



Cloud Secure Service Edge

Contracting body

30 Jan 2026

Issue 1.0

© 2026 CGI IT UK Ltd

CGI

Table of contents

1.	Service Description	5
2.	Data backup and restore	5
3.	Service Continuity	6
4.	Onboarding and Offboarding	6
4.1.	Onboarding	6
4.2.	Offboarding	7
5.	Service constraints	7
5.1.	Cloud SSE Service Dependencies	7
5.2.	Operational Scope	8
5.3.	Direct Costs	8
5.4.	Provisioning and Delivery	8
5.5.	Cancellation and Early Termination	8
6.	Service levels	8
6.1.	Service Hours	9
6.2.	Call Priorities	9
6.3.	Asset Ownership, licensing and warranty	10
7.	After sales support	10
8.	Technical requirements	10
9.	Outage and maintenance management	10
10.	Hosting options and locations	11
11.	Security	11
11.1.	Information Assurance	11
12.	Service Pricing and Terms and Conditions	12
12.1.	Pricing	12
12.2.	Terms and Conditions	12
13.	Further information	12
PROPRIETARY AND CONFIDENTIAL		13

Service Definition overview

CGI's Cloud Secure Service Edge provides a fully managed service for delivering secure, zero-trust access to internet and private applications using Zscaler technology. Leveraging Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA), this cloud-native solution protects users wherever they work without relying on traditional VPNs or data centre-based security.

Designed and managed by CGI, this service combines policy-driven security, advanced threat protection, and seamless access to SaaS, internet, and internal applications. We configure and operate the platform on your behalf simplifying security management, enhancing visibility, and supporting your cloud-first strategy.

Features

- Zscaler Internet Access (ZIA) – Cloud-delivered secure web gateway, firewall, and SSL inspection for user internet traffic
- Zscaler Private Access (ZPA) – Zero trust access to private apps without exposing the network
- Cloud-native architecture – Delivered via Zscaler's global cloud platform
- Centralised policy and visibility – Unified management of internet and private access security
- Fully managed by CGI – Configuration, support, and ongoing optimisation.

Benefits

- Protects users from internet-based threats and enforces security policies consistently
- Minimises attack surface and improves user experience without VPN dependency
- Enables scalable, high-performance access without traditional infrastructure constraints
- Simplifies governance and strengthens operational control
- Reduces internal burden while maintaining expert-managed security operations.

Why CGI?

Our 50 years' experience in business and IT consultancy ensures that we have the experience and vision to develop new networks to mirror your business function and outcomes, offering insight into application performance and user experience.

CGI has over 25 years of experience providing fully integrated, managed network services built to enable our clients' best possible performance. We have our own UK network services practice and have relationships with all major carriers and network equipment vendors, designing and supporting major networks for large public and private sector clients.

We optimise our client's service, seeking savings through vendor consolidation and using next-generation software-defined services that reduce the time and effort needed to build and maintain the network. CGI is trusted to manage networks for more than 80 clients across secure government and commercial clients. We support more than 2,000 WAN links, over 20,000 physical LAN devices, and hundreds of physical and virtual managed firewalls.

Our network services are provided from our centralised Digital Command Centre located at our 24/7/365 UK Control Bridge, supported by local engineering and service delivery resources. The Control Centre serves as a centralised hub to monitor, control, and operate business-critical infrastructure enhanced by CGI's AIOps platform, which applies automation and intelligent event correlation to drive faster incident resolution and improve service availability.

Our operations teams are supported by a pool of project architects and engineers who work closely with our clients to design and deliver project-initiated change activities. CGI professionals are certified with all main technology vendors. We are a Cisco Cloud and Managed Services Advanced Partner, Zscaler Partner, Fortinet Expert Level, and Microsoft Gold Certified Partner.

We balance the need to transform networks whilst proving a stable service by ensuring interoperability of new technology with old technology and associated management platforms. We avoid big-bang implementations through using proof of concept, pilot sites and rigorous testing all supported by our dedicated project management and network architect teams.

1. Service Description

Our Zscaler offering enables secure access to internet services, SaaS platforms, and internal applications from any device or location, without relying on legacy VPNs or traditional perimeter security. Designed to support hybrid and cloud-first working environments, the service improves user experience while enforcing consistent security policies and reducing attack surface.

CGI provides end-to-end service delivery including initial discovery, solution design, policy configuration, deployment, and ongoing operational support. Following an assessment of your user profiles, application landscape, and access policies, CGI configures Zscaler Client Connector for endpoint integration and deploys App Connectors where required for private application access. These elements enforce user-level policy controls based on identity, device posture, and contextual risk enabling a zero-trust access model that ensures users connect only to authorised applications.

CGI configures and manages security policies across key Zero Trust Exchange components, including:

- Secure Web Gateway (SWG) – We define and maintain URL filtering, threat protection, SSL inspection, bandwidth control, and file type controls, ensuring users have secure, policy-compliant access to internet and SaaS resources.
- Cloud Access Security Broker (CASB) – We configure in-line controls to monitor and manage the use of sanctioned and unsanctioned cloud applications. This includes policy enforcement for data protection, risky app detection, and user behaviour monitoring.
- Firewall as a Service (FWaaS) – CGI sets up and manages firewall rules in the cloud to control outbound and inbound traffic. This includes L3/L7 rule configuration, geolocation filtering, DNS control, and application-based access policies.

All policy configurations are aligned with your organisation's security posture, business use cases, and compliance obligations, reviewed regularly as part of ongoing managed service activities.

We manage the full lifecycle of the solution, including security policy administration, software and connector updates, threat protection configuration, and integration with your existing identity providers (e.g., Azure AD, Okta). CGI can also interface with your internal or third-party Security Operations Centre (SOC) to support incident triage and threat visibility. Real-time analytics and audit logging provide insight into user activity, application usage, and policy enforcement across the environment.

The solution is delivered entirely via Zscaler's distributed global cloud infrastructure, ensuring high performance, minimal latency, and no dependency on backhaul or data centre infrastructure. With centralised management and ongoing support provided by CGI, your organisation benefits from a robust, scalable, and secure access framework without the overhead of maintaining complex perimeter security infrastructure.

2. Data backup and restore

CGI's Cloud Secure Service Edge is delivered using Zscaler's globally distributed, cloud-native platform, which is designed with built-in resilience and high availability. The service architecture ensures continued access to internet, SaaS, and private applications in the event of infrastructure disruption, with disaster recovery features in place to maintain secure operations.

As part of our managed service, CGI configures and maintains scheduled backups of your ZIA and ZPA policy configurations. In the event of misconfiguration or service interruption, we can restore settings to a known good state. We also support disaster recovery readiness through proactive configuration, policy validation, and operational support. This provides assurance that your secure access services remain resilient and recoverable.

3. Service Continuity

We are ISO:27001 and ISO:22301 certified and maintain a corporate business continuity plan, supporting ITDR and ITSC. CGI has a dedicated Business Continuity Manager (BCM), who ensures that all services and contracts have a service continuity plan, reviewed, and updated at least annually and logged centrally.

In addition, technical recovery plans are prepared for each centralised service. Each service and site conduct a full BC test at least annually and often more frequently. The BCM compiles and communicates a quarterly report to all client services, which includes BC and DR testing, and any lessons learned to enable knowledge sharing.

Our primary delivery location sits within our Data Centre complex, as a result it benefits from the same levels of security and service resilience that a modern Data Centre provides. The site is protected by backup power, high-capacity data communication links supporting high availability and mature Business Continuity plans.

Members have laptops and are equipped to work from home, receiving the same level of support and monitoring as our primary delivery location. If the site is compromised, our members will return home to work, updating telephony routing remotely to redirect traffic to alternative locations.

3.1.1. Business Continuity

Our approach to business continuity ensures that we can continue to operate throughout disaster scenarios and enables us to deliver a continuous, high-quality service for our clients.

We operate to a UK BCMS, with associated templates, audited and certified to ISO:22301 (the international Business Continuity standard) and designed to align with the Business Continuity Institute Good Practice Guidelines (2018).

We maintain a UK Business Recovery plan, which defines roles and responsibilities for the UK Business Recovery Team (BRT) managing events 'on the ground' and a UK Crisis Management Plan, operating at the top level in CGI.

Each CGI site has a Facility Continuity plan, and each shared service team has a Service Line Continuity plan which deals with all aspects which are relevant to the team's services (such as people, skills, information, systems, premises, suppliers) and the strategies and recovery processes covering them.

Our emergency procedures cover risks including fire, bomb/terrorist threat, flood/natural disasters, and pandemics, as well as IT incidents such as virus or malware attacks.

Communications in a disaster include notification to clients via our client engagement managers, to senior managers in CGI, and externally via our Corporate Communications unit.

4. Onboarding and Offboarding

4.1. Onboarding

CGI has proven and effective on and off-boarding skills, tools, and methodologies. We have successfully transitioned numerous Public Sector clients onto our managed network service. CGI has a dedicated team of managers who specialise in transition and who apply considerable previous experience in this area. CGI will apply its standard transition methodology which has been used in all service on- and off-boarding's within CGI for many years. The transition process is flexible and can be used for both small and large scale on-boarding requirements.

The approach taken by CGI is to understand the client's requirements and make the transition phase specific to the needs of the client whilst leveraging the experience, lessons learnt and methodology from many years of transition experience.

4.2. Offboarding

Service offboarding is instigated by a client request or after expiration of the service agreement. Deletion of any managed device and data will occur in line with the service agreement. Any required data will be made available using appropriate media, in line with the data security classification. Pricing of this service is dependent on requirements; please contact CGI for details. After client notification that data has been successfully recovered, CGI will purge and destroy client data from any compute or storage device/media that remains part of CGI's estate.

Cease notices should be provided with a minimum of four calendar months as this allows formal notice to be served on sub-contracted suppliers who usually have a cease notice of three calendar months or 90 days. Where contracts with suppliers specify duration and/or cease notice periods that extend beyond this, then the notice period of the subcontractor will prevail.

Cessation penalties may apply for any cease notice within contract term. These and reasonable incidental costs will be passed to the client where applicable.

4.2.1. Access to data upon exit

Data retention periods and the handover or destruction of data at contract end will be specific to services consumed and vendor policy at the time that a service and components thereof, are agreed.

5. Service constraints

5.1. Cloud SSE Service Dependencies

To ensure reliable, secure, and well-managed delivery of Cloud Secure Service Edge services, the following dependencies and client-side considerations apply:

- Access governance: Where CGI implements and manages the ZIA and ZPA environments, we will provision client access in a controlled and role-based manner to support visibility and collaboration. To maintain service integrity, configuration changes should be coordinated through CGI to prevent any unintended service impact. We will work with you to define appropriate access levels based on operational roles and support needs.
- Identity integration: The client is responsible for providing and maintaining access to their identity provider (e.g. Azure AD, Okta) for authentication and policy enforcement. CGI will require support in integrating and validating identity federation during setup and ongoing operation.
- Client Connector deployment: The deployment and upkeep of Zscaler Client Connector on user devices should be supported by the client's endpoint management or desktop team. CGI will provide configuration guidance and support, but the actual rollout may require internal tooling or GPO scripting.
- App Connector deployment: For private application access, the client must support the hosting and network placement of App Connector instances, including firewall and DNS configuration as required for connectivity.
- Proof of concept and testing: The client will need to provide suitable test users, environments, and applications to validate policy and access behaviour prior to live deployment.
- Network and DNS configuration: CGI may rely on the client's internal networking team to implement DNS or routing changes necessary for policy-based forwarding or disaster recovery readiness.
- Change control alignment: Changes to application architecture, authentication flows, or security policies should be communicated to CGI in advance so that policy configurations can be adjusted without disruption.

5.2. Operational Scope

CGI's Managed Network Services are typically contracted for a minimum term of one year. Services will continue beyond the contract term unless notice is provided. CGI may revise pricing at renewal to reflect current commercial conditions.

All hardware and software licences procured as part of the service will be owned by the client upon delivery. CGI will support the configuration, management, and lifecycle of these assets as part of the managed service.

The managed service includes the following standard capabilities:

- Network monitoring, either 8x5 or 24x7 as required.
- Incident and problem management.
- Access to network spares or agreed hardware replacement service.
- Secure network access to support service delivery.
- Reporting against defined key performance indicators (KPIs).
- Software updates and patching in line with agreed processes.
- A defined service request catalogue and change management approach.

5.3. Direct Costs

The following activities are typically not included in standard support and are discussed separately during pre-sales or transition planning:

- Due diligence, transition, and transformation activities.
- Technology refresh, hardware purchases, and software subscriptions.

Significant moves, adds, or changes, including:

- Out-of-hours work or support at remote sites.
- Activities requiring third-party services (e.g. cabling, WAP installation).

5.4. Provisioning and Delivery

Service lead times are dependent on receiving complete and accurate information at the time of order. Orders may be subject to surveys, third-party dependencies, or landlord permissions. Delivery timelines begin from CGI's formal acceptance of the order, once all prerequisites are met.

5.5. Cancellation and Early Termination

Cancellations or significant amendments to placed orders may incur charges, particularly where third-party telecoms services are involved. Early termination may result in charges up to the full remaining contract value. Multi-year term discounts may also be subject to adjustment upon early cessation.

6. Service levels

CGI operates an ITIL compliant, award winning service management solution, a mandatory element of our service to ensure seamless delivery of service and ongoing support.

Services include:

- Continual Service Improvement
- 24x7 Digital Command Centre
- Major Incident Management
- Problem Management
- Change Management
- Availability and Capacity Management
- Service Level Management

- Configuration Management.

The CGI Digital Command Centre operates during normal UK business hours Monday to Friday and extends up to 24x7 subject to business need. Network support is facilitated by secure remote access. On-site attendance is provided subject to business need.

CGI will provide an event monitoring service as part of its overall Service Management responsibilities. CGI teams will monitor events generated through alerts from monitoring tools. Where the service desk is not a CGI provided service, incidents will be passed to and logged by the client's service desk.

CGI shall collaborate with the client to investigate and seek root cause for any problems, with investigation being handled by CGI.

Several criteria define the applicability the services on offer. There are variances, exceptions, additions, limitations, and particular elements that are associated with individual services and will be peculiar to those services. Nonetheless, several common elements are evident in all services. These include, but are not limited to:

- The service is confined to instances where CGI has built the service offering or the service offering conforms to a design or architecture that CGI supports.
- Standard service based on accepted standard manufacturer infrastructure. Other manufacturer elements would be subject to review and separate negotiation.
- In instances where the Design Authority remains with either the client or alternative third party, the applicability of standard costs will be subject to a review and separate negotiation.

6.1. Service Hours

Two levels of service hours are available:

- Standard Hours – covered by standard service and covering Monday to Friday, from 08:00 to 18:00, excluding UK Public Holidays.
- 24x7 – provided at an additional cost, this provides limited incident resolution service outside of Standard Hours with a cover of 24 hours a day, 7 days a week, 365 days a year.

6.2. Call Priorities

CGI works with established carriers, vendors and support partners to align service levels wherever possible, ensuring timely and effective incident resolution.

Severity		Definition	Users Impacted	Response from initial call being received	Resolution (See note)
P1	Critical	Total loss of service	All	30 Minutes	4 Hour
P2	Major	Major functionality unavailable with NO work round available.	Department or Location	1 Hour	8 Hours
P3	Minor	Major functionality unavailable with work round available.	Single User or Small group	4 Hours	24 hours
P4	Warning	Individual user affected	Single User	8 Hours	72 Hours
P5	N/A	Request for change, etc.	As agreed	As agreed	As agreed

Table 1 - Response and resolution times

6.3. Asset Ownership, licensing and warranty

CGI can assume management responsibility for an existing ZIA or ZPA deployment, provided that the client retains ownership of the subscription and is responsible for all associated licensing costs. We will work with you to onboard the existing environment into our managed service framework, aligning configurations with your security policies and operational objectives.

Alternatively, CGI can provision ZIA and ZPA as part of a broader transition to a managed Secure Service Edge (SSE) solution. In this case, we will support service procurement, initial design, deployment, and handover into ongoing managed operations.

7. After sales support

Networking can be a complicated subject. CGI has network consultancy practice that can offer tailored network assessments, consulting on technical roadmaps as well as designing, configuring, and maintaining services. CGI specialists are certified by vendors including Cisco, Fortinet and Checkpoint.

Examples of areas for consultancy:

- Audit and Inventory Management.
- Design core, edge and cloud network solutions.
- Transition from data centre to cloud / moving toward software-defined networks / adopting ZTNA.
- Configuration, training and knowledge transfer.
- Assessment and optimisation to improve performance and user experience.
- Security / network segmentation / firewall reviews.

This service is typically provided on a time and materials basis, although a fixed price may be agreed depending on the defined scope and specification.

8. Technical requirements

To manage and support your network environment, CGI uses secure connectivity methods such as VPN tunnels and, where required, dedicated private links. We will work closely with you to agree appropriate remote access configurations and determine where connections should terminate within your infrastructure.

Our CGI technical staff follow strictly controlled, audited access procedures when connecting to client environments, always ensuring security and compliance.

In cases where a dedicated connection or increased bandwidth is required to meet specific project needs or performance requirements, this may be provided at an additional annual cost and reviewed regularly to ensure suitability.

9. Outage and maintenance management

CGI will work collaboratively with the client to agree a schedule for routine operational patching and software upgrades, managed through the agreed Operational Change Management process. This schedule will cover all devices that form part of the Managed Network Service.

As part of our service, CGI proactively reviews vendor-issued updates to identify security vulnerabilities. We assess each update's relevance and risk to the client's environment and apply appropriate patches in alignment with the client's security policies and standards ensuring both protection and continuity.

10. Hosting options and locations

Our Cloud Secure Service Edge is delivered using Zscaler's global, cloud-native platform. Zscaler operates more than 150 data centres worldwide, enabling client traffic to be routed through the nearest point of presence (PoP) to ensure minimal latency and high availability.

During the onboarding phase, CGI works with you to agree the preferred service region based on organisational requirements, compliance or data-sovereignty needs. Traffic will be forwarded to a Zscaler Service Edge location closest to the user's location.

CGI manages the configuration and ongoing support regardless of location, giving your users secure, performant access to internet, SaaS, and private applications anywhere, while ensuring that the chosen geographic hosting aligns with your policy or regulatory obligations.

11. Security

11.1. Information Assurance

CGI uses our Management Foundation including our Integrated Management System (IMS) for information assurance. These IMS processes are independently certified to BS/EN/ISO 9001:2008.

CGI is committed to retaining our current range of UK-based certifications and will extend these to meet client expectations as required.

The CGI Management Foundation design allows incorporation of best practice from across all of our Public Sector and Commercial engagements.

Our accreditations include:

- ISO9001, ISO27001 and ISO20000
- ISO/IEC 27001:2005 Audit and Certification SSAE 16/ISAE 3402 Attestation
- E.U. Data Protection Directive - (95/46/EC).

All information is held at the appropriate security level for the service. CGI hosted services can be provided at any level defined in the new Government Security Classification (GSC) policy with the appropriate assurance.

Information Principles for the UK Public Sector supported and documented

CGI recognises the UK Public Sector information principles which are fundamental to the efficient and effective delivery of public services. Where we store and manage government information in our G-Cloud services, we aim to ensure that it is appropriately protected and available to exploit. Through this we would aim to maintain and, depending on the service purchased, enhance the quality of the information stored in a standard manner that enables its re-use. Where the selected services require it, we would engage positively both to support the buyer in the publication of public information and to support them in the access of information by citizens and business.

Government ICT Strategy and Greening Government ICT Strategy supported and documented

The design and delivery of our Cloud-based SaaS offerings is consistent with the principles of the Greening Government ICT Strategy. Scalable, Cloud-based services allow pooling of capacity across multiple clients, reducing overall hardware requirements. These are further reduced through virtualisation, which has delivered up to a 90% reduction in server numbers and power consumption for some of our services. We select modern, energy efficient servers, storage and network hardware and have also invested heavily in improving the energy efficiency of our data centres. This includes initiatives such as free air cooling, aisle containment, power supply upgrades, lighting controls and power management and monitoring software. In the UK, electricity for our data centres is sourced from renewables, which is also the case for many of our third-party hosting providers. We closely manage the impact of IT hardware throughout its lifecycle, aiming to optimise refresh cycles to balance in-use carbon savings of newer, more efficient hardware against the carbon impact of its manufacture. At end of life, we also ensure responsible disposal through resale or recycling of old hardware wherever possible. Our

sustainability performance has won widespread recognition, including our listing on the Carbon Disclosure Leadership Index for four consecutive years and our certification under the Carbon Trust Standard. We are recognized as a global leader within the IT sector on the CDP (Carbon Disclosure Project), Climate Performance Leadership Index. This demonstrates a coordinated progress and actions on climate issues.

12. Service Pricing and Terms and Conditions

12.1. Pricing

Please refer to the associated Pricing Document relevant for this Service.

12.2. Terms and Conditions

Please refer to the associated Terms and Conditions Document relevant for this Service including termination by the Buyer or Supplier.

13. Further information

For more information about this or any of our G-Cloud services, please contact us:

Phone: +44 0845 070 7765. Ask to speak to the G-Cloud team.

Email: uk.gen.ccsframeworks@cgi.com, including the following information:

1. The name of this service.
2. The name of your organisation.
3. Your name and contact details.
4. A brief description of your business situation.
5. Your preferred timescales for starting the work.

We will prepare a quotation for you. Once the quotation is agreed upon, we will issue you the necessary documentation (as required by the G-Cloud Framework) and ask you to provide us with a purchase order.

Once we have received your purchase order, the services will be configured to the requirements agreed with invoices issued to you for the services procured.

On a monthly basis, we will also complete the mandated management information reports to Government Procurement.

PROPRIETARY AND CONFIDENTIAL

The information contained in this document is confidential to CGI and/or CGI group companies. This document shall not be reproduced in any form or by any mechanical or electronic means, including electronic archival systems, or submitted to a generative AI tool without the prior written approval of CGI. The receiving party may use this document and the information contained in it for the purpose of evaluating CGI's proposal only. Any personal data included in this document must not be replicated, stored or distributed beyond the immediate recipient or used for any purpose other than evaluating the document.

This proposal is subject to contract and shall not be binding unless and until execution by CGI and Contracting body of a final agreement to the proposal, containing the terms and conditions that will govern the relationship between the parties. Any final agreement is conditional (inter alia) upon due diligence and customary business investigations by CGI. The results of such due diligence and/or investigations may impact upon content of this proposal, including the business structure, business terms and financial arrangements.

If you have received this document by mistake, note that the reading, the reproduction or the distribution of this document is strictly forbidden. You are hereby requested to inform us by telephone at +44 0845 070 7765 and to return this document by special delivery marked for the attention of Simon Figg.

Except where indicated otherwise, all names, trademarks, logos and brands (registered or not) referred to in this document are the property of a company in the CGI group or its licensors.

The information in this proposal is submitted on 30 Jan 2026 - Issue 1.0 on behalf of CGI by the following authorised representative:

Simon Figg

Frameworks Manger

CGI IT UK Ltd

14th Floor, 20 Fenchurch Street, London, EC3M 3BY

Tel: +44 0845 070 7765

