CenturyLink Service Guide

Web Application Firewall 1.0

Web Application Firewall 1.0 CPE

This CenturyLink Service Guide ("SG") sets forth a description of Web Application Firewall 1.0 ("Service") and Web Application Firewall 1.0 CPE ("Service") offerings by CenturyLink, including technical details and additional requirements, if any. This SG is subject to and incorporated into the Agreement and Service Schedule between the parties. The specific details of the Service ordered by Customer will be set forth on the relevant Service Order. For avoidance of doubt, any references in the Agreement, Schedules, or Service Orders to SSG, shall mean SG.

Version	Previous	Section Modified	Date
SEC-SG-WebApplicationFirewall-20180315	SEC-20141204-SG-WebApplicationFirewallServiceForms	Incident Response	March 15, 2018

Table of Contents

Service Description Web Application Firewall 1.0

1. **Service Description:** Web Application Firewall 1.0 (WAF) is a CenturyLink provided service (the "Service"). The standard features of the Service consist of the, installation, configuration, administration, monitoring, maintenance and support for the CenturyLink provided components listed in Section 1.1. Customer must execute a Security Service Schedule to purchase the Services. The Service Level Agreement (SLA) associated with this Service is located in Appendix A. CenturyLink does not represent or warrant that the CenturyLink Equipment or the Service will be uninterrupted or error-free; will detect or generate an alert for every security event that may be recorded in Customer logs, or meets any particular data security standard. This Service can be provided in a CenturyLink managed environment or Customer Premises ("CPE"). Unless specifically noted, all Service components, tasks, requirements, etc. listed are for both options.

    1.1. **Service Components**

        1.1.1. **CPE and CenturyLink Managed Environment**

            1.1.1.1. **Appliance:** Imperva ("Supplier) firewall appliance. Customer chooses the performance tier defined in Table 2.0 Performance Tiers. CenturyLink will configure the Service to support up to 10 individual web servers (or 10 virtual IPs). Support for more than 10 web servers or virtual IPs is at the discretion of CenturyLink and requires additional Customer fees.

            1.1.1.2. **Design** / **Planning:** CenturyLink will provide design consultation to include suggestions on sizing the correct WAF appliance, taking into account Customer throughput to protected web servers, the number of protected web servers and applications in addition to anticipated infrastructure growth and scale projections. CenturyLink WAF service is supported as a layer 2 bridge (see Definition), deployed in a failover configuration using the Imperva appliance onboard physical interfaces joined as 'bridge pairs'.

            1.1.1.3. **Incident Response ("IR"):** Incident Response ("IR") is performed as a function of the WAF event investigation process. Only IR activities that are associated with a WAF event are included in the Service. Incident Response as part of the WAF event investigation process will consist of the CenturyLink Security Operation Center performing an analysis of the detected event. The WAF analysis may include the use of both internal and commercial tools in determining the event impact to a specific Customer environment. Review of system logs, system statistics and files from live systems may be used in the event analysis process, (only for CenturyLink managed security service devices). The result of the event analysis could result in the following Customer recommended actions: Suggestions to perform host application hardening, recovery operations for Managed Hosting services or Customer host computer or suggestion to perform modification of firewall and IDS/IPS configuration rules.

        1.1.2. **CenturyLink Managed Environment Only**

            1.1.2.1. **Connectivity:** One connection to the CenturyLink internal management network to allow for out-of-band device administration.

    1.2. **Installation:** CenturyLink will provide installation tasks marked with an "X" in the CenturyLink column in Table 1.0 Roles and Responsibilities Web Application Firewall 1.0.

        1.2.1. **Billing Cycle**: The WAF service will be considered installed for billing following a five-day burn-in cycle and any follow-up conversations with Customer to make any required adjustments. Upon approval from Customer, the device will be set to blocking status and billing will commence.

    1.3. **Configuration:** CenturyLink will provide configuration tasks marked with an "X" in the CenturyLink column in Table 1.0 Roles and Responsibilities Web Application Firewall 1.0.

        1.3.1. **Backup**: CenturyLink will provide WAF configuration data backup whenever there is a configuration change – and off-site storage of the current configuration for the time period in which Customer maintains the Service with CenturyLink.

        1.3.2. **Simulation Mode**: CenturyLink will configure the WAF in monitoring or simulation mode, which alerts in the event of a suspected attack. Alerting will be categorized as high, medium or low. High priority alerts will be reviewed by CenturyLink and medium and low alerts logged. Alerts will be reviewed with

Customer during scheduled review sessions.

1.4. **Administration**: CenturyLink will provide administration tasks marked with an "X" in the CenturyLink column in Table 1.0 Roles and Responsibilities Web Application Firewall 1.0.

1.4.1. **System Administration:** In order to maintain configuration consistency and accountability for changes, all system administration and WAF passwords will be managed by CenturyLink. Customer will not have access to firewall passwords or be able to make direct changes to WAF configurations. Customer must request changes by first submitting a ticket or calling the CenturyLink Service Center. Customer must provide complete authentication credentials to the CenturyLink Response Center when requesting changes. See the Response Times in Table 3.0 for more information on response times.

1.4.2. **Reporting:** Reporting is provided on the customer portal and includes a summary of blocked and non-blocked connections, top 20 URLs and unusual response codes. Raw firewall logs files (i.e. thread logs will be retained online for 30 days). Reports have daily, weekly and monthly views.

1.5. **Monitoring:** CenturyLink will provide monitoring tasks marked with an "X" in the CenturyLink column in Table 1.0 Roles and Responsibilities Web Application Firewall 1.0.

1.5.1. **WAF Traffic Activity**: Customer can view traffic activity in the customer portal.

1.5.2. **ICMP Monitoring:** (e.g., ping) Monitoring of the WAF to determine system availability (24X7). In the event that the firewall fails to respond, CenturyLink will notify Customer via phone and/or email and initiate corrective action.

1.5.3. **CPU Threshold:** In the event that the firewall exceeds 80% CPU load for a sustained 5-minute time period, CenturyLink will investigate to confirm that WAF is functioning properly.

1.5.4. **Memory Usage:** In the event that the firewall exceeds 80% memory usage for a sustained 5-minute time period, CenturyLink will investigate to confirm that WAF is functioning properly.

1.5.5. **Maintenance and Support:** CenturyLink will provide maintenance and support tasks marked with an "X" in the CenturyLink column in Table 1.0 Roles and Responsibilities Web Application Firewall 1.0.

1.5.5.1. **Upgrades**: If CenturyLink determines an upgrade is necessary to fix a security or performance issue, CenturyLink will work with Customer to schedule a time to make necessary changes, during the Scheduled Maintenance Windows. Customer must allow CenturyLink to make these changes within five (5) business days of receipt of the request from CenturyLink, or CenturyLink's obligation to provide this service in accordance with this CenturyLink Service Guide will be suspended until Customer grants CenturyLink the access CenturyLink requires to make such changes. CenturyLink shall not be liable for any failure to perform in the event of Customer's failure to provide access. If CenturyLink determines that an emergency security change is required, CenturyLink will make the change as quickly as possible. CenturyLink will make commercially reasonable attempts to contact the Customer's technical contact prior to making said change.

1.5.5.2. **WAF policy**: CenturyLink will, upon Customer's request, provide a review of Customer's WAF policy when major changes are made to the environment or when new applications are introduced to the environment. Each review may be conducted telephonically and includes a review of WAF alerts, preparation for rule configuration and communication with Customer. To initiate a review, Customer should contact the CenturyLink Service Center to open a ticket. CenturyLink will support up to one (1) review per month as part of the standard Service.

1.5.5.3. **Attack Mitigation**: Customer must notify (telephonically) CenturyLink of an attack on Customer's site. CenturyLink will then modify Customer's WAF policy to mitigate attacks using commercially reasonable efforts.

1.5.5.4. **Hardware Maintenance**: Service includes hardware break-fix maintenance, with a next business day response time.

1.5.5.5. **Response Notification:** Response times for all incidents/requests are defined in Table 3.0 Response times.

2. **Customer Responsibilities (CenturyLink Managed and Customer Premise)**: Customer is responsible for all tasks with an "X" in the Customer column in Table 1.0 Roles and Responsibilities. Customer acknowledges and agrees that its failure to perform its obligations set forth in Table 1.0 and those customer responsibilities listed

below in this Section 2 and if applicable Section 3 may result in CenturyLink's inability to perform the Services and CenturyLink shall not be liable for any failure to perform in the event of Customer's failure. CenturyLink shall not be liable for any failure to perform in the event Customer does not fulfill Customer's responsibilities and requirements as detailed herein and in the event of Customer's errors or omissions in setting up the required environment. In addition, CenturyLink is not responsible for any loss or corruption of data or information. CenturyLink's obligations related to data are exclusively governed by the Security and Compliance section of the applicable Agreement.

2.1.1. **Network Topology Changes**: The Customer must notify CenturyLink in advance of any network topology or system changes that may affect the WAF or the effectiveness of the WAF policy. Failure to notify CenturyLink of system changes may result in the inability to monitor traffic or the generation of false alerts. CenturyLink will work with the Customer to resolve chronic false positives and other nuisance alerts; however, if alerting issues are not resolved satisfactorily, CenturyLink may modify the IDS configuration to reduce repetitive alarms caused by Customer actions that are not indicative of security incidents.

2.1.2. **Testing and Third Party Access**: The Customer shall not attempt (nor instruct or allow others to attempt) any testing, assessment, circumvention or other evaluation or interference with any Service without the prior written consent of CenturyLink. The Customer will not instruct or permit any other party to take any actions that would reduce the effectiveness of the Service or any used to deliver the Service. Without limiting the foregoing, Customer is specifically prohibited from conducting unannounced or unscheduled penetration testing or external network scans. The Customer shall not attempt (nor instruct or allow others to attempt) any testing, assessment, circumvention or other evaluation or interference with any Service without the prior written consent of CenturyLink

2.1.3. **SSL Certificates:** IPSec or SSL VPN termination is not supported with this service. While end point VPN termination is not supported, the WAF will offer the capability to inspect SSL traffic. When configured to inspect SSL traffic, Customer will be responsible for providing CenturyLink with a copy of their SSL certificate(s) that are to be installed on the WAF appliance. As the SSL certificate(s) change(s), it will be Customer's responsibility to provide CenturyLink with updated certificate(s). SSL-based Diffie-Hellman key exchange (as defined below) protocol is not supported. It should be expected that during SSL inspection, overall WAF performance would be reduced.

2.1.4. **Fault Reporting and Service Restoration:** Suspected faults on the Service should be reported to CenturyLink at the telephone number provided to the Customer for this purpose. To diagnose and resolve suspected faults, CenturyLink requires certain information when the problem is first reported. Required information can be found in Table 4.0 Fault Reporting.

2.1.5. **Onsite Availability:** The Customer will incur additional charges if CenturyLink dispatches a technician to a Customer site on a date agreed with the Customer, and the technician must return to the Customer site to complete the work because the Customer was not available or ready when the technician first arrived at the Customer site.

2.1.6. **Third Party Software:** If any third party software, including any corresponding documentation, is provided to Customer by CenturyLink in connection with the Service, Customer agrees to use such third party software strictly in accordance with all applicable licensing terms and conditions. CenturyLink makes no representations or warranties whatsoever with regard to such third party software.

2.1.7. **Sensitive Payload**: Customer has sole and exclusive responsibility for any Sensitive Payload contained within WAF log data. Customer owns the content running on the system. It is CenturyLink's responsibility is to manage the health of the system, as well as notifying the customer of any capacity constraints of such system.

2.1.8. Customer acknowledges and agrees that it is solely responsible for selecting and ensuring its software and systems are up to date and supportable.

2.1.9. Customer further acknowledges it is solely responsible for ensuring all devices and hardware are upgraded to meet vendor configurations and agrees that CenturyLink's SLA only applies to currently supported configurations (including but not limited to related devices, software, and operating systems) at the time SLA support requests are triggered. If any configuration or version is identified as "unsupported" by a vendor, the Services are subject to all of the following conditions and/or requirements: (i) a service level objective ("SLO") referring to CenturyLink's reasonable effort to

provide support will apply in lieu of any other applicable SLA and will automatically apply from the time CenturyLink receives notice from the vendor of such unsupported service; (ii) CenturyLink, in its reasonable discretion may elect to charge the customer for any support or additional tasks/work incurred by CenturyLink resulting from Customer's continued use of unsupported configuration until Customer purchases the required and supported upgrades or extended support at an additional cost from the vendor. The requirement to purchase upgrades or extended support from vendor shall apply at any time, regardless of any contract term, term commitments, or renewal periods. Customer's failure to do so may result in CenturyLink's inability to provide the Services and CenturyLink shall have no liability therefrom.

2.1.10. Customer consents to CenturyLink's and its affiliates or subcontractors' use and transfer to the United States, or other countries, data or information (including Customer Contact information such as names, phone numbers, addresses and/or email addresses) of the Customer for the sole purpose of: (i) fulfilling its obligations under the Agreement; and (ii) providing information to Customer about CenturyLink's products and services. Customer represents that it will ensure that all information provided to CenturyLink is accurate at all times and that any business contact has consented to CenturyLink's processing of such information for the purposes identified herein.

2.1.11. Customer consents to CenturyLink collecting and compiling system and security event log data to determine trends and threat intelligence. CenturyLink may associate this security event log data with similar data of other Customers so long as such data is merged in a manner that will not in any way reveal the data as being attributable to any specific Customer.

2.1.12. Access and Permissions: Customer shall provide CenturyLink approved personnel immediate access to CenturyLink managed firewall if there is a service outage and at reasonable times in all other situations. Should CenturyLink determine the need for CenturyLink personnel to physically access the firewall or secure support modem, Customer must allow CenturyLink personnel access to the Customer site. Customer shall ensure that all permissions of any kind needed for the installation and operation of CenturyLink managed firewalls are in place at all times. If the Customer has an Access Control List (ACL) that interferes with management connections, the Customer must allow CenturyLink access for management and monitoring.

3. **Customer Responsibility (Customer Premises Only)**

3.1. **Internet Connectivity**: For Web Application Firewall 1.0 CPE installations, management and alert events are transmitted to the CenturyLink infrastructure utilizing a Customer-provided Internet connection. Therefore, Customer is required to maintain Internet connectivity to the WAF appliance.

3.2. **Protected Network**: CenturyLink design requirements mandate that the WAF appliance be installed on a protected network, behind a sufficiently configured perimeter firewall.

3.3. **Topology**: In order for CenturyLink to perform proper configuration and installation, Customer must provide CenturyLink with a topology of their existing network.

3.4. **Infrastructure**: Customer must provide 2U to 4U of rack space and necessary power for the WAF appliance. CenturyLink will provide the specification and configuration information.

3.5. **Network**: Customer-provided 10/100/1000 network connection(s) into Customer's switching infrastructure in addition to a Customer-provided public IP address for WAF management.

3.6. **Standard Procedures**: Customer will, using CenturyLink standard procedures, notify CenturyLink of initial and later changes to the network and application information to be configured by CenturyLink in conjunction with the Service.

3.7. **Installation**: Customer will have responsibility for the physical network installation of the WAF appliance. Implementation of the WAF appliance may require perimeter firewall rules be opened and/or adjusted to allow for communication to isolated network segments.

3.8. **POTS** Telephone: Customer will arrange and pay for a standard (POTS) telephone line (with direct inward dialing) for each Customer site to enable CenturyLink to perform remote network management functions on the WAF appliance. CenturyLink will not be responsible for any problems related to the delivery of the WAF service on Customer Premises, if this telephone line is not available or if it is not functioning properly at all times.

3.9. **Alerts**: Customer will have the responsibility to investigate all alerts provided to them as part of the Service.

4. **Additional Services:** At Customer's option and expense Customer can choose to add the services listed below. The items can be added to the standard Service (described in Section 1.0) for an additional fee described in a separate Statement of Work ("SOW") or Service Order. Contact a sales representative for additional information.
   4.1. **Ethernet Upgrade (CenturyLink Managed Only):** The Fiber Gigabit Ethernet Upgrade provides up to four Gigabit fiber interfaces available for Customer use. The Gigabit Ethernet Upgrade utilizes the WAF chassis expansion slot, and Customer should be aware that this eliminates future expansion capability for additional interfaces.
   4.2. **Attack Investigation:** CenturyLink can conduct an additional investigation to determine the source, impact and then implement mitigation measures.

Tables and Appendices

Table 1.0 Roles and Responsibilities Web Application Firewall 1.0

Activity	Task	CenturyLink	Customer
Installation	Perform an initial set-up review to define WAF requirements and application-specific information.	X	
	The selection of the WAFs that meet the Customer organizations security policies, performance requirements and architecture.	X	
	The creation of Customer rules that govern the device configuration policies.		X
	Verification that device configuration adhere to the Customers organizations security policies.		X
	WAF architecture - while based on the WAF Policies, the WAF architecture is the vision and logical building blocks needed to feed into final design, including the network diagram, based on the Customer organizations security policies.	X	
	Set the device to a "burn-in" status for a minimum period of five calendar days. This will allow CenturyLink security engineers to evaluate alert traffic and make appropriate recommendations for policy tuning	X	
	Following the burn-in period and any follow-up conversations with Customer to discuss alert traffic, required adjustments will be made to Customer's policy as necessary, and the device will be set to blocking status if approved by Customer	X	
	Install and configure the system, apply the initial policy of the device, and set the device to a 'burn in' status for a minimum period of one week to allow CenturyLink's security engineers opportunity to evaluate alert traffic and make appropriate recommendations for policy tuning	X	
	Creation of CenturyLink base build configuration (including logging and alert configuration).	X	
	Installation of operating system to CenturyLink standard.	X	

Activity	Task	CenturyLink	Customer
	The creation of WAF alerting and notification documentation to include alert policies and escalation procedures.	X	
	For Web Application Firewall 1.0 CenturyLink will provide on-site physical installation of the WAF, including racking and cabling of the appliance	X	
Configuration	Testing that all relevant network connections and traffic can be established and maintained through the WAF.	X	
	Deployment of baseline WAF policy.	X	
	Customer test and verification of the WAF configuration policy / rule set.		X
	The testing that known WAF operating system vulnerabilities are identified and patched.	X	
	Testing that WAF logging and data management functions are performing in accordance with the WAF policies and Customer's logging and data management strategies.	X	
	Testing and verification that CenturyLink WAF administrators can configure and manage the WAF effectively and securely from the appropriate networks.	X	
	CenturyLink will configure event policies and notifications for up to 10 Customer-defined rules	X	
	Rate limiting of WAF log traffic will be implemented to protect firewall from denial of service type of attacks	X	
	Review and apply applicable signatures issued by WAF vendor.	X	
	Customer specific WAF rules and filters (if not captured via WAF learning mode).		X
	Customer to sign off on the WAF testing prior to CenturyLink support initiated.		X
	Verification and testing that network communications between Customer specified application components, that traverse the WAF, perform as per the WAF configuration policies.		X
	CenturyLink will provide customized configuration of the WAF according to Customer's reasonable application security requirements	X	
Administration	Adherence to industry standard compliance regulations.		X
	The requesting and gaining approval of changes to the WAF policy rules via the Customer's change management process.		X
	Implement WAF policy rules after appropriately approved via the Customer's change management process.	X	
	Policy review to enhance the performance of the WAF policy. Based on Customer request, once per month.	X	
	CenturyLink security engineers will perform ongoing WAF configuration and rule-set	X	

Activity	Task	CenturyLink	Customer
	changes as reasonably requested by Customer		
	Testing to verify that WAF rules are functioning as expected. Based on customer request, once per month.	X	
	The regular backup of WAF operating system, configuration, policies and rule sets.	X	
	Explanation of the WAF reports and statistics provided on web portal	X	
	CenturyLink will provide Customer at their request the triggered WAF alerts.	X	
Monitoring	CenturyLink will conduct SNMP statistics on WAF performance and make available via CenturyLink Customer facing web portal.	X	
	Receive and review of threat events issued by the WAF device and react to appropriate alerts in accordance with Customer defined escalation process.	X	
	CenturyLink will monitor WAF devices for performance load to include CPU and memory allocations.	X	
	The continuous observation of WAF health and availability alerts and or events that are reported from the WAF	X	
	CenturyLink will conduct ICMP (e.g., ping) monitoring of the WAF appliance to determine system availability (24/7).	X	
Maintenance and Support	CenturyLink will work with the technology vendor to facilitate repair of hardware. This includes assisting in the reinstallation of the required equipment.	X	
	24/7 support for firewall problem resolution and Customer inquiries	X	
	Will provide vendor based maintenance / support contracts to enable code updates and patches	X	
	Will provide hardware break-fix support with a next business day response time for new equipment.	X	
	Support configuration requests associated with full active blocking will be completed within the next business day of Customer's request.	X	

Table 2.0 Performance Tiers

Hardware/Software	Firewall Type	Support	Hardware Dedicated Firewall Appliance	Network Interfaces (10/100/1000 interfaces per WAF)		
				Total	Reserved	Available
Imperva Web Application Firewall Appliance	Small	(1) monthly tuning session	up to 100 Mbps aggregate throughput*	5	1	2 bridged pairs (WAF connect to Network)
	Medium	(1) monthly tuning session	up to 500 Mbps aggregate throughput*			
	Large	(1) monthly tuning session	up to 1 Gbps aggregate throughput*	9	1	4 bridged pairs

*(WAF throughput numbers in the chart above are based on cleartext traffic; the inspection of encrypted SSL traffic will reduce overall throughput capability).

Table 3.0 WAF Response Times

Response Description	Response Time & Procedure
Fault reaction time to Service outage. Maps to SLO P1 (Urgent).	CenturyLink opens a Service Request and begins work on issue within 15 minutes of Customer call or problem detection.
Network design changes, including the addition of new applications. Maps to SLO P3 (Medium) Request.	WAF configuration changes associated with a network re- design or addition of a new or updated application.
Hardware fault resolution time to Service outage	If CenturyLink determines that the firewall must be swapped, CenturyLink will complete the swap by the next business day from the date of problem detection.
Configuration changes to firewall rule-set. Maps to SLO P3 (Medium) Request.	CenturyLink will complete work on the change within next business day of Customer request. CenturyLink personnel update Customer once per day via Customer's preferred method (e.g. phone, email, page) until change is made or Customer declines updates. **Request Management section.**
Event	**Response Time & Procedure**
WAF generated threat event. Maps to SLO P2 (High) Incident.	**Incident Management section.**

Table 4.0 Fault Reporting

Required information
The CenturyLink references for the circuit(s) and/or any other part of a service thought to be affected
Symptoms of the problem
Details of any tests carried out in attempting to isolate the problem
Whether affected services can be taken out of service for testing, if necessary
The name and telephone number of the person reporting the fault

Definitions

CenturyLink Service Center: The primary organization for resolving infrastructure issues that is staffed 24/7/365 to respond in a timely manner to incidents and requests pertaining to Customer IT infrastructure.

Diffie–Hellman key exchange (D–H) is a specific method of exchanging cryptographic keys. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

Failover Solution: Redundancy is built into the CenturyLink Virtual Firewall service. If the primary firewall fails, traffic will be redirected to a hot standby service. This capability is delivered at no additional charge to the standard service fee. The Failover Solution is designed to deliver firewall high-availability by providing a dedicated hot standby. In the event that the primary device fails, the secondary device detects the failure and begins operation. The primary and secondary devices are connected to the Customer's networks on the front- and back-ends of the device via switches or hubs. CenturyLink will work with the Customer to mutually agree a solution based on the Customer's requirements. The agreed solution may require additional network equipment and network services.

Gigabit Ethernet: is a term describing the transmission of Ethernet frames at a rate of a gigabit per second (1,000,000,000 bits per second).

IDS/IPS: Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it.

Layer 2 Bridge (L2 Bridge): An L2 bridge checks the destination media access control (MAC) address of each incoming frame. If the MAC address is assigned to the bridge computer, the frame is processed by it as the destination. If the MAC address is not assigned to the bridge computer, the Network Bridge notes the source address of the frame and the port on which the frame was received and either creates or refreshes an entry in a Layer 2 bridge table.

Maintenance Windows: A period of time designated in advance by CenturyLink, during which preventive maintenance that could cause disruption of service may be performed. Current Scheduled Maintenance windows are:

- Americas: Saturday 00:00AM to 5:00AM; Sunday 00:00AM to 5:00AM
- EMEA: Saturday 02:00AM to 6:00AM
- APAC (Except Japan): Saturday 21:00 (GMT) AM to Sunday 01(GMT)
- Japan: Sunday 04:00 (JST) to 8:00 (JST)

Scheduled Maintenance Windows: A period of time designated in advance by CenturyLink, during which preventive maintenance that could cause disruption of service may be performed.

Security Operations Center: A security operations center (SOC) is a centralized unit in an organization that deals with security issues, on an organizational and technical level. A SOC within a building or facility is a central location from where staff supervises the site, using data processing technology.

Sensitive Payload: Payload in computing (sometimes referred to as the actual or body data) is the cargo of a data transmission. It is the part of the transmitted data which is the fundamental purpose of the transmission, to the exclusion of information sent with it (such as headers or metadata, sometimes referred to as overhead data) solely to facilitate delivery.

Appendix A: Service Level Agreement

Response Times SLA

In the event that CenturyLink is unable to provide service within the "Response Time" windows outlined in Table 3.0, the Customer's sole and exclusive remedy shall be a service credit in the amount of three percent (3%) of the affected service MRC for each response time failure. In no event will the credits accrued in any single month exceed, in the aggregate across all response time goals and incidents, thirty percent (30%) of the invoice amount for the affected service.

CenturyLink's obligation to meet stated Response Times will not apply to:

- Any problems caused by or associated with the Customer's failure to meet specified Customer Requirements
- Underlying Internet access service
- Any security tests

SLA Process

Customer must request any credit due hereunder within 30 days of the conclusion of the month in which it accrued. Customer waives any right to credits not requested within this 30-day period. Credits will be issued once validated by CenturyLink and applied toward the invoice which Customer receives no later than two months following Customer's credit request. All performance calculations and applicable service credits are based on CenturyLink records and data.

The applicable SLA provides Customer's sole and exclusive remedies for any Service interruptions, deficiencies, or failures of any kind. The SLA and any remedies hereunder will not apply and Customer will not be entitled to receive a credit in the case of an Excluded Event. "Excluded Event" means any event that adversely impacts the Service that is caused by,

a) the acts or omissions of Customer, its employees, Customers, contractors or agents
b) the failure or malfunction of equipment, applications or systems not owned or controlled by CenturyLink
c) Force Majeure events
d) scheduled maintenance
e) any suspension of Service pursuant to the Agreement
f) the unavailability of required Customer personnel, including as a result of failure to provide CenturyLink with accurate, current contact information

General Service Requirements

If any third party software, including any corresponding documentation, is provided to Customer by CenturyLink in connection with the Service, Customer agrees to use such third party software strictly in accordance with all applicable licensing terms and conditions. CenturyLink makes no representations or warranties whatsoever with regard to such third party software.

Customer shall:

a) Provide CenturyLink with sufficient system passwords, privileges and access to allow CenturyLink to install, configure, monitor and modify the Service.
b) Not attempt (nor instruct or allow others to attempt) any testing, assessment, circumvention or other evaluation or interference with any Service without the prior written consent of CenturyLink.
c) notify CenturyLink at least 5 business days in advance of any changes that may affect the applicable Service (e.g., infrastructure, network topology changes)
d) purchase and maintain a reliable, stable and always-on, high speed connection to the public Internet (i.e., DSL, T1, cable modem etc. -- a dial-up connection is not sufficient) and/or a standard (POTS) telephone line (with direct inward dialing) for each Customer site to enable CenturyLink to perform remote network management functions.

e) Designate and maintain a Customer Contact during the Service Term (including current contact information). "Customer Contact" means an English-speaking technical point of contact available 24 x 7 with sufficient knowledge, authority and access to address configuration issues, event notifications, system or infrastructure modifications and authentication of applicable CenturyLink systems.
f) For CenturyLink Managed Hosting environments any Ports and VLANs in addition to those included in the standard CenturyLink design shall be subject to incremental charges as set forth in the relevant Service Order. Any Port or VLAN requested by Customer after the initial installation of the Service shall also be subject to additional, incremental charges. Provision of the Service is subject to Customer's compliance with this Section.

CenturyLink may manage all system administration passwords, including root level access, and may do so exclusively. In such case, Customer will not have access to system passwords nor able to make changes to the system configurations and must instead submit change requests to CenturyLink.

CenturyLink may require access to Customer's staging environment that matches production configuration in order to test configuration stability prior to implementing software changes. A successful test on the staging system does not guarantee success on the production system. The Services do not include the development of a comprehensive change control process. There may be incompatibilities between a Service and particular Customer environments which cannot be resolved. In such cases, CenturyLink reserves the right to withdraw the Service from those particular environments, but only to the extent necessary to resolve the incompatibility and without modifying either party's obligations with regard to unaffected environments.

Customer may incur additional charges if:
a) Customer impairs the Service;
b) CenturyLink dispatches a technician to a Customer Site and the technician is unable to complete the work because Customer was not available when the technician arrived.
c) Customer incurs three false alarms in a month; in which case, Customer will pay a $300 false alarm fee, plus an additional fee for each additional false alarm during that month (except where CenturyLink provides the Internet connection). Customer may request that CenturyLink discontinue Service monitoring in order to avoid false alarm fees; provided, however, CenturyLink shall have no further monitoring obligations whatsoever with regard to the affected Service. CenturyLink may require the purchase of Incident Response ("IR") Services, which consist of CenturyLink personnel responding to security events impacting Customer. IR Services are limited to response and mitigation of incidents and do not include ongoing or long-term security consulting, which are subject to additional terms and charges.

If a Service requires reconfiguration or retuning for any reason, including reducing false positives and nuisance alerts, CenturyLink will contact Customer, if necessary, to schedule the activity (typically during normal maintenance windows) and Customer agrees to cooperate with CenturyLink to schedule such activity. If CenturyLink determines that an emergency security change is required, CenturyLink will make the changes deemed necessary as soon as reasonably possible and will notify the Customer of the changes as soon as practicable.