your failure to meet the configuration requirements set forth in the Documentation for this Cloud Service;
- Denial of service attacks on the installed email security infrastructure or ancillary services such as SenderBase; or
- Events outside of Cisco's reasonable control, including without limitation acts of God, earthquake, labor disputes, industry wide shortages of supplies, actions of governmental entities, riots, war, terrorism, fire, epidemics, or delays of common carriers.

Availability SLA Percentage and Credits.
Cisco will provide at least 99.999% Service Availability for the Cloud Service (including but not limited to the portal, hosted sensors (if applicable) and other licensed components) during each calendar month, excluding up to thirty (30) minutes per month for Scheduled Maintenance and Emergency Maintenance. Service Availability is calculated as follows:

Availability = (X/Y) x 100, where

X = the total number of minutes of Service Availability (as defined above), and

Y = (the Total number of minutes in the calendar month) – (the Total # of minutes of downtime from Scheduled Maintenance and Emergency Maintenance which shall not exceed thirty (30) minutes).

If the Service Availability is less than 99.999%, Cisco will provide You with a Service Credit for the month in which the failure to meet the Availability SLA has occurred. The Service Credit will be calculated in accordance with the table below.

% of Service Availability per Calendar Month	Service Credit
< 99.999%	20%
< 99.0%	40%
< 98.0%	100%

4. Data Protection

Cisco's data protection obligations are set forth in the Agreement. Additionally, the Cisco CES and CRES, APP and DMP Privacy Data Sheet(s) (available here) supplement the Cisco Privacy Statement and describe the Personal Data that Cisco collects and processes as part of the delivery of the Cloud Services.

If You use the Cloud Service in China, You (1) acknowledge that You are the entity causing data to be transferred outside of China in connection with your use of the Cloud Service, and (2) acknowledge Your obligation to comply with China's cybersecurity requirements and other requirements related to the cross border transfer of data.

If You use the Cloud Service in Russia, You acknowledge that You are the data operator as defined under Russian law for purposes of Your users' personal data that is collected and processed in connection with the Cloud Service.

5. Support & Maintenance.

The Cloud Services include online support and phone support. Cisco will respond as set forth in the table below and may require information from you to resolve service issues. You agree to provide the information requested and understand that a delay in providing the information to Cisco may delay resolution and response time.

Online Support allows access for support and troubleshooting via online tools, email and web case submission only. No telephone access is provided. Case severity or escalation guidelines are not applicable. Cisco will respond to a submitted case no later than the next business day during standard business hours.

Phone Support provides Cisco Technical Assistance Center (TAC) access 24 hours per day, 7 days per week to assist by telephone, or web case submission and online tools with use and troubleshooting issues. Cisco will respond within one (1) hour for Severity 1 and 2 calls received. For Severity 3 and 4 calls, Cisco will respond no later than the next business day.

You will also have access to Cisco.com, which provides helpful technical and general information about Cisco products, as well as access to Cisco's on-line knowledge base and forums. Please note that access restrictions identified by Cisco from time to time may apply.

The below table outlines Cisco's response objectives based on case severity. Cisco may adjust assigned case severity to align with the Severity definitions below.

Software Support Service	Technical Support Coverage	Response Time Objective for Case Severity 1 or 2	Response Time Objective for Case Severity 3 or 4
Basic with Phone Support	24x7 via Phone & Web	Response within 1 hour	Response within next Business Day
Basic with Online Support	Web	Response to all cases within next Business Day during Standard Business Hours	

The following definitions apply to this Section.

Response time means the time between case submission in the case management system to support engineer contact.

Severity 1 means the Cloud Service is unavailable or down or there is a critical impact to a significant impact to Case Submitter's business operation. Case Submitter and Cisco both will commit full-time resources to resolve the situation.

Severity 2 means the Cloud Service is degraded or significant aspects of Case Submitter's business operation are negatively impacted by unacceptable software performance. Case Submitter and Cisco both will commit full-time resources during Standard Business Hours to resolve the situation.

Severity 3 means the Cloud Service is impaired, although most business operations remain functional. Case Submitter and Cisco both are willing to commit resources during Standard Business Hours to resolve the situation.

Severity 4 means minor intermittent functionality or performance issue, or information is required on the Cloud Service. There is little or no impact to Case Submitter's business operation. Case Submitter and Cisco both are willing to provide resources during Standard Business Hours to provide assistance or information as requested.

Business Day means the generally accepted days of operation per week within the relevant region where the Cloud Services will be performed, excluding local holidays as observed by Cisco.

Local Time means Central European Time for support provided in Europe, Middle East and Africa, Australia's Eastern Standard Time for support provided in Australia, Japan's Standard Time for support provided in Japan and Pacific Standard Time for support provided in all other locations.

Standard Business Hours means 8am to 5pm Local Time at the location of the respective Cisco TAC, on Business Days, for the handling of TAC calls.

Your access to and use of the Cloud Services may be suspended for the duration of unanticipated or unscheduled downtime, including as a result of catastrophic events, external denial of service or other security breach, or operational incidents.

Definitions.

Cisco Threat Content means any Cisco provided threat intelligence, content or data including, but not limited to, rules, signatures, threat data feeds or suspicious URLs and IP address data feeds for use with any Cisco product or service.

Telemetry Data means Telemetry Data as defined in the Agreement and for the avoidance of doubt, includes without limitation: netflow data; origin and nature of malware; network security policies; the types of software or applications installed on a network or an endpoint; information related to the usage, origin of use, traffic patterns and behavior of the users of a network or cloud service; any geolocation data; or network traffic data such as cookies, web logs, web beacons, and other similar applications.

Users means the employees, contractors and other agents authorized by You to use email services via Your email and Internet services.