

# **PSN CONNECT: CLOUD TO PSN**

## **SERVICE DEFINITION**

V2.0

Issue Date: 14/10/2025

Commercial in Confidence

This is a controlled document and the information contained therein is the property of Cloud Gateway Ltd. Uncontrolled if printed or held outside the jurisdiction of the company.

<b>About this document</b>	<b>3</b>
<b>What is Cloud to PSN?</b>	<b>3</b>
<b>Basic operation</b>	<b>4</b>
Private connectivity to cloud (on-ramp)	4
PSN Code of Connection (CoCo)	4
Connecting to the PSN	4
IP Addressing	4
Security arrangements	5
Foundation Security	5
<b>Acceptance testing</b>	<b>5</b>
Acceptance criteria	5
<b>Exclusions</b>	<b>6</b>
<b>Customer responsibilities</b>	<b>6</b>
<b>Cloud Gateway responsibilities</b>	<b>7</b>
<b>Ordering and lead time</b>	<b>7</b>
Ordering and volume	7
Lead time	7
<b>Service management</b>	<b>8</b>
Secure service administration	8
Service support	8
Support escalations	8
Complaints	8
Reporting	8
<b>Service levels</b>	<b>8</b>
<b>Data processing</b>	<b>9</b>
Security arrangements	9
Log storage	9
<b>Business continuity and disaster recovery</b>	<b>9</b>

# About this document

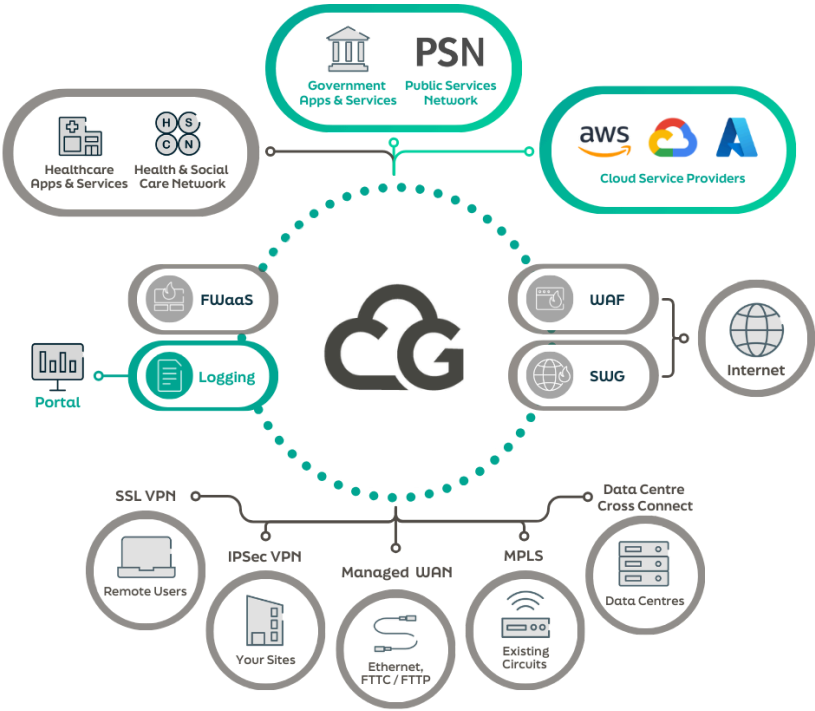
This document is designed to provide a straightforward, clear description of our **Cloud to PSN** service. It covers basic operation, support, what's included and excluded. It defines your responsibilities, and our responsibilities when deploying and running the service.

## What is Cloud to PSN?

Cloud to PSN provides connectivity between the Public Services Network (PSN) and your Cloud Service Provider (CSP). This service allows you to connect one cloud environment to the PSN. Cloud Connectivity is deployed through private connection via a dedicated on-ramp through our UK data centre presence

Traffic is secured via our Foundation Security component, which is included in this service. This set of configurable firewall capabilities manages and controls the traffic passing between the CSP and the PSN.

This is a network connectivity service. You are responsible for contracting with the CSP(s) directly to obtain their cloud services. This includes any charges that might be incurred.



Ecosystem View



Diagram View

## Basic operation

### Private connectivity to cloud (on-ramp)

To connect to your cloud environment privately, we use a dedicated on-ramp within our data centre presence. This on-ramp gives us access to an aggregated fabric of CSPs.

Each cloud provider has a different method to establish network connectivity. As part of the service, we will engage with you to provide technical guidance during the setup process.

### PSN Code of Connection (CoCo)

All organisations that require access to the PSN network are required to complete a set of policy documents making up the PSN Code of Connection. This must be completed before PSN Connectivity can be provisioned.

Information should be provided to Cloud Gateway in order for us to establish the connection.

Guidance on obtaining this can be found on our website

<https://www.cloudgateway.co.uk/knowledge-centre/customer-guides/psn-compliance-process/>

### Connecting to the PSN

PSN Connectivity connects our platform tenancy to the PSN networks. We can connect you to both PSN Assured (PSN-A) and PSN Protect (PSN-P).

Our PSN Connectivity Service has been through the PSN Assurance process, specifically Cabinet Office PSN-Compliance offering SRV\_0454.

This service may be used both to consume services on the PSN, or publish cloud hosted services to the PSN (or both).

Cloud Gateway supports the connection of a customer via our Cloud to PSN service remote access service (SSL VPN), Internet IPsec VPN or NNI to their own virtualized instance of the Security Enforcement Core (SEC), with onward connection to AWS, Internet, other cloud providers and the proposed PSN connection. All connectivity goes through the SEC and must be configured to allow onward connections.

### IP Addressing

IP connectivity and addressing schemes for Cloud to PSN Connectivity are defined below:

- Network Address Translation (NAT) to a single Cloud Gateway PSN IP (for customers requiring outbound PSN connectivity only).
- IP ranges allocated by the PSN Network's IPAM team (for PSN customers requiring inbound/outbound PSN connectivity).

### PSN IP migration

For PSN customers, Cloud Gateway offers the option to use or migrate existing PSN IP ranges. This requires proof of PSN IP subnet ownership and also incurs additional costs to manage the PSN IP migration.

## Security arrangements

A Security Incident is an event that compromises the confidentiality, integrity, or availability of information or information systems. It typically involves unauthorised access, use, disclosure, modification, or destruction of data, or interference with system operations.

Where network vulnerabilities are identified, Cloud Gateway will utilise its vulnerability management process and aim to address the vulnerability within the following timescales:

Severity	Base Score (CVE)	Remediation Target
None	0	N/A
Low	0.1 - 3.9	60 days
Medium	4.0 - 6.9	60 days
High	7.0 - 8.9	30 days
Critical	9.0 - 10	14 days

## Foundation Security

Layer 3 / Layer 4 firewall monitors and controls incoming and outgoing network traffic, based on predetermined security rules. It is designed to establish a barrier between your cloud service provider and the PSN.

The below information is required in order to configure firewall policies to allow specific traffic through the platform:

- **Rule Name** - for example 'ACME RULE'
- **Source (IP address)** - for example '1.2.3.4/32'
- **Destination (IP address)** - for example '1.1.1.1/32'
- **Service (Protocol/Port)** - for example 'TCP/443'

## Acceptance testing

### Acceptance criteria

The acceptance criteria for Cloud to PSN, as part of the platform onboarding are:

- Basic connectivity testing from your CSP to PSN endpoint(s)
- Failover test between Primary and Secondary connection

## Exclusions

The service does not include:

- Code of Connection. Cloud Gateway have a PSN certificate themselves as a PSN connectivity provider, you will require your own PSN certificate to access the PSN too.
- Internet or MPLS connectivity
- Hardware
- Data egress charges from your CSP
- The licensing or right-to-use PSN applications

## Customer responsibilities

You are responsible for:

- Providing details of services that are required for incoming and outgoing traffic to PSN. We'll capture this during our engagement with you
- Providing a PSN connection compliance certificate to Cloud Gateway. This document proves you have completed the PSN CoCo
- Setting up and preparing the cloud environment(s) to which the service is connecting
- Providing us with the name of the CSP(s) with which you wish to connect
- Following any instructions provided by us, or the CSP to establish network connectivity. Some steps in the setup process will rely on you, including (but not limited to) acceptance of invitations, and supplying service keys
- Any User Acceptance Testing (UAT) before, during or after the service goes live
- All negotiation, contracts and costs relating to your CSP, including (but not limited to) ingress and egress charges, application running costs and data storage costs
- Providing Rule Name, Source (IP), Destination (IP) and Service (Protocol/Port) for each firewall rule that is to be applied
- Ongoing maintenance, management and/or decommissioning of your other security capabilities
- Backups. You are responsible for backing up your own systems. We don't hold customer data. We will back up our own platform, and will store logs as detailed in the Log Storage section below
- Verification of PSN IP ownership, as confirmed by the PSN IPAM team, is required.

## Cloud Gateway responsibilities

We are responsible for:

- Resilient IP connectivity to the PSN-A or PSN-P
- Ensuring you've completed the PSN CoCo prior to live service commencing
- All IP routing including failover and dynamic routing
- Application and management of firewall rules gathered during onboarding process
- 24/7 proactive monitoring of the service
- Where network vulnerabilities are identified, Cloud Gateway will utilise its vulnerability management process and aim to address the vulnerability in accordance with the [Security arrangements](#) section
- Providing access to the Cloud Gateway Portal (subject to the Terms of Use)

## Ordering and lead time

### Ordering and volume

We calculate your cost on a bandwidth basis. The bandwidths available to purchase are:

- 10Mbps
- 25Mbps
- 50Mbps

You can request an increase in bandwidth volume from our Sales Team, or via the Cloud Gateway Portal. During the service contract term, you will not be able to reduce the bandwidth volume.

A standard service request charge applies to PSN services requiring a firewall change. A standard Service Request charge will also apply if you wish to remove access to any PSN services.

### Lead time

Our Service Level Agreement (SLA) to deliver the service is 5 working days. The lead time is measured from receipt of a valid Purchase Order (PO) and contract acceptance, to live service ready for any acceptance testing. Please be aware that third parties are involved in the process of you obtaining a PSN compliance certificate, therefore we recommend starting this process as early as possible to mitigate any risk of delay to your service provision. The SLA timer will be paused when there is a dependency on you or external parties to provide information or input.

## Service management

### Secure service administration

Secure service administration is carried out by appropriately cleared Service and Technical professionals, with clearance levels such as BPSS, SC or NPPV3 depending on client requirements.

Role separation is maintained to ensure individuals access only the information necessary for their duties.

Changes are managed using systems including the Service Management Platform and specialised platforms for technical components. A dedicated Service Desk team engages with both the system and end users, working alongside the engineering team to investigate issues and implement solutions.

### Service support

We have an experienced Service Desk team who are responsible for the day-to-day operational service between you and us.

The Service Desk team's primary responsibility is to provide a single point of contact within Cloud Gateway – to which issues surrounding satisfaction of service may be escalated and resolved.

### Support escalations

We strive to ensure that all incidents, service requests, or simple advice and guidance requests from our customers are fulfilled efficiently and effectively within our published timescales.

If you feel that a request is not being managed effectively or would like to escalate a particular issue, this can be raised with our Service Management team.

### Complaints

We take complaints seriously and ask that any customer wishing to raise a formal complaint does so in writing to [service@cloudgateway.co.uk](mailto:service@cloudgateway.co.uk).

Full details of our complaints procedure can be found within the Cloud Gateway Customer Service Pack, which you will receive during the onboarding process.

### Reporting

Various types of reports can be provided. You can request these by contacting [service@cloudgateway.co.uk](mailto:service@cloudgateway.co.uk), or raising a ticket via the Cloud Gateway Portal. Charges may apply.

## Service levels

The service levels that apply to this service are available in our Service level Agreement (SLA).



## Data processing

The data processing terms that apply to this service are available in the Cloud Gateway MSA, found here: <https://www.cloudgateway.co.uk/compliance/msa/>.

## Security arrangements

- The core platform infrastructure that supports this component service is hosted in geographically diverse UK data centres. All data remains within UK sovereignty (with exception if endpoints connect to our platform via the internet)
- We are ISO 27001 and ISO 9001 accredited. We are also compliant with CyberEssentials Plus

## Log storage

- All traffic logs and policy controlled events are stored in our Log Aggregation Platform (LAP)
- Logs are retained for 62 days as standard, and are used to populate graphs and visualisations in the Cloud Gateway Portal

## Business continuity and disaster recovery

Cloud Gateway maintains a comprehensive approach to operational resilience, ensuring continuity of service through robust business continuity and disaster recovery planning. Our internal continuity and disaster recovery plans are reviewed and tested regularly, and staff receive training to ensure they can respond effectively to a disruption.

Our infrastructure is designed for high availability across data centres. Network component configurations are backed up regularly and can be used to recover from disruptive scenarios. Supplier relationships are governed by rigorous due diligence, including reviews of the supplier's own continuity and recovery practices. Data centres and hosting providers, where under our selection, are selected based on secure practices and continuity capabilities. Certifications held by the supplier are reviewed, such as ISO 22301, ISO 27001, ISO 9001 and ISO 14001.

Our operational model supports full remote working, whereby all staff are equipped to operate securely from the office, home or other locations.

**cloudgateway.co.uk**



**+44 (0)20 3870 2444**



**sales@cloudgateway.co.uk**



**Cloud Gateway**  
The Ministry, Borough  
79 Borough Rd, London SE1 1DN

