

SERVICE: C8 PUBLIC CLOUD

VCPU REQUIRED (X 2GHZ)	MEMORY REQUIRED (X 1GB)	HDD REQUIRED (X 1GB)	CLOUD PROTECT (BACKUP)	CLOUD PROTECT (BACKUP) DATA STORAGE COMMIT REQUIRED (GB)	BANDWIDTH RATE
2	8	1000	☐		0.72174
CDT TIER FEES	INCLUSIVE CDT (GB)	WAAP - NUMBER WEBAPPS INCLUDED	WAAP - BANDWIDTH INCLUDED (MBPS)		
\$0.00		1	10		
NETWORK INTERCONNECT	NETWORK INTERCONNECT SERVICE TYPE	NUMBER OF EDGE DEVICE PAIRS REQUIRED	NUMBER OF IP ADDRESSES REQUIRED	CLOUD SUBSCRIPTION FEES	
☐		1	1	\$1,500.00	
FLEXIBLE OR COMMITTED MODEL	INTERNET ACCESS TYPE		NUMBER OF PROFESSIONAL SERVICES HOURS		
Committed	Data Transfer (per GB)		1		
TOTAL ACTIVATION FEES (NRF)	TOTAL MONTHLY FEES (MMRF)				
\$485.00	\$1,500.00				

Notes
Additional Terms



manage⁸

CONTINENT 8 PUBLIC CLOUD

For Continent 8 Standard Definitions and Common Abbreviations, see Appendix A

1. SERVICE DESCRIPTION

The Continent 8 Public Cloud is a flexible IaaS (Infrastructure-as-a-Service) platform running on resilient, scalable server hardware from industry-leading vendors. It utilizes VMware virtualization for agile service delivery across multiple integrated data centres. This uniform architecture enables consistent, highly available services that can scale on-demand with no downtime.

1.1. SERVICE AND PRODUCT SUPPORT

Upon assessing and agreeing to the Customer's Public Cloud requirements including the Virtual Data Centre (VDC) resource pool size, Continent 8 will:

- Build the VDC to the specified resource and IP address allocation per the CSOF (Customer Service Order Form); and
- Provide Customer with login credentials, portal URL, and User Guide.

The standard Continent 8 Public Cloud provisioning expects Customer to self-configure VMs (Virtual Machines), networking, and edge devices through the provisioned tenant portal.

Customers have full responsibility for VDC configuration. Continent 8 will provide support to customers to assist them with managing their VDC (i.e. to assist with "how to" questions about the C8 Cloud platform, features, operation, and configuration). Additional support beyond this will incur additional charges.

1.2. PROFESSIONAL SERVICES – [OPTIONAL ADDITIONAL CHARGES APPLY]

If requested, Continent 8 can provide Professional Consultancy Services to assist the Customer with VDC provisioning and defined SLAs, including:

- Building the VDC to specified resources;
- Deploying VMs per the completed New Build sheet;
- Configuring existing VMs;
- Installing initial OS (Operating System) and IP allocation;
- Configuring edge devices and network services; and
- Configuring backups and assisting with restores.

Any technical assistance not explicitly in scope or not covered by professional services time requires additional cost at published rates as found on the Customer Support Portal.

Subsequently requested services will be detailed in a separate Customer Service Order Form ("CSOF").

1.3. CONTINENT 8 PUBLIC CLOUD SERVERS

The Continent 8 Public Cloud supports virtual servers with any enterprise operating system per published guidance.



manage8



Continent 8 has a Microsoft SPLA agreement for Windows licensing on a rental basis if specified under a separate CSOF.

If unspecified, Customer must provide appropriate software licenses and remain responsible for management, security, and maintenance unless otherwise indicated.

1.4. CONTINENT 8 PUBLIC CLOUD INTERNET

All Continent 8 Public Cloud VDCs include metered Internet access, with fees determined by the volume of data transferred (measured in GB) within the calendar month and are based on the higher of Inbound or Outbound traffic volumes.

Fees will consist of any Committed Data Transfer (CDT) commitment (which can be zero) along with any overage above the contracted CDT level.

Continent 8 monitors VDC traffic, and in the event of network congestion or detrimental events, will manage traffic to ensure efficiency and maximize availability across customers.

1.5. CONTINENT 8 PUBLIC CLOUD EDGE SERVICES

The Continent 8 Public Cloud includes a standard edge device on all deployments for basic firewall, load balancing, and other functions. Customers can configure the edge device to pass all traffic and supplement with a virtual firewall appliance within their VDC, with resources included in overall requirements.

The Continent 8 Public Cloud Edge is also available as a standalone Network Edge as a Service (NEaaS) interconnected to external infrastructure, with identical functionality per documentation.

Charges apply for any public IP addresses allocated to edge devices. All public IP address allocations require justification meeting Local Internet Registry (LIR) guidelines.

1.6. CONTINENT 8 PUBLIC CLOUD 'NETWORK INTERCONNECT' – [OPTIONAL]

The Continent 8 Public Cloud Network Interconnect service connects the cloud to other Continent 8 products:

- **MPLS** - Global multipoint network between Continent 8 locations;
- **iGaming Exchange** – Exclusive iGaming eco-system;
- **Cloud Exchange** - Direct connectivity to public clouds like AWS, Azure, Google; and
- **Colocation** - Cross connect to existing Continent 8 colocation services.

Setup and monthly recurring fees apply for the Network Interconnect service.

Due to complex configuration, each interconnected Continent 8 product requires a separate CSOF with specific terms and conditions relative to the product.

manage⁸

1.7. CONTINENT 8 PUBLIC CLOUD L3-7 DDoS MITIGATION

Layer 3-7 DDoS mitigation is included for Continent 8 Public Cloud customers. Licences included:

- Layer 3-4 DDoS for all traffic; and
- Layer 7 DDoS and website/ app/ API protection for one app and 10Mbps throughput.

Customer may purchase additional licenses as required at the published price. If Customer exceeds the assigned 95th percentile throughput license for an application more than twice in a 12-month period, Continent 8 reserves the right to increase the throughput license amount accordingly. If SecureEdge license costs increase, Continent 8 reserves the right to pass on the increase to the Customer with 30 days' notice.

The Continent 8 Layer 3-7 DDoS Mitigation Service protects Customer from malicious Internet traffic and DDoS attacks through four main components: monitoring, mitigation, a Cloud Web Application and API Protection (SecureEdge) portal, and a Customer Support Portal.

Monitoring: Continent 8 continuously monitors incoming Customer traffic from Continent 8 or Customers network. Layer 7 monitoring is performed by Customer via the SecureEdge portal unless Customer subscribes to a Continent 8 managed security service like Managed SecureEdge or SIEM.

Layer 3-4 Mitigation: Continent 8's DDoS Scrubbers mitigate Layer 3-4 DDoS attacks by filtering and shaping malicious traffic at the network border or scrubbing nodes, ensuring delivery of clean traffic to Customer. Clean traffic will be returned over Customer IP Transit port if DDoS service is considered On-net, or can be delivered via GRE tunnel, Private circuit, or another agreed medium if considered an Off-net service. For more detail regarding clean traffic return, please refer to the DDoS Mitigation Guide on the Customer Support Portal.

After a Layer 3-4 attack, Continent 8 will continue mitigating the affected circuit for 60 minutes minimum. Mitigation may be discontinued sooner per Customer request. Beyond 36 hours post-attack, Continent 8 may discontinue mitigation with Customer notification. Layer 7 rules remain active until modified by the Customer or Continent 8's managed service.

Layer 7 Mitigation: The SecureEdge mitigates Layer 7 DDoS attacks and other threats based on Customer-configured rules, including rate/connection limiting, reputation filtering, protocol validation, attack signatures, Anti-Virus, Data Loss Prevention, behavioral analysis, and more.

The SecureEdge portal: Provides visibility and control of the monitoring and mitigation components and configuration. <https://Continent8.waasonline.com/doc/Continent8/Content/CloudWAF/Overview.htm>

The Customer Support Portal: Provides visibility of historic and current DDoS. <https://support.continent8.com/> - Continent 8 Support Portal

manage⁸

1.8. CONTINENT 8 L3-7 DDoS PROFILING – [OPTIONAL]

For an additional fee, Customer may fully provision DDoS protection in advance of attacks via proactive profiling support. Profiling uses predefined, Customer-specific profiles and thresholds to ensure the fastest, most effective mitigation and reduce false positives or blocking legitimate traffic.

Profiling requires Customer's network team to work with Continent 8 engineers to create custom DDoS protection profiles applied to specific IP addresses/ranges. Customers can then update these profiles via the Continent 8 portal and API.

Information necessary from Customer includes:

- Internet-facing network topology/data flow diagrams;
- IP assignment list - subnets to devices;
- Device services - active ports, services, function; and
- Whitelists - networks always allowed.

Customers must provide accurate, reliable technical/configuration info to Continent 8 and inform of any changes. Customers are responsible for providing/updating escalation contacts.

1.9. SECUREEDGE – FULLY MANAGED SERVICE/ ONBOARDING AND CONFIGURATION SUPPORT– [OPTIONAL]

For additional fees, Customer may choose to utilize Continent 8 engineers to onboard and/ or configure protection for their application. This will require Continent 8 engineer to work with Customer to deploy. An ongoing, fully managed service is also available.

1.10. CONTINENT 8 PUBLIC CLOUD 'CLOUD PROTECT (BACKUP)' – [OPTIONAL]

Pricing is a fixed monthly subscription fee per GB of Customer-defined backup storage quota.

- Customers manage backups and restores via the Continent 8 Protect portal
- Flexible backup scheduling options available, minimum 4-hour incremental backup frequency
- Customer-selected restore points for backups
- Restore options: Full VM, vApp, individual files/folders (per backup type)
- Backup types: Full VM-level, application-aware, with guest indexing
- Encrypted backup data

NOTE: Deleted VMs are deleted from backup after 14 days by default unless Continent 8 is advised in writing by the Customer to retain them.

1.11. TECHNICAL SUPPORT SERVICES

The Service level agreement, including response and resolution times for Technical Support Services is outlined in **APPENDIX D: 'Response Times and Escalation Thresholds'**.

24x7 infrastructure monitoring and technical support is provided by Continent 8 with defined response times based on severity as per standard published response times as found on the Customer Portal.



manage⁸



Customers can contact Continent 8 technical support in relation to the subscribed service, either by e-mail, on the portal or by telephone on a 24x7 basis, as per the process outlined in **APPENDIX C: 'Technical Support Services'**.

Additional fees may be applicable for support (e.g. if it is not explicitly included within the scope of the service described in this document). In such cases, the fees will apply as outlined in **APPENDIX E: 'Technical Support Fees'**.

Continent 8 employs technicians on a 24x7 basis, who are on-call for critical issues, as described in **APPENDIX C: 'Technical Support Services'**.

Continent 8 can also provide second level 24x7 support for non-critical issues, as described in the **APPENDIX C: 'Technical Support Services'**, provided that the Customer gives at least seven days' advance notice to Continent 8.

2. RESPONSIBILITIES AND OBLIGATIONS

CONTINENT 8:

- Installation, commissioning, and testing of all VDCs and associated networking to ensure the cloud service is fully operational;
- Provision of remote access to Customer for each VDC instance upon configuration completion;
- Secure delivery of IP addressing and login credentials to Customer;
- Formal handover of the Continent 8 Public Cloud service to the Customer, with coordination of any trial phase and written confirmation of the service activation date;
- Commencement of Customer support and billing after the service activation date is agreed upon;
- Management of service releases and engineering changes, including hardware, software, or firmware, necessary for the maintenance or enhancement of cloud services;
- Assurance of Customer notification at least five days in advance of any scheduled maintenance expected to impact operations, with a commitment to minimizing service disruption;
- Vigilant protection of physical hardware and software hypervisor against security threats and the implementation of industry-standard security measures to prevent unauthorized access or misuse of Customer data; and
- Continuous 24/7 monitoring of the Continent 8 Public Cloud platform, with a commitment to adhere to the support SLA in responding to incidents and outages.

CUSTOMER:

- Collaboration with Continent 8 during the VDC setup for remote access facilitation;
- Receipt of IP addressing and login credentials from Continent 8;
- Engagement with Continent 8 for the handover and activation of the Public Cloud service;
- Acknowledgement of service activation date and commencement of billing as agreed via email;
- Preparation for scheduled maintenance activities following Continent 8's notice;
- Cooperation with Continent 8's security protocols to ensure the integrity of user data and web interfaces;

A stylized handwritten signature in black ink, located in the bottom right corner of the page.

manage⁸

- VDC, O/S, application availability, operation, and maintenance;
- Data sovereignty - Compliance with regulations on stored data location/movement;
- Customer assesses and secures VDC against security threats and ensures necessary data encryption;
- Data Backup - Customer ensures suitable data protections. For Cloud Protect service, Customer manages requirements, monitoring, testing. Customer promptly reports backup issues requiring Continent 8 support;
- O/S and software licensing - excluding any provided Continent 8 OS licenses;
- DDoS Mitigation – Assists determining traffic levels/profiles for service. Facilitates Continent 8 requests to assist mitigation. Facilitates periodic mitigation testing; and
- SecureEdge Service – Request license activation from support@continent8.com when required. Configure and support all elements of the service, unless subscribed to Continent 8 managed service, and/ or onboarding or configuration support.

3. SERVICE LEVEL AGREEMENT (SLA)

3.1. CONTINENT 8 PUBLIC CLOUD SERVICE AVAILABILITY

Continent 8 makes all reasonable efforts to ensure 99.95% availability for each Continent 8 Public Cloud location, as monitored 24x7x365. A location is "available" if usable by Customer.

If monthly availability drops below 99.95%, Customer may request to receive 100% credit of the public cloud subscription fee only for the affected service. Please see section 3.4 for claim directions.

3.2. L3-7 DDOS MITIGATION LIMITATIONS

Due to the complex nature of DDoS attacks, Continent 8 cannot guarantee detection, mitigation, or prevention of attacks disrupting Customer networks.

Continent 8 may start billing for attack traffic after 36 hours if an attack persists despite consultation with the Customer on mitigation options.

Continent 8, in its sole discretion reserves the right to disconnect Customer network if an attack harms the Continent 8 network and affects other customers, after reasonable efforts to notify Customer and avoid disconnection.

To protect overall network integrity, Continent 8 may route Customer traffic to any location needed during an attack.

3.3. TECHNICAL SUPPORT SERVICES

The service level agreement, including response and resolution times for technical support services is outlined in **APPENDIX D: 'Response Times and Escalation Thresholds'**.

3.4. EXCLUSIONS

- Service credits apply only for specific service unavailability reported via a ticket.



manage⁸



- Credits do not apply if Customer is in breach of the agreement or if unavailability is caused by:
 - a) Customer applications, equipment, facilities;
 - b) Customer negligence or misconduct;
 - c) Actions at Customer request;
 - d) Scheduled maintenance;
 - e) DNS issues outside Continent 8 control;
 - f) Issues affecting Internet IP traffic overall;
 - g) Third party services for Customer;
 - h) Malware, defects, failures on Customer side;
 - i) Force majeure events;
 - j) Customer failure to perform obligations; and
 - k) Exclusions per the service agreement.
- Customer must claim credits by end of month after incident via written notice.
- Eligible credits apply to next month's invoices.

4. SCHEDULED MAINTENANCE

- Continent 8 may perform scheduled maintenance affecting Customer operations.
- Continent 8 will notify Customer at least five days in advance of such maintenance via email.
- Maintenance activities will be performed to minimise service disruption and unavailability for Customer.

A handwritten signature in black ink, appearing to be "J. B.", located in the bottom right corner of the page.



APPENDIX A: Common Abbreviations and Definitions

ASHRAE – This refers to the American Society of Heating, Refrigerating and Air Conditioning Engineers. In context of C8 services, the standards set by this organisation inform the parameters within which the Cooling and Humidity Control systems in our Datacentre Rooms are set to operate.

Authorised Person or Authorised Official – Any person who is duly authorised by a customer to act on their behalf. Such authorisation should be given to C8 in writing or by email.

BGP / BGP Peering – is a method by which larger networks 'path' (routing) information.

C8 - Continent 8 Technologies

CDR – Committed Data Rate refers to the minimum monthly customer commitment, in terms of network pipe size and is usually shown in 'Mega Bits per Second' or Mbps.

Clean Traffic – this is Internet (IP) traffic, which is delivered to the customer after filtering by the DDoS Mitigation service, at optimum mitigation the amount of traffic the customer would utilise when not under attack.

CLOUD – In context of C8 Services, 'Cloud' refers to a high-performance hosting platform, available across many different C8 global datacentres, on which a suite of virtualised services is built.

CPE – The 'Customer Premise Equipment' is the device(s) which C8 will locate at the customer premises (or rack location) to enable connectivity to C8 services, such as MPLS or Internet.

CSOF – Customer Service Order Form. This is the first part of the C8 customer contract on which the detail of the service ordered and associated costs are outlined.

Designate or Designated Person – A person denoted as 'designated' on customer access forms.

DDoS Attack - A DDoS (Distributed Denial of Service) Attack, is defined as an event in which a single or multiple compromised system(s) on the internet target IP traffic at a single or multiple destination host systems, thereby causing a denial of service for users accessing services on the targeted host systems.

DDoS Mitigation Service – hardware and software deployed and configured to reduce, disrupt or prevent the denial of service attack from affecting the target.

DNS – The 'Domain Name System' is a global network service, by which user friendly internet names – such as 'www.website.com' - are translated in to IP addresses, which can be used by network devices.

IP Address – An 'Internet Protocol Address' is a numerical address given to a device connected to a network. It is necessary for the device to talk to other devices across any network in the same way a postal (or email) address is necessary to send a letter (or email).

ISP – Internet Service Provider

LAN – A 'Local Area Network' is a network that is local (usually geographically as well as logically) to an organisation or application environment.

Latency – Latency is a measure of the 'round trip time' for data to travel between two locations on a network.

A stylized handwritten signature in black ink, located in the bottom right corner of the page.



LOA – 'Letter of Authority' or 'Letter of Authorisation'. These are commonly required by hosting companies, such as C8, to allow access by a 3rd party in to another customers datacentre rack, or for a 3rd party to act on behalf of a customer.

MMRF – The Minimum Monthly Recurring Fee

MPLS – 'Multiprotocol Label Switching' is a routing method used by C8 to pass data from one part of our global network to another, in an efficient manner, using the best path.

MSA – The 'Master Services Agreement' is the over-arching agreement a customer has with C8.

NNI – A Network-to-Network Interface is a method by which C8 customers can connect to the C8 network at a 'core' network level. This is usually only used for large bandwidth or multi-service requirements in datacentres and is not used as a typical service delivery method.

OS – Operating System

PDU – 'Power Distribution Unit'. These are the 'power sockets' provided in the back of Datacentre Equipment racks.

PoP – Point of Presence. In the C8 context, this usually refers to a datacentre location in which we have a Network Node or other service located.

RACK - In context of C8 services, a 'Rack' means a Datacentre Equipment Rack.

Router – A router is a device used to connect one network to another network, where different IP Address ranges are used. For example, connecting a C8 customer network to the internet.

SPLA – Service Provider License Agreement. An agreement which Continent 8 has in place with Microsoft (and other vendors), which allows C8 to supply, at additional cost, software licenses to customers of C8 for their use while subscribed to C8 services.

SLA – Refers to a 'Service Level Agreement'. This forms part of a customer contract, usually included with a service description, in which C8 outline their commitment to a customer, in terms of the Availability or Performance of a service.

SNMP – Simple Network Management Protocol is a method used by C8 to monitor some customer equipment.

Switch – a network 'switch' facilitates connectivity between multiple network enabled devices, such as computers.

VPN – A 'Virtual Private Network' is a way of providing a private customer network securely across a public network, such as the internet.

WAN – Wide Area Network. This refers to the Global C8 Network Infrastructure.



APPENDIX B: ISO 27017 and ISO 27018 Cloud Certifications

C8 is certified to the cloud standards ISO 27017 and ISO 27018. The ISO 27017 standard is composed of security controls. Holders of the standard must also demonstrate a stringent process of internal auditing and regular training for technical teams. The ISO 27018 standard ensures that personal data is adequately protected when processed by a cloud service provider. These standards require providers to inform customers about incident reporting, disclosure of detected incidents, corrective action and customer responsibilities.

1. Scope of Incident Reporting by C8 to Customer

All major security incidents will be notified to affected customers. Major security incidents are defined as "any event within a C8 environment which threatens the standard operation or security of a service to customers and which causes, or may cause, an interruption to, or a reduction in, the quality and security of the service".

In the case of personal data breaches, the standard for notification to supervisory authorities is 72 hours in the case of a breach that is likely "to result in a risk to the rights and freedoms of natural persons". Work will be undertaken to retrieve the information, the person affected will be notified and the company will carry out root cause analysis to identify and implement corrective and preventative solutions. In the case of a breach of customer contact details, it would be expected to inform them as soon as possible and within 24 hours.

2. Disclosure of Detected Incidents

C8 Support are responsible for 24/7 security incident monitoring and contacting the escalation manager in the case of an incident. This includes alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.

Customer designates will be notified by C8 technical support. Each company will have one or more designated individuals who will be responsible for their company's authorisation listing. This group will contain top level people who can make decisions regarding who will have equipment access, at which facility, and at what level.

The target timeframe for which notification of information security incidents will be given to Customer by C8 is outlined in Appendix D.

3. Corrective Action

C8 has a corrective and preventive action (CAPA) process which provides a formal method by which the company identifies and implements corrective and preventive actions. It focuses on the systematic investigation of the root causes of identified problems or identified risks to prevent their recurrence (for corrective action) or to prevent occurrence (for preventive action).

4. C8 Contact for Issues Relating to Information Security Incidents

support@continent8.com

A handwritten signature in black ink, consisting of stylized, overlapping loops and lines.



North America: +1.514.461.5111
Europe: +44.1624.694.611

If a customer requests further information on a security incident impacting their service, this will be managed by the relevant resolution group manager. Such requests must be from a customer designate. If this is not sufficient to address Customer's concerns, the resolution group manager or the customer designate should escalate to the head of global support services.

5. Customer Responsibilities

As per the MSA, C8 recognises that all personal data relating to your customers or end-users is encrypted by you (both at rest and in-transit). C8 is not responsible for security incidents related to this data.

It is the responsibility of the customer to ensure that suitable precautions are taken to protect the confidentiality, integrity and availability of applications and data hosted by the customer on, or facilitated by, any C8 services.

It is also the responsibility of the customer to ensure that they are aware of, and adhere to, any regulations and/or laws that may be applicable to data stored on or transmitted by the customer, or their agents, through C8 services, including but not limited to rules concerning the data storage location and/or movement of any such data, by any means, across national or international boundaries.

A handwritten signature in black ink, appearing to be a stylized 'J' or 'B' followed by a flourish.



APPENDIX C: Technical Support Services

1. Access to Technical Support

C8 will provide Technical Support 24 hours a day, 365 days a year as part of Services. There is a "Basic" service level for all non-urgent requests, while an enhanced service "Network Assurance" is available at an additional cost. These services include telephone support, email support, incident response, change response, basic or enhanced proactive monitoring, device replacement, and software/hardware maintenance.

Basic (Non-Urgent Requests)

For all non-urgent requests for service, worldwide, email: **support@continent8.com**.

This process will open a support ticket with C8's technical support team. Customer will receive an automated response and will be provided with a ticket number identified in all correspondence in connection to the service request. The next available C8 technician will respond to your request. When communicating with C8 technicians, kindly ensure that the ticket number is always in the subject line for C8 to readily identify the service request.

Network Assurance (Urgent Requests)

In the event of an urgent request or emergency, we recommend that you telephone Technical Support on one of the following numbers:

Europe: +44.1624.694.611

North America: +1.514.461.5111

When placing a telephone call for an urgent request, please have the following information available:

1. Company acronym as Customer is referred to by C8;
2. First and last name of individual calling;
3. Password or passphrase if applicable;
4. Detailed nature of the urgent request;
5. Equipment name and location;
6. Direct telephone line in the event of needing to call individual back;
7. Any other relevant information;

Global Distribution List

C8 has a Global Distribution List for the purpose of providing maintenance advisories to all customers. These can be either scheduled or emergency notifications. Customer shall elect one or more of the authorised person(s) to be on the Global Distribution List. A department email address or a company distribution list can be given as an alternative to individuals.

A handwritten signature in black ink, appearing to be "J. B.", located in the bottom right corner of the page.



2. Notification and Logging of Incidents

C8 aims to immediately detect incidents with any of its Services, sometimes pro-actively informing Customer. However, any problems detected by Customer must be promptly reported by an authorised customer contact (and in any event within 72 hours) to C8. After the authorised customer contact notifies C8 of an incident, the incident will then be logged by C8 and Customer will receive a "ticket" number. This ticket number will form the basis of all follow-up actions. Customer must assign a severity to all incidents submitted to C8, in accordance with the matrix provided in **Appendix D 'Response Times and Escalation Thresholds'**.

3. Response time and Escalation Targets

C8 response and resolution targets, and escalation processes in relation to any support requests, performance issues and/or problems with the provisioning of the services hereunder are detailed in **Appendix D 'Response Times and Escalation Thresholds'**.

4. Planned Work

All planned work and installations should be scheduled with C8, 10 working days in advance. Support tickets opened for planned or installation activities will be categorised as non-critical and this work will be completed during normal working hours unless otherwise agreed.

A handwritten signature in black ink, consisting of a stylized 'A' followed by a series of loops and a final flourish.



APPENDIX D: Response Times and Escalation thresholds

Applicable product(s): **ALL**

Applicable Location: **ALL (ALL)**

	Priority	Definition	Target	Escalation Path (Customer peer)			
			Response Time	SMC/ Escalation Manager (Team Lead/ Supervisor)	SDM/Head of Support (Operations Manager)	Head of Support/ COO (CTO/ Director)	Office of the CEO (MD/COO/ CEO)
Critical	1	Critical C8 service is unavailable; with no workaround available, affecting Customer's business operation	15 Minutes	>4 Hours	>24 Hours	+1 Day	+2 Days
	2	High Priority C8 service is degraded; intermittent or reduced quality of service	2 Hours	>1 Business Day	>3 Business Days	+2 Days	+3 Days
Non-Critical	3	Medium Priority General issue or request for assistance or support with an existing product or service; usually a workaround is available	1 Business Day	>3 Business Days	>5 Business Days	+5 Business Days	+10 Business Days
	4	Low Priority A question, request, or enhancement request	2 Business Days	>5 Business Days	>7 Business Days	+7 Business Days	Not Applicable
Customer suitable and necessary resources will be in contact to support identical prioritisation and liaison				Escalation is expected in-line with appropriate Customer and C8 peer level contacts			

- **Response time** – measured from the time Customer contacts support via published channels, and when case is opened by the engineer, triaged, and priority confirmed.

Note: any period the ticket is "on hold" awaiting response from the customer is excluded from target.

APPENDIX E: Technical Support Fees

The following fees will apply to Level 1 and 2 Support

Region Currency (Locations)	Units (currency)	Level 1		Level 2	
		Standard Business Hours	Outside Standard Business Hours	Standard Business Hours	Outside Standard Business Hours
Minimum Increment per request		1 Hour	3 Hours	1 Hour	3 Hours
EURO (Europe)	Hourly (EUR)	200	250	250	300
GBP (UK, Isle of Man, Channel Islands & Gibraltar)	Hourly (GBP)	200	250	250	300
USD (Kahnawake, US & Asia)	Hourly (USD)	200	250	250	300
CAD (Canada excluding Kahnawake)	Hourly (CAD)	200	250	250	300

Standard Business Hours are defined per the location.

Below guidance for Level 1 and Level 2 activity categorisation

Level 1 support includes the following:

- Power cycling of equipment
- Remote hands and eyes on server consoles
- Escorting service technicians
- Receiving and unpacking equipment

Level 2 support includes the following:

- Replacement of defective components, such as hard drives and power supplies
- Basic hardware installation and configuration
- Basic software installation and configuration
- Network provisioning and support
- Advanced troubleshooting of Client's hardware and software