cywestEdge™

# cywestEdge Cloud Hosting and Delivery Policies

October 2022

StrongBox™

Ticketsys™

SIMPLE™

Cywest Communications, Inc.

# Table of Contents


OVERVIEW ..... 4

1. CYWESTEDGE CLOUD SECURITY POLICY ..... 5

1.1 cywestEdge Information Security Practices - General ..... 5
1.2 Physical Security Safeguards ..... 5
1.3 System Access Controls ..... 6
1.4 Data Access Controls ..... 6
1.5 User Encryption for External Connections ..... 6
1.6 Input Control ..... 6
1.7 Data and Network Segregation ..... 7
1.8 Confidentiality ..... 7
1.9 Asset Management ..... 7
1.10 cywestEdge Internal Information Security Policies ..... 7
1.11 Internal Security Reviews and Enforcement ..... 7
1.12 External Reviews ..... 7
1.13 Security Logs ..... 8
1.14 Other Customer Security Related Obligations ..... 8

2. CYWESTEDGE CLOUD SERVICE CONTINUITY POLICY ..... 9

2.1 cywestEdge Cloud Services High Availability Strategy ..... 9
2.2 cywestEdge Cloud Services Backup Strategy ..... 9

3. CYWESTEDGE CLOUD SERVICE LEVEL AGREEMENT ..... 9

3.1 Hours of Operation ..... 9
3.2 Service Availability ..... 10
3.2.1 Measurement of Availability ..... 10
3.2.2 Reporting of Availability ..... 10
3.2.3 Service Credits ..... 10
3.3 Definition of Unplanned Downtime ..... 11
3.4 Monitoring ..... 11
3.4.1 Monitored Components ..... 11
3.4.2 Customer Monitoring & Testing Tools ..... 11

4. CYWESTEDGE CLOUD CHANGE MANAGEMENT POLICY ..... 12

4.1 cywestEdge Cloud Change Management and Maintenance ..... 12
4.1.1 Emergency Maintenance ..... 12
4.1.2 Major Maintenance Changes ..... 13
4.1.3 Data Center Migrations ..... 13

5. CYWESTEDGE CLOUD SUPPORT POLICY ..... 13

5.1 cywestEdge Cloud Support Terms ..... 13
5.1.1 Support Fees ..... 13

5.1.2 Support Period ..... 13
5.1.3 Technical Contacts ..... 13
5.1.4 cywestEdge Cloud Support ..... 14
5.2 cywestEdge Cloud Customer Support Systems ..... 14
5.2.1 cywestEdge Cloud Customer Support Portal (TicketSys) ..... 14
5.2.2 Customer Authorized Users ..... 14
5.3 Severity Definitions ..... 14
5.4 Change to Service Request Severity Level ..... 15
5.4.1 Initial Severity Level ..... 15
5.4.2 Downgrade of Service Request Levels ..... 15
5.4.3 Upgrade of Service Request Levels ..... 15
5.4.4 Adherence to Severity Level Definitions ..... 15
5.5 Service Request Escalation ..... 15
6. CYWESTEDGE CLOUD SUSPENSION AND TERMINATION POLICY ..... 16
6.1 Termination of cywestEdge Cloud Services ..... 16
6.2 Termination of Pilot Environments ..... 16

## OVERVIEW

These cywestEdge Cloud Hosting and Delivery Policies (these “Delivery Policies”) describe the cywestEdge Cloud Services ordered by You. These Delivery Policies may reference other cywestEdge Cloud policy documents; any reference to "Customer" in these Delivery Policies or in such other policy documents shall be deemed to refer to “You” as defined in Your order.

References in these Delivery Policies to a Cloud Services’ “data center region” refers to the geographic region listed in Your order for such Services or, if applicable, the geographic region that You have selected when activating the production instance of such Services.

With respect to Your ordered cywestEdge Cloud Services, Your Content will be stored in the data center region applicable to such services. cywestEdge may replicate Your Content to other locations within the applicable data center region in support of data durability. Capitalized terms that are not otherwise defined in these Delivery Policies shall have the meaning ascribed to them in the cywestEdge agreement, Your order or the policy, as applicable. The cywestEdge Cloud Hosting and Delivery Policies are generally updated on a biannual basis.

Your order or cywestEdge’s Service Specifications (such as cywestEdge Cloud and ISVN Service Level Agreement Policy) may include additional details or exceptions related to specific cywestEdge Cloud Services. The *cywestEdge Cloud and ISVN Service Level Agreement Policy* documentation for cywestEdge Cloud Services are available at edge.cywest.com

cywestEdge Cloud Services are provided under the terms of the cywestEdge agreement, Your order, and Service Specifications applicable to such services. cywestEdge’s delivery of the cywestEdge Cloud Services is conditioned on Your and Your users’ compliance with Your obligations and responsibilities defined in such documents and incorporated policies. These Delivery Policies, and the documents referenced herein, are subject to change at cywestEdge's discretion; however, cywestEdge policy changes will not result in a material reduction in the level of performance, functionality, security, or availability of the cywestEdge Cloud Services provided during the Services Period of Your order.

cywestEdge Cloud Services are deployed at data centers or third-party infrastructure service providers retained by cywestEdge. cywestEdge ISVN Services may incorporate components (e.g. Edge devices, routers or switches) that are deployed at Your data center or at a third-party data center retained by You. You may purchase these services standalone or they may be deployed as the underlying platform for other cywestEdge Cloud Services. For cywestEdge ISVN Services, cywestEdge will deliver to Your data center or branch office certain hardware components, including gateway equipment, needed by cywestEdge to operate these services. You are responsible for providing adequate space, power, and cooling to deploy the cywestEdge hardware (including gateway equipment) and allowing cywestEdge building access for network connectivity to cywestEdge Cloud Operations to access the services. cywestEdge is solely responsible for maintenance of the cywestEdge hardware components (including gateway equipment) and any network connectivity cywestEdge deploys at Your site.

Service Description.

# 1. CYWESTEDGE CLOUD SECURITY POLICY

## 1.1 cywestEdge Information Security Practices - General

cywestEdge has adopted security controls and practices for cywestEdge Cloud Services that are designed to protect the confidentiality, integrity, and availability of Your Content that is hosted by cywestEdge in Your cywestEdge Cloud Services environment and to protect Your Content from any unauthorized processing activities such as loss or unlawful destruction of data. cywestEdge continually works to strengthen and improve those security controls and practices.

cywestEdge Cloud information security practices establish and govern areas of security applicable to cywestEdge Cloud Services and to Your use of those cywestEdge Cloud Services. cywestEdge personnel (including employees, contractors, and temporary employees) are subject to the cywestEdge information security practices and any additional policies that govern their employment or the services they provide to cywestEdge.

cywestEdge takes a holistic approach to information security, implementing a multilayered defense security strategy where network, operating system, database, and software security practices and procedures complement one another with strong internal controls, governance, and oversight.

For those cywestEdge Cloud Services which enable You to configure Your security posture, unless otherwise specified, You are responsible for configuring, operating, maintaining, and securing the operating systems and other associated software of these select cywestEdge Cloud Services (including Your Content) that is not provided by cywestEdge. You are responsible for maintaining appropriate security, protection, and backup of Your Content, which may include the use of encryption technology to protect Your Content from unauthorized access and the routine archiving of Your Content.

## 1.2 Physical Security Safeguards

cywestEdge employs measures designed to prevent unauthorized persons from gaining access to computing facilities in which Your Content is hosted such as the use of security personnel, secured buildings, and designated data center premises. cywestEdge provides secured computing facilities for both office locations and production cloud infrastructure. Common controls between office locations and cywestEdge controlled co-locations/data centers may include, for example:

- Physical access requires authorization and is monitored. Under no circumstances will unauthorized personnel, or third-party contractors not retained by cywestEdge be allowed into cywestEdge data center areas containing cloud compute, memory, data storage, network, or power resources and/or equipment. This includes, but is not limited to third-party auditors not directly retained by cywestEdge.

- All employees and visitors must visibly wear official identification while onsite
- Visitors must sign a visitor's register and be escorted and/or observed while onsite
- Possession of keys/access cards and the ability to access the locations is monitored. Staff leaving cywestEdge employment must return keys/cards

## 1.3 System Access Controls

cywestEdge may, depending upon the particular Cloud Services ordered, apply among others the following controls: authentication via passwords and/or multi-factor authentication, documented authorization and change management processes, and logging of access. All remote access to the cywestEdge Cloud Network by cywestEdge personnel that have access to Your Content is restricted through the use of a Virtual Private Network which utilizes multi-factor authentication.

For Cloud Services hosted at cywestEdge: (i) log-ins to Cloud Services environments are logged and (ii) logical access to the data centers is restricted and protected.

## 1.4 Data Access Controls

For service components managed by cywestEdge, cywestEdge's access to Your Content is restricted to authorized staff.

With respect to cywestEdge personnel accessing the Services environment for the Cloud Services (including Your Content residing in the Cloud Services), cywestEdge enforces Role Based Access Controls (RBAC) and employs the access management principles of "need to know", "least privilege" and "segregation of duties." In addition, cywestEdge provides a mechanism by which You control Your access to Your Cloud Services environment and to Your Content by Your authorized staff.

## 1.5 User Encryption for External Connections

Your access to cywestEdge Cloud Services is through a secure communication protocol provided by cywestEdge. If access is through a Transport Layer Security (TLS) enabled connection, that connection is negotiated for at least 128 bit encryption. The private key used to generate the cipher key is at least 2048 bits. TLS is implemented or configurable for all web-based TLS-certified applications deployed at cywestEdge. It is recommended that the latest available browsers certified for cywestEdge programs, which are compatible with higher cipher strengths and have improved security, be utilized for connecting to web enabled programs.

## 1.6 Input Control

The source of Your Content is under Your control and Your responsibility, and integrating Your Content into the Cloud Services environment, is managed by You.

## 1.7 Data and Network Segregation

Your Content is logically or physically segregated from the content of other customers hosted in the cywestEdge Cloud Services environments. All cywestEdge Customer networks are segregated from cywestEdge's Corporate networks.

## 1.8 Confidentiality

cywestEdge personnel that may have access to Your Content are subject to confidentiality agreements. All cywestEdge personnel that have access to Your Content have gone through rigorous background checks.

## 1.9 Asset Management

cywestEdge is responsible for the protection and inventory of cywestEdge's Cloud Services assets. The responsibilities may include reviewing and authorizing access requests to those who have a business need and maintaining an inventory of assets.

You are responsible for the assets You control that utilize or integrate with the cywestEdge Cloud services, including: determining the appropriate information classification for Your Content, and whether the documented controls provided by cywestEdge Cloud Services are appropriate for Your Content. You must have or obtain any required consents or other legal basis related to the collection and use of information provided by data subjects, including any such consents or other legal basis necessary for cywestEdge to provide the Cloud Services.

## 1.10 cywestEdge Internal Information Security Policies

cywestEdge Cloud information security policies establish and govern areas of security applicable to cywestEdge Cloud Services and to Your use of cywestEdge Cloud Services. cywestEdge personnel are subject to the policies that govern their employment or the services they provide to cywestEdge.

## 1.11 Internal Security Reviews and Enforcement

cywestEdge employs internal processes for regularly testing, assessing, evaluating and maintaining the effectiveness of the technical and organizational security measures described in this section.

## 1.12 External Reviews

cywestEdge may conduct independent reviews of Cloud Services utilizing third parties in the following areas (the scope of any such reviews may vary by service and country):

- SOC 1 (based on Statement on Standards for Attestation Engagements (SSAE) No 18) and/or SOC 2 reports
- Other independent third-party security testing to review the effectiveness of administrative and technical controls

## 1.13 Security Logs

Logs are generated for security-relevant activities on operating systems. Systems are configured to log default security activities, access to information or programs, system events such as alerts, console messages, and system errors. cywestEdge reviews logs for forensic purposes and incidents; identified anomalous activities feed into the incident management process. Security logs are stored within the cywestEdge TicketSys Cluster system (or equivalent system) in a native, unaltered format and retained in accordance with cywestEdge's internal policies. Such logs may be retained online for a minimum of 1 year, depending on the monitoring objectives, or as otherwise required by an applicable regulatory framework.

These logs are retained and used by cywestEdge for internal security operations for Cloud Services.

## 1.14 Other Customer Security Related Obligations

You are responsible for:

- Implementing Your own comprehensive system of security and operational policies, standards and procedures, according to Your risk-based assessments and business requirements
- Ensuring that end-user devices meet web browser requirements and minimum network bandwidth requirements for access to the cywestEdge Cloud Services
- Managing client device security controls, so that antivirus and malware checks are performed on data or files before importing or uploading data into the cywestEdge Cloud Services
- Maintaining Customer-managed accounts according to Your policies and security best practices
- Additionally, for cywestEdge ISVN Services, You are responsible for the following:
    - Adequate physical and network security
    - Security monitoring to reduce the risk of real time threats and prevent unauthorized access to Your cywestEdge Cloud Services from Your networks; this includes intrusion detection systems, access controls, firewalls and any other network monitoring, and any management tools managed by You.

# 2. CYWESTEDGE CLOUD SERVICE CONTINUITY POLICY

## 2.1 cywestEdge Cloud Services High Availability Strategy

cywestEdge deploys the cywestEdge Cloud Services on resilient computing infrastructure designed to maintain service availability and continuity in the case of an incident affecting the services. Data centers retained by cywestEdge to host cywestEdge Cloud Services have component and power redundancy with backup generators in place, and cywestEdge may incorporate redundancy in one or more layers, including network infrastructure, program servers, database servers, and/or storage.

## 2.2 cywestEdge Cloud Services Backup Strategy

cywestEdge does not make backups of Your Content in your production environment of the cywestEdge Cloud Services outside of any Agreement for such. Backups are stored at the primary site used to provide the cywestEdge Cloud Services, and may also be stored at an alternate location for retention purposes. Under a valid Agreement, a production backup is typically retained online or offline for a period up to 30 days after the date that the backup is made. cywestEdge typically does not update, insert, delete or restore Your data on Your behalf. However, on an exception basis and subject to written approval, cywestEdge may assist You to restore data which You may have lost as a result of Your own actions. Data that is replicated for Disaster Recovery (DR) purposes can not be used for data restoration, although DR systems may be spun up and placed into production.

For cywestEdge Cloud Services which enable You to configure backups in accordance with Your own policies, You are responsible for performing backups and restores of Your data, non-cywestEdge software, and any cywestEdge software that is not provided by cywestEdge as part of these services. Additionally, You are encouraged to develop a business continuity plan to ensure continuity of Your own operations in the event of a disaster.

# 3. CYWESTEDGE CLOUD SERVICE LEVEL AGREEMENT

## 3.1 Hours of Operation

The cywestEdge Cloud Services are designed to be available 24 hours a day, 7 days a week, 365 days a year, except during maintenance periods, technology upgrades and as otherwise set forth in the cywestEdge agreement, Your order and this *cywestEdge Cloud Service Level Agreement*.

## 3.2 Service Availability

Commencing at cywestEdge's activation of Your production cywestEdge Cloud Service, cywestEdge works to meet the Target Service Availability Level, or Target Service Uptime of 99.9%. This is in accordance with the terms set forth in the *cywestEdge Cloud and ISVN Service Level Agreement Policy* documentation for the applicable cywestEdge Cloud Service (or such other Target Service Availability Level or Target Service Uptime specified by cywestEdge for the applicable cywestEdge Cloud Service in such documentation).

The foregoing is contingent on Your adherence to cywestEdge's recommended minimum technical configuration requirements for accessing and using the cywestEdge Cloud Services from Your network infrastructure and Your user work stations as set forth in the Program Documentation for the applicable cywestEdge Cloud Services.

### 3.2.1 Measurement of Availability

Following the end of each calendar month of the applicable Services Period, cywestEdge measures the Service Availability Level or Service Uptime over the immediately preceding month by dividing the difference between the total number of minutes in the monthly measurement period and any Unplanned Downtime (as defined below) by the total number of minutes in the measurement period, and multiplying the result by 100 to reach a percent figure.

### 3.2.2 Reporting of Availability

cywestEdge Ticketsys and monitoring systems measure metrics on the Service Availability Level for cywestEdge Cloud Services that You purchased under Your order. cywestEdge will provide metrics on the Service Availability Level upon receipt of a Service Request submitted by You to cywestEdge requesting the metrics.

### 3.2.3 Service Credits

You may receive Service Credits in the event that the Target Service Availability Level or Target Service Uptime for cywestEdge Cloud Services that You purchased under Your order is below the defined Target Service Availability Level or Target Service Uptime applicable to such Services. Service Credits are defined in the *cywestEdge Cloud and ISVN Service Level Agreement Policy* documentation or Service Description applicable to Your purchased cywestEdge Cloud Services. Notwithstanding the provisions of this section, if Your order with cywestEdge or Service Specifications applicable to your order for a particular cywestEdge Cloud Service provides a right to receive a higher amount of Service Credits, then You may receive the Service Credits under the provision which provides for the highest amount of Service Credits to You, but You may not recover Service Credits under multiple provisions for the same event.

## 3.3 Definition of Unplanned Downtime

"Unplanned Downtime": cywestEdge Services are deployed in resilient computing facilities with resilient infrastructure, redundant network connections, and power at each hosting facility. "Unplanned Downtime" means any time during which a problem with the cywestEdge Services prevents Your connectivity. Unplanned Downtime does not include any time during which the cywestEdge Services or any cywestEdge Services component are not available due to: (i) scheduled maintenance, (ii) circumstances outside of cywestEdge's control and other force majeure events (e.g., outages initiated at Your request, outages caused by non- cywestEdge infrastructure such as electrical, network, telecommunication, or other connectivity equipment, security attacks, natural disasters, or political events), (iii) any actions or inactions of You, Your Users or any third party (other than any cywestEdge agents and contractors who cywestEdge has engaged to perform the applicable cywestEdge Services) or (iv) any suspension by cywestEdge permitted under Your cywestEdge agreement or Your order. In addition, with respect to cywestEdge Services that originate from Your data center or branch office, Unplanned Downtime also does not include downtime or other unavailability (i) of Your data center or branch office (e.g., due to maintenance) or (ii) occurring outside the on-site hours defined under Your order for cywestEdge personnel at Your data center or branch office location.

## 3.4 Monitoring

cywestEdge uses a variety of software tools to monitor the availability and performance of the cywestEdge Cloud Services and the operation of infrastructure and network components. cywestEdge does not monitor, or address deviations experienced by any non-cywestEdge managed components used by You in the cywestEdge Cloud Services, such as non-cywestEdge applications.

### 3.4.1 Monitored Components

cywestEdge monitors the hardware that supports the cywestEdge Cloud Services, and currently generates alerts for monitored components, such as CPU, memory, storage, database and other components. cywestEdge Cloud Operations staff monitors alerts associated with deviations to cywestEdge defined thresholds, and follows standard operating procedures to investigate and resolve underlying issues.

### 3.4.2 Customer Monitoring & Testing Tools

All monitoring of Customer assets within a vDC are the responsibility of the Customer.

cywestEdge permits You to conduct limited functional testing for cywestEdge Cloud Services in Your test environment. cywestEdge reserves the right to remove or disable access to any tools or technologies that violate the guidelines applicable to cywestEdge Acceptable Use Policy, without any liability to You.

# 4. CYWESTEDGE CLOUD CHANGE MANAGEMENT POLICY

## 4.1 cywestEdge Cloud Change Management and Maintenance

cywestEdge Cloud Operations performs changes to cloud hardware infrastructure, operating software, product software, and supporting application software that is provided by cywestEdge as part of the cywestEdge Cloud Services, to maintain operational stability, availability, security, performance, and currency of the cywestEdge Cloud Services. cywestEdge follows formal change management procedures to review, test, and approve changes prior to application in the production service.

Changes made through change management procedures include system and service maintenance activities, upgrades and updates, and customer specific changes. cywestEdge Cloud Services change management procedures are designed to minimize service interruption during the implementation of changes.

cywestEdge reserves specific maintenance periods for changes that may require the cywestEdge Cloud Services to be unavailable during the maintenance period. cywestEdge works to ensure that change management procedures are conducted during scheduled maintenance windows, while taking into consideration low traffic periods and geographical requirements.

cywestEdge will provide prior notice of any maintenance periods scheduled. For Customer-specific changes and upgrades, where feasible, cywestEdge will coordinate the maintenance periods with You.

For changes that are expected to cause service interruption, the durations of the maintenance periods for planned maintenance are not included in the calculation of Unplanned Downtime minutes in the monthly measurement period for Service Availability Level (see the *cywestEdge Cloud and ISVN Service Level Agreement Policy*). cywestEdge uses commercially reasonable efforts to minimize the use of these reserved maintenance periods and to minimize the duration of maintenance events that cause service interruptions.

For cywestEdge Cloud Services which enable You to perform maintenance activities, You are responsible for configuring and maintaining the operating systems and other associated software.

### 4.1.1 Emergency Maintenance

cywestEdge may be required to execute emergency maintenance in order to protect the security, performance, availability, or stability of the cywestEdge Cloud Services. Emergency maintenance is required to address an exigent situation (e.g., a hardware failure of the infrastructure underlying such Service) with the Service or cywestEdge infrastructure that cannot be addressed except on an emergency basis. cywestEdge works to minimize the use of emergency maintenance, and to the extent reasonable under the circumstances as determined by cywestEdge, will work to provide 24 hours prior notice for any emergency maintenance requiring a service interruption.

### 4.1.2 Major Maintenance Changes

To help ensure continuous stability, availability, security and performance of cywestEdge Cloud Services, cywestEdge reserves the right to perform major changes to its hardware infrastructure, operating software, applications software and supporting application software under its control. Each such major change event is considered scheduled maintenance and may cause the cywestEdge Cloud Services to be unavailable. Each such event is targeted to occur at the same time as the scheduled maintenance period. cywestEdge will work to provide no less than 30 days prior notice of a major change event.

### 4.1.3 Data Center Migrations

cywestEdge may migrate Your cywestEdge Cloud Services deployed in data centers retained by cywestEdge between production data centers in the same data center region as deemed necessary by cywestEdge or in the case of disaster recovery. For data center migrations for purposes other than disaster recovery, cywestEdge will provide a minimum of 30 days notice to You.

## 5. CYWESTEDGE CLOUD SUPPORT POLICY

The support described in this *cywestEdge Cloud Support Policy* applies only for cywestEdge Cloud Services, and is provided by cywestEdge as part of such cywestEdge Cloud Services under Your order. cywestEdge may make available, and You may order for additional fees, additional support service offerings made available by cywestEdge for the cywestEdge Cloud Services.

## 5.1 cywestEdge Cloud Support Terms

### 5.1.1 Support Fees

The fees paid by You for the cywestEdge Cloud Services under Your order include the support described in any cywestEdge Support Agreement negotiated. Additional fees are applicable for additional cywestEdge support services offerings purchased by You, rates can be found at ticketsys.cywest.com.

### 5.1.2 Support Period

cywestEdge Cloud support becomes available upon the service start date and ends upon the expiration or termination of the Services (the "support period"). cywestEdge is not obligated to provide the support described in this cywestEdge Cloud Support Policy beyond the end of the support period.

### 5.1.3 Technical Contacts

Your technical contacts are the sole liaisons between You and cywestEdge for cywestEdge support for cywestEdge Cloud Services. Those technical contacts must have, at a minimum, initial basic service training and, as needed, supplemental training appropriate for specific role or implementation phase, specialized service/product usage, and migration. Your technical contacts

must be knowledgeable about the cywestEdge Cloud Services in order to help resolve system issues and to assist cywestEdge in analyzing and resolving service requests. When submitting a service request, Your technical contact should have a baseline understanding of the problem being encountered and an ability to reproduce the problem in order to assist cywestEdge in diagnosing and triaging the problem. To avoid interruptions in cywestEdge support for cywestEdge Cloud Services, You must notify cywestEdge whenever technical contact responsibilities are transferred to another individual.

#### 5.1.4 cywestEdge Cloud Support

cywestEdge support for cywestEdge Cloud Services consists of:

- Diagnoses of problems or issues with the cywestEdge Cloud Services
- Reasonable commercial efforts to resolve reported and verifiable errors in the cywestEdge Cloud Services so that those cywestEdge Cloud Services perform in all material respects.
- Assistance with technical service requests 24 hours per day, 7 days a week
- 24 x 7 access to a Cloud Customer Support Portal (TicketSys) designated by cywestEdge.

### 5.2 cywestEdge Cloud Customer Support Systems

#### 5.2.1 cywestEdge Cloud Customer Support Portal (TicketSys)

cywestEdge provides support for the cywestEdge Cloud Service acquired by You through the Cloud Customer Support Portal referred to as TicketSys. Access to TicketSys is governed by the Terms of Use posted on the designated support web site, which are subject to change. Where applicable, TicketSys provides support details to Your designated technical contacts to enable use of cywestEdge support for cywestEdge Cloud Services. All service notifications and alerts relevant to Your cywestEdge Cloud Service are posted on this portal.

#### 5.2.2 Customer Authorized Users

Access to TicketSys is limited to Your designated technical contacts and other authorized users of the cywestEdge Cloud Services. All authorized users have the implied authority and authorization to agree to the Support Fees as declared in Subsection 5.1.1 of these Delivery Policies.

### 5.3 Severity Definitions

Service requests for cywestEdge Cloud Services may be submitted by Your designated technical contacts via TicketSys noted above. The severity level of a service request submitted by You is selected by both You and cywestEdge.

## 5.4 Change to Service Request Severity Level

### 5.4.1 Initial Severity Level

cywestEdge's initial focus, upon acceptance of a service request, will be to resolve the issues underlying the service request. The severity level of a service request may be adjusted as described below.

### 5.4.2 Downgrade of Service Request Levels

If, during the service request process, the issue no longer warrants the severity level currently assigned based on its current impact on the production operation of the applicable cywestEdge Cloud Service, then the severity level will be downgraded to the severity level that most appropriately reflects its current impact.

### 5.4.3 Upgrade of Service Request Levels

If, during the service request process, the issue warrants the assignment of a higher severity level than that currently assigned based on the current impact on the production operation of the applicable cywestEdge Cloud Service, then the severity level will be upgraded to the severity level that most appropriately reflects its current impact.

### 5.4.4 Adherence to Severity Level Definitions

You shall ensure that the assignment and adjustment of any severity level designation is accurate based on the current impact on the production operation of the applicable cywestEdge Cloud Service. You acknowledge that cywestEdge is not responsible for any failure to meet performance standards caused by Your misuse or mis-assignment of severity level designations.

## 5.5 Service Request Escalation

For service requests that are escalated, cywestEdge Ticketsys provides a facility for requesting support escalation. If the issue underlying the service request continues to remain unresolved, You may use the Ticketsys escalation facility to escalate to the next level within cywestEdge as required. To facilitate the resolution of an escalated service request, You are required to provide contacts within Your organization that are at the same level as that within cywestEdge to which the service request has been escalated.

# 6. CYWESTEDGE CLOUD SUSPENSION AND TERMINATION POLICY

## 6.1 Termination of cywestEdge Cloud Services

For a period of 60 days upon termination of the cywestEdge Cloud Services, cywestEdge will make available, via secure protocols and in a structured, machine-readable format, Your Content residing in the production Cloud Services environment, or keep the service system accessible, for the purpose of data retrieval by You.

For free trials of Cloud Services, cywestEdge will make Your Content available for a period of 30 days following termination of the trial. During this retrieval period, cywestEdge's Cloud Service Level Agreement does not apply and the service system may not be used for any production activities. cywestEdge has no obligation to retain Your Content after this retrieval period.

If You need assistance from cywestEdge to obtain access to or copies of Your Content, You must create a service request in TicketSys applicable to the service.

Data retrieval and any related assistance by cywestEdge is not applicable for cywestEdge Cloud Services that do not store Your Content. You are responsible for ensuring that if those cywestEdge Cloud Services are dependent on separate cywestEdge Cloud Services (such as Storage Cloud Service or Database Cloud Services) for the storage of data, those separate cywestEdge Cloud Services must have a valid duration through the end of the terminating cywestEdge Cloud Service to enable data retrieval, or for otherwise taking appropriate action to back up or otherwise store separately Your Content while the Production Cloud Services environment is still active prior to termination.

Following expiry of the retrieval period, cywestEdge will delete Your Content from the cywestEdge Cloud Services environments (unless otherwise required by applicable law).

For cywestEdge ISVN Services, You must make available for retrieval by cywestEdge any cywestEdge ISVN-related hardware components (including the gateway equipment) provided by cywestEdge in good working order and the same condition as at the start of the cywestEdge ISVN Services subject to reasonable wear and tear for appropriate use.

## 6.2 Termination of Pilot Environments

This *cywestEdge Cloud Suspension and Termination Policy* applies to production pilots of cywestEdge Cloud Services. Production pilots are not available for all cywestEdge Cloud Services.

## CONNECT WITH US

Call +1.949.544-1454 or visit edge.cywest.com.

www.linkedin.com/company/cywest-communications/



cywestEdge Cloud and ISVN Services Policy Document
October 2022