Jisc Managed SD-WAN

G-Cloud 15 Service Definition

1. Summary

Jisc Managed SD-WAN is a fully managed, software-defined wide area networking service that provides secure, performant, and flexible connectivity to the Janet Network. Built in partnership with BT (leveraging Openreach's national footprint) and Fortinet (market-leading security), the service enables rapid deployment over existing internet circuits, consolidates network platforms, and reduces operational overhead through a single, centrally managed solution. Customers adopt an as-a-Service model Jisc delivers circuits (if required), hardware, software, configuration, policy, monitoring, and ongoing management.

Use cases:

- Replacing or augmenting MPLS with modern SD-WAN
- Securely connecting multi-site campuses, branch locations, and remote learning environments
- Deployment to sites with little to no network expertise. Managed SD-WAN is a fully outsourced service, so you don't have to think about planning, development, and improvement efforts
- Increased speed and flexibility of Janet Network delivery to new or temporary sites at your organisation

1.1 Features

- Secure VPN overlays connect customer sites to Janet network hubs for private, reliable communication.
- Enterprise-grade security and performance delivered through Fortinet FortiGate edge devices.
- Resilient, scalable connectivity via high-capacity SD-WAN hubs.
- Logical multisite configuration supports geographically distributed locations.
- Basic DDoS mitigation included for enhanced protection and reliability.
- Integrated DNS services for secure and efficient domain name resolution.
- Optional advanced security features configurable on SD-WAN devices.
- Trusted delivery in partnership with BT, ensuring robust service and support.
- Flexible internet bearer options for cost-effective connectivity.
- Centralised management platform simplifies deployment, monitoring, and ongoing optimisation.
- Scalable Architecture: Seamlessly add sites/users; support hybrid architectures and cloud on-ramps.

- Managed Service Wrap: Design, build, configure, test, operate, and lifecycle management (hardware/software).

1.2 Benefits

- Rapid deployment: Achieve secure WAN connectivity quickly without investing in new core infrastructure.
- Cost efficiency: Reduce total cost of ownership by replacing or augmenting MPLS with SD-WAN and leveraging multi-tenant economies of scale.
- Enhanced performance: Application-aware routing and dynamic path selection improve user experience for education, research, and collaboration workloads.
- Stronger security posture: Built-in encryption, optional next-generation firewall, and Janet protective services mitigate risks from DDoS, malware, and DNS threats.
- Operational simplicity: Jisc manages design, deployment, changes, and incidents—freeing internal teams to focus on strategic outcomes.
- Future-proof scalability: Easily expand to new sites and support hybrid/cloud connectivity as organisational needs evolve.
- Resilience and redundancy: High-capacity SD-WAN hubs and diverse connectivity options ensure continuity for critical operations.
- Alignment with sector priorities: Addresses key challenges—cost control, cyber security, and infrastructure scalability for members and customers.
- Trusted delivery: Enterprise-grade hardware and partnership with BT guarantee robust performance and support.

2. Service Description

2.1 Core Service Offering

2.1.1 Managed SD-WAN Service

The Services provide you with an alternative means of connecting to the Janet network, the UK's national research and education network (NREN).

2.1.2 Overview of Managed SD-WAN Services

The Services provide a complete WAN connectivity service using the latest “SD-WAN” technology. This will enable the Customer to build private data networks that connect their sites with applications and resources on the network, in data centres, or in the cloud, using only conventional internet access circuits.

The Services include the supply of WAN connectivity, FortiGate firewall equipment and licences, installation and maintenance, in-life managed services, and professional services for deployment and service management. Jisc provides Managed SD-WAN in partnership with BT on Fortinet’s FortiGate platform.

- Secure connectivity via VPN overlays to Janet hubs.
- Enterprise-grade security with encryption, optional NGFW, and Janet protective services.
- Application-aware routing for optimised performance.
- Centralised management for deployment and monitoring.
- Flexible design supporting multisite, hybrid, and cloud connectivity.

- Integrated DNS and basic DDoS mitigation.
- Delivered in partnership with BT for trusted support.

The services are fully described in Schedule 1 (Services Description)

2.1.3 Administration of Services

- Fully Managed Service: Jisc provides end-to-end administration, including design, deployment, configuration, monitoring, and incident management.
- Change Management: All configuration changes, firmware updates, and security policy adjustments are handled by Jisc under ITIL-aligned processes.
- Proactive Monitoring: Continuous monitoring of SD-WAN devices and connectivity to ensure optimal performance and security.
- Incident Response: Jisc manages fault resolution and escalation in line with agreed SLAs.
- Customer Engagement: Regular service reviews and reporting to ensure alignment with organisational objectives.
- Role-Based Access: Customers can request read-only or administrative access for specific functions if required.

2.1.4 Eligibility

Available to:

- UK education and research organisations, including Higher Education Institutions (HEIs), Further Education Colleges (FECs), and research bodies connected to the Janet network.
- Public sector organisations that require secure, scalable WAN connectivity and meet technical prerequisites.
- Suitable on-premises environment for SD-WAN edge device installation.
- Internet bearer options as per organisational requirements.
- Organisations must have existing Janet connectivity or plan to establish it as part of the service.
- Service is offered to Jisc members, customers, and eligible public sector bodies in alignment with sector strategy.
- Buyers must comply with UK data protection and security standards.

2.1.5 Target Availability

The service is designed for high availability, with a target uptime of 99.9% across core SD-WAN hubs and management systems.

Resilience is achieved through:

- Redundant SD-WAN hubs in geographically diverse locations.
- Failover mechanisms for edge devices and connectivity paths.
- Availability excludes planned maintenance windows, which are communicated in advance.
- Monitoring and proactive incident management ensure rapid response to faults.

2.1.6 Resilience

- High Availability Design: SD-WAN hubs deployed in geographically diverse locations to ensure redundancy.

- Failover Mechanisms: Automatic failover between multiple connectivity paths and edge devices to maintain service continuity.
- Janet Backbone Integration: Leverages Janet's resilient core network for added reliability.
- Proactive Monitoring: Continuous health checks and performance monitoring to detect and resolve issues before they impact users.
- Disaster Recovery: Configurations backed up and recoverable to minimise downtime in case of hardware failure.

2.2 Service Options

- Availability: High availability design with resilient SD-WAN hubs and diverse connectivity options.
- Support: 24/7 service desk with incident management and escalation.
- Response Times: Critical incidents addressed within agreed SLA windows.
- Monitoring: Proactive monitoring and performance optimisation via centralised management platform.

Site Type	Services Target Availability	Services availability coverage	Services repair coverage
Resilient ethernet based site	99.9%	24x7x365	Working days 8am-6pm
Non-resilient ethernet based site	99.5%	24x7x365	Working days 8am-6pm
Non-resilient broadband based site	99.0%	24x7x365	Working days 8am-6pm

2.2.1 Service Level Exclusions

Where a Customer chooses the Bring Your Own Bearer (BYOB) as a WAN connectivity type for the Service, the Service Level clock shall be paused during any period in which the restoration of service is dependent on information or actions from the Customer or any third-party service providers. This includes, but is not limited to, delays caused by:

- Awaiting necessary information or approvals from the Customer.
- Actions or inactions of third-party service providers, including but not limited to circuit providers, that are beyond the control of the Jisc / BT.

The Services are fully described in Schedule 2 (Service Levels)

2.3 Processing Locations

- All customer data is processed and stored within the UK in compliance with UK GDPR and relevant data protection legislation.
- SD-WAN management systems and Janet network hubs are hosted in UK-based data centres.
- No data is transferred outside the UK unless explicitly agreed with the customer and subject to appropriate safeguards (e.g., Standard Contractual Clauses).
- Service operations, monitoring, and support are delivered from UK-based teams.

2.4 Information Assurance

- The service is designed to meet UK Government security principles and is aligned with CESG/NCSC guidance.
- Data is processed and stored in compliance with UK GDPR and relevant data protection legislation.
- All VPN traffic is encrypted using industry-standard protocols (IPsec).
- Optional Next-Generation Firewall (NGFW) features provide advanced threat protection.
- Janet protective services mitigate risks from DDoS, DNS attacks, and malware.
- Service management follows ITIL-aligned processes for change, incident, and security management.
- Regular vulnerability assessments and patching ensure ongoing compliance and security posture.

2.5 Service Onboarding

- Initial consultation to define requirements and design solution.
- Deployment of SD-WAN edge devices and configuration of VPN overlays.
- Integration with existing Janet circuits and customer infrastructure.
- Testing and validation of connectivity, security, and performance.

The estimated timescale for the delivery of your connection is 60 days from the date of receipt of the completed Janet Connection and Upgrade Request (JCUR) form and signature of this Agreement. If you are purchasing a connection which utilises BTnet and ethernet fibre is not present in your area, the estimated timescale may be up to 120 days.

The exact timescale for delivery is subject to Jisc's agreement with its Subcontractor and changes to your requirements. We will provide you with an estimated delivery date 21 to 33 days after signature of this Agreement.

Upon completion of the installation of the site connection(s), Jisc will issue notification to you to advise that the Services are ready for use. Notification will be sent to your nominated managerial contact. The date of such notification will be the "Services Commencement Date".

If the Customer requests a change to the Services before the Services Commencement Date, Jisc may revise the Services Commencement Date to accommodate that change.

Jisc will commission the Services during Working Hours on Working Days. When Jisc advises the Customer of the Services Commencement Date, the Customer will carry out the Acceptance Tests in accordance with this Agreement.

Any additional installation services requested by the Customer outside the scope of the site survey may be subject to additional charges. Additional installation services will be priced using Jisc's professional services rates, available on request.

Further details regarding service onboarding are provided in Schedule 1 (Services description).

2.6 Service Off-boarding

- Decommissioning of SD-WAN edge devices.

- Removal of VPN overlays and associated configurations.
- Secure data wipe and return of hardware (if applicable).
- Final reporting and confirmation of service termination

2.7 Customer Responsibilities

- Provide accurate requirements during onboarding to ensure correct design and configuration.
- Maintain Janet connectivity or arrange for connectivity as part of the service.
- Ensure suitable on-premises environment for SD-WAN edge device installation (e.g., power, rack space, cabling).
- Manage internal LAN configuration and integration with SD-WAN edge devices.
- Comply with security policies and UK data protection legislation.
- Notify Jisc of changes to network topology, site locations, or critical infrastructure that may impact service.
- Provide authorised contacts for incident management and change approvals.
- Ensure physical security of installed SD-WAN devices at customer sites.

The customer responsibilities are fully set out in the The Terms and Conditions are available at the website below or a successor website as designated by Jisc from time to time:

https://www.jisc.ac.uk/managed-sd-wan

3. Service Management

3.1 Support Services

Jisc will provide access to the Jisc Service Desk so the Customer can log Tickets in response to Incidents. The Customer will be able to log Tickets at all times.

Jisc will respond to and use reasonable endeavours to resolve an Incident if the Customer reports an Incident with the Services during the Service Coverage Period.

Support services will consist of remote support and, where necessary, on-site support. If the Customer requests on-site support outside of the Service Coverage Period, this may incur additional charges.

Jisc may carry out maintenance from time to time and will use reasonable endeavours to inform the Customer at least 10 Business Days before any planned maintenance to the Services. However, Jisc may inform the Customer with less notice where emergency maintenance is required or where Jisc has not been provided sufficient notice by a third party supplier.
Jisc may provide software updates, configuration management and patch management on Jisc Equipment from time to time.

Jisc can provide ad hoc, remote, technical support on request. Charges for these services are available on request.

3.2 Incident Management

Jisc will use reasonable endeavours to provide the Services in accordance with the following Service Levels.

The target response and target resolution times will commence following a 30 minute period (which will commence when Jisc has issued the Customer with a Ticket).

These Service Levels will not apply where the recommended User limit advised by Jisc is exceeded or where there is a fault with Jisc's head-end Fortinet device. The recommended User limit for each connection type is available on request.

Incident resolution service level objectives for sites utilising BTnet:

Priority Level	Description of impact of Incident	Target Response Time	Target Resolution Time
1	The Services are unavailable at a single Customer site. E.g., there is no connectivity service available at a single Customer site.	1 hour	6 hours
2	The Services are degraded at a single Customer site. E.g.: • a single Edge Device or single internet tail is unavailable at a resilient site but site connectivity is still operational; • an Incident which is intermittent in nature is affecting a non-resilient site but connectivity is still available.	2 hours	10 hours
3	Any other Incident associated with the Services	4 hours	2 working days
4	Request for information	16 hours	10 working days

Incident resolution service level objectives for sites utilising Broadband One:

Priority Level	Description of impact of Incident	Target Response Time	Target Resolution Time
1	The Services are unavailable at a single Customer site. E.g., there is no connectivity service available at a single Customer site.	1 hour	8 hours
2	The Services are degraded at a single Customer site. E.g.: • a single Edge Device or single internet tail is unavailable at a resilient site but site connectivity is still operational;	2 hours	12 hours

	• an Incident which is intermittent in nature is affecting a non-resilient site but connectivity is still available.		
3	Any other Incident associated with the Services	4 hours	2 working days
4	Request for information	16 hours	10 working days

3.3 Service Requests

- Jisc Internal Centralised Management Portal for configuration changes, performance reports, and monitoring.
- 24/7 Service Desk for incident management, change requests, and technical support.

If the Customer requests a change to the Services before the Services Commencement Date, Jisc may revise the Services Commencement Date to accommodate that change.

Jisc will commission the Services during Working Hours on Working Days. When Jisc advises the Customer of the Services Commencement Date, the Customer will carry out the Acceptance Tests in accordance with this Agreement.

Any additional installation services requested by the Customer outside the scope of the site survey may be subject to additional charges. Additional installation services will be priced using Jisc's professional services rates, available on request.

4. Appendix

Schedule 1 (Services description)

Overview of Managed SD-WAN services

The Services provide a complete WAN connectivity service using the latest "SD-WAN" technology. This will enable the Customer to build private data networks that connect their sites with applications and resources on the network, in data centres, or in the cloud, using only conventional internet access circuits.

The Services include the supply of WAN connectivity, FortiGate firewall equipment and licences, installation and maintenance, in-life managed services, and professional services for deployment and service management. Jisc provides Managed SD-WAN in partnership with BT on Fortinet's FortiGate platform.

WAN connectivity

WAN connectivity is end-to-end and includes a choice of suitable internet access circuits connected to FortiGate firewall device(s):

Internet access circuit	FortiGate firewall device	Auxiliary hardware
Btnet	Customer Premises Equipment (CPE) as per Order Details within Cover Letter	As per Order Details within Cover Letter
Broadband One (BB1)		Draytek modem to be used as pass-through adaptor for SOGEA underlay internet access circuits
Bring Your Own Bearer (BYOB)		As required and to be supplied by Customer
The port speeds listed in the Order Form(s) are available in varying increments based on ethernet speeds. The Customer acknowledges that due to network and IP overheads, the actual throughput that the Customer experiences during speed tests or IP application usage will be lower than the ethernet line speed and port speed selected. The reduction is typically 5-10%. The actual figure will vary depending on the IP application the Customer is using and is not fixed or guaranteed.		

Btnet

BTnet is a leased line internet service delivered across BT's dedicated leased line Internet Access service. As a leading network provider in the UK BT have unparalleled experience in delivering internet connectivity and solutions to all types of business.

BTnet is available with bearers and port speeds ranging from 1Gbps to 10Gbps. The Service is delivered using a high speed, highly resilient access platform and is accessible through over 1700 access nodes across the UK.

Broadband One (BB1)

Broadband One is a platform offering UK wide coverage and speeds of up to 1Gbps. The Service offers a strong foundation for Customers now and is the first step towards an all-IP future.

Broadband One will provide the Customer with an internet access service available in a range of options and delivered over a compatible access line using traditional copper wiring, fibre optic cabling or a combination of both (depending on the geographical area where the internet access service is provided).

Bring Your Own Bearer (BYOB)

Bring Your Own Bearer (BYOB) provides the flexibility to utilise your existing underlay network from an alternative provider of your choice. When BYOB is deployed, the Customer has the responsibility to ensure that the internet access circuit has sufficient capacity to terminate on the FortiGate firewall device. The Customer may need to provide Auxiliary hardware, dependent on internet access circuits type.

Fortinet SD-WAN (via FortiGate firewall device)

The SD-WAN implementation leverages a shared core Fortinet FortiGate firewall as the headend device, located within Jisc's datacentres and a separate Fortinet FortiGate firewall appliance as CPE edge devices, architected in a hub and spoke network design.
Fortinet's FortiAnalyzer and FortiManager appliances are used for management and analytics of the WAN.

The FortiGate headend device is tasked with handling SD-WAN traffic and provides a secure overlay network, enabling access to Janet and the internet.

For branch sites, the solution establishes IPSec tunnels back to the headend device. This setup ensures that Unified Threat Protection (UTP) is enhancing the security of network communications for those Customers that opt for a 'secure' service. For Customers that have alternative network security arrangements, Managed SD-WAN is configured with a 'standard' configuration, without UTP.

Depending on the underlying WAN connectivity, additional Auxiliary hardware might be deployed to handle specific termination requirements. Key considerations for branch deployments include user-count and throughput for either the standard or secure service.

The Customer will be provided with a Service that:

- delivers a security-driven networking WAN edge transformation through SD-WAN, advanced routing and WAN optimization capabilities.
- provides UTP license for the duration of the of Service when specified in the Order Form for the secure service option.
- provides traditional Layer 4 firewall to be utilised to secure the service where appropriate, along with enhanced capabilities at layer 7. Firewalling will be enabled by UTP and the secure service option.
- enables explicit firewall rules to be utilised which will be determined at the point of design.

Multisite(s) SD-WAN

Multisite SD-WAN enables the routing of Customer traffic from one or more Customer branch sites to another main Customer site via overlay tunnels between sites. Where the standard configuration routes single sites traffic directly to Jisc's headend, this functionality allows direct communication between multiple Customer sites. The Customer will need to ensure they have considered their network requirements correctly to size FortiGate firewall device(s) as well as provide the network topology prescribing which sites are branches and which are hubs. In a multisite configuration, traffic to the internet will route via hub sites to the Janet network.

Application Aware Routing

When specified in the Order Form, the Customer will be provided with a facility that manages Customers traffic and Applications to improve the efficiency of their network 'Application Aware Routing'. The Customer will be able to categorise certain Applications as business critical through the Customer's own pre-defined categories, subject to the limitation of WAN connectivity and network design.

Any changes to the categorises will be dealt with as a change request. Application Aware Routing will work optimally if there are multiple WAN connectivity configured to a FortiGate firewall device.

Managed Services

The core infrastructure which underpins the Managed SD-WAN service, and responsibilities for it are shown below.

A check mark (✓) indicates services provided by Jisc									
Category	Description	Location / Premises	Estate Mgmt	TACACS permission admin	BAU Support	Implement Changes	Monitor and event management	Provision of Back Up Mechanism	In Life Configuration Back Up
Operating System	Forti-Manger VM	**Jisc**	✓	✓	✓	✓	✓	✓	✓
Operating System	Forti-Analyser VM	**Jisc**	✓	✓	✓	✓	✓	✓	✓
Software	Forti-Manger application	**Jisc**	✓	✓	✓	✓	✓	✓	✓
Software	Forti-Analyser application	**Jisc**	✓	✓	✓	✓	✓	✓	✓
Logical element	"SD-WAN VDOM(s)" ADOM(s) on FMG	**Jisc**	✓	✓	✓	✓	✓	✓	✓
Logical element	"SD-WAN End-Customer Group" ADOM(s) on FMG	**Jisc**	✓	✓	✓	✓	✓	✓	✓
Logical element	All other Customer ADOM(s) on FMG	**Jisc**	✓	✓	✓	✓	✓	✓	✓
Hardware & Software	7000-E & 6001-F Chassis	**Jisc**	✓	✓	✓	✓	✓	✓	✓
Logical element	"SD-WAN VDOM(s)" on 7000-E & 6001-F	**Jisc**	✓	✓	✓	✓	✓	✓	✓
Logical element	All other Customer VDOM(s) on 7081-F & 6001-F	**Jisc**	✓	✓	✓	✓	✓	✓	✓
Hardware & Software	SD-WAN End Point Firewalls or switches (CPE)	**Customer**	✓	✓	✓	✓	✓	✓	✓

	(FortiGate(s) on Order Form)								
Hardware	SD-WAN End Point converter (Draytek Vigor 167 on Order Form) (CPE)	**Customer**	Hardware Replacement only – not an intelligent device.						
Network Underlay	BTnet	n/a	n/a	n/a	✓	n/a	✓	n/a	n/a
Network Underlay	BT BroadBand1	n/a	n/a	n/a	✓	n/a	✓	n/a	n/a

Managed SD-WAN technical responsibilities

The Managed SD-WAN related activities and data would be hosted in the UK, and the management platform used to store the data and systems would be administered by UK administrators.

The Customer shall be provided with services and functionalities as outlined in the Order Form. Two options are available: Managed SD-WAN standard and Managed SD-WAN secure.

	Managed SD-WAN service options	
Technical responsibilities	Standard	Secure (UTP required)
Hosted Control Infrastructure	✓	✓
VPN	✓	✓
Firewall Intrusion Detection and Prevention	n/a	✓
Firewall Anti-Virus	n/a	✓
Firewall Anti-Bot	n/a	✓
Traditional Layer 4 firewalling	n/a	✓
Application Control	n/a	✓
Ad Hoc professional services	On request	On request

Jisc / BT shall provide the Customer with and fulfil responsibilities including:

Hosted Control Infrastructure

- orchestrate the delivery of the Service;
- monitor in real time the SD-WAN network and the performance of the devices on the Order Form and on Jisc premises;
- identify issues, inefficiencies or delays with the SD-WAN network;
- troubleshoot issues with the SD-WAN network; and
- view data flows across SD-WAN network and Sites.

VPN

Jisc / BT will set up and configure the following types of VPNs in accordance with its technical standards:

- remote access VPNs, for remote Users to gain access to the Janet network and the internet;
- implement Jisc's rules to authenticate the User's access against Jisc's authentication server; setup up to three VPNs, additional VPNs can be requested; and
- management access VPNs from BTs DMZ to each of Jisc's Sites to manage and administer the Service.

Firewall Intrusion Detection and Prevention (UTP licenses required)
Jisc / BT has the responsibility to purchase and manage the security licence subscription for the Customer which will perform UTP for the individual SD-WAN CPE edge devices. Jisc / BT will via UTP:

- monitor traffic passing through Customer's` SD-WAN CPE edge device for attacks, in accordance with the applicable intrusion signature files;
- implement this Service with a default configuration setting, including a standard intrusion signature list;
- as part of the Customer's subscription, manage the intrusion signature updates;
- apply the signature updates following issue to Jisc / BT by the SD-WAN device vendor of the detection software;
- block high impact or high confidence attacks as defined in the CSP; and
- disable the appropriate signature (or signature group if necessary) if the Customer advises Jisc / BT of a conflict with any of Customer's legitimate business traffic.

The Customer acknowledges that Jisc / BT will not:

- make changes to the standard signature list;
- evaluate the signatures before applying them; and
- monitor, provide alerts or service specific reports outside of the generic monitoring, alerting or summary reporting.
- If the Customer requests Jisc / BT to alter the parameters for applying new signatures in "block" mode (default mode set for blocking potential attacks), the Customer will accept responsibility for the increased risk of false positives (blocks to legitimate traffic) or the increased risk of attacks being missed.

Firewall Anti-Virus (UTP licenses required)
Jisc / BT will, via UTP:

- check web browser (http) traffic for known malware;
- inspect requests from Users for an executable file from a site on the Internet, against the current antivirus definition file set out in the applicable intrusion signature files. If no virus is detected, the file will be passed to the User. If a virus is detected the file will be blocked and deleted; and
- keep antivirus definition files up to date by regular downloads direct from Fortinet (firewall supplier).

Firewall Anti-Bot (UTP licenses required)
Jisc / BT will via UTP check and block outbound traffic for communication with known command and control servers used by owners of malicious software.

Traditional Layer 4 firewalling (UTP License required)
Traditional Layer 4 firewall will be utilised to secure the service where appropriate, along with enhanced capabilities at layer 7 which will be via the UITP licensing.

- The explicit firewall rules to be utilised will be determined at the point of design via the SD-WAN CSP.
- A total of 50 firewall rules per site across traditional Layer 4 and through to Layer 7 firewalling.
- Any additional firewall rules post design requires a change request and will be chargeable.

Application Control (UTP licenses required)
Jisc / BT will via UTP:

- Apply the Application control policies to control the consumption of WAN bandwidth by applications and ensure maximum bandwidth availability for critical applications.
- For application control policies, refer to the SD-WAN CSP. A maximum of 10 application control policies are included.

Ad Hoc professional services
- Jisc / BT can provide ad hoc technical support, chargeable per day, upon request for services that are out of scope of this Service Description.
- Ad Hoc professional services are delivered remotely.
- It should be noted that the transition of existing Customer(s) / end Customer group(s) to a different architecture (for example, a multisite architecture), may require a change controls.

Customer Security Policy (SD-WAN-CSP)
Jisc / BT will maintain a set of security rules that define the Service, which are pre-templated and may change periodically, "SD-WAN CSP". These rules are applied to the FortiGate firewall device(s) to determine the Service operation.

SSL Inspection
SSL inspection is supported but it will be the Customer's responsibility to provide the required SSL certificate.

Service Onboarding
In addition to the details provided in the Cover Letter, this section describes service onboarding. If the Customer requests a change to the Services before the Services Commencement Date, Jisc may revise the Services Commencement Date to accommodate that change.

Jisc will commission the Services during Working Hours on Working Days. When Jisc advises the Customer of the Services Commencement Date, the Customer will carry out the Acceptance Tests in accordance with this Agreement.

Any additional installation services requested by the Customer outside the scope of the site survey may be subject to additional charges. Additional installation services will be priced using Jisc's professional services rates, available on request.

Support Services

Jisc will provide access to the Jisc Service Desk so the Customer can log Tickets in response to Incidents. The Customer will be able to log Tickets at all times.

Jisc will respond to and use reasonable endeavours to resolve an Incident if the Customer reports an Incident with the Services during the Service Coverage Period.

Support services will consist of remote support and, where necessary, on-site support. If the Customer requests on-site support outside of the Service Coverage Period, this may incur additional charges.

Jisc may carry out maintenance from time to time and will use reasonable endeavours to inform the Customer at least 10 Business Days before any planned maintenance to the Services. However, Jisc may inform the Customer with less notice where emergency maintenance is required or where Jisc has not been provided sufficient notice by a third party supplier.

Jisc may provide software updates, configuration management and patch management on Jisc Equipment from time to time.

Jisc can provide ad hoc, remote, technical support on request. Charges for these services are available on request.

Additional Jisc Security services

When access is provided to Janet, the Services include the following security services:

Foundation DDOS

Jisc monitors traffic across Janet for unexpected patterns indicating a DDoS attack. If an alert is triggered, traffic to the address under attack is re-routed via the mitigation scrubbing centre. Attack traffic is filtered out using carefully selected criteria and benign, business-as-usual traffic continues to flow to and from your Services.

Foundation DDoS Protection shall be available during the Service Coverage Period. DDoS mitigation applies only to traffic transiting the Customer's WAN connectivity service.

The protection mechanisms are designed to detect and mitigate distributed denial-of-service attacks targeting the SD-WAN overlay and associated logical endpoints. They do not extend to, or provide protection for, the underlying IP bearer circuits or any other internet-facing services the Customer may operate.

Janet Network Resolver Service (JNRS)

JNRS acts as a protective DNS forwarder for your entire infrastructure. It prevents your devices and network from accessing known malicious or compromised domains. Our security analysts and specialists work closely with the National Cyber Security Centre and other security researchers to create response policy zone (RPZ) feeds that block malicious domains. These feeds are continuously curated by our cyber threat intelligence team, ensuring that the Janet network resolver can adapt to emerging threats.

Access to Jisc's Cyber Security Community

Jisc's Cyber Security Community is a collaborative Microsoft Teams group run by the community, for the community. It provides timely threat intelligence and vulnerability alerts, monthly webinars, training and awareness (with on-demand content) and a space for sharing best practice. Customers also benefit from access to practical guidance documents, templates, and other resources designed to strengthen cyber resilience across the community.

Limited access to Cyber Security Incident Response Team (CSIRT):

Access to Jisc's highly skilled CSIRT is provided on a reasonable endeavours basis, offering limited advice and guidance via ticketed support during the Service Coverage Period. This service includes:

- Janet IP traffic monitoring to support the Customers' incident investigation;
- Network edge containment to block inbound internet access during major incidents.

Access to Cyber Threat Intelligence (CTI) services:

The cyber threat intelligence team identifies, analyses and disseminates the intelligence that underpins all of Jisc's cyber security activities. In addition, the team works closely with Jisc's incident response and defensive services teams, responsible for DDoS mitigation and defence of the Janet Network.

Using in-house expertise alongside commercial and open-source services, threats and vulnerabilities impacting education and research sectors are monitored, tracked and notified. We work closely with institutions, national agencies and international partners to share actionable threat intelligence to help protect the Janet Network and connected organisations.

Schedule 2 (Service Levels)

Jisc will use reasonable endeavours to provide the Services in accordance with the following Service Levels.

The target response and target resolution times will commence following a 30 minute period (which will commence when Jisc has issued the Customer with a Ticket).

These Service Levels will not apply where the recommended User limit advised by Jisc is exceeded or where there is a fault with Jisc's head-end Fortinet device. The recommended User limit for each connection type is available on request.

Incident resolution service level objectives for sites utilising BTnet:

Priority Level	Description of impact of Incident	Target Response Time	Target Resolution Time
1	The Services are unavailable at a single Customer site. E.g., there is no connectivity service available at a single Customer site.	1 hour	6 hours
2	The Services are degraded at a single Customer site.	2 hours	10 hours

	E.g.: • a single Edge Device or single internet tail is unavailable at a resilient site but site connectivity is still operational; • an Incident which is intermittent in nature is affecting a non-resilient site but connectivity is still available.		
3	Any other Incident associated with the Services	4 hours	2 working days
4	Request for information	16 hours	10 working days

Incident resolution service level objectives for sites utilising Broadband One:

Priority Level	Description of impact of Incident	Target Response Time	Target Resolution Time
1	The Services are unavailable at a single Customer site. E.g., there is no connectivity service available at a single Customer site.	1 hour	8 hours
2	The Services are degraded at a single Customer site. E.g.: • a single Edge Device or single internet tail is unavailable at a resilient site but site connectivity is still operational; • an Incident which is intermittent in nature is affecting a non-resilient site but connectivity is still available.	2 hours	12 hours
3	Any other Incident associated with the Services	4 hours	2 working days
4	Request for information	16 hours	10 working days

Availability service level objective:

Site Type	Services Target Availability	Services availability coverage	Services repair coverage
Resilient ethernet based site	99.9%	24x7x365	Working days 8am-6pm
Non-resilient ethernet based site	99.5%	24x7x365	Working days 8am-6pm
Non-resilient broadband based site	99.0%	24x7x365	Working days 8am-6pm

Service Level Exclusions

Where a Customer chooses the Bring Your Own Bearer (BYOB) as a WAN connectivity type for the Service, the Service Level clock shall be paused during any period in which the restoration of

service is dependent on information or actions from the Customer or any third-party service providers. This includes, but is not limited to, delays caused by:

- Awaiting necessary information or approvals from the Customer.
- Actions or inactions of third-party service providers, including but not limited to circuit providers, that are beyond the control of the Jisc / BT.

Schedule 3 (Terms and Conditions)

The Service Terms and Conditions are included with our G-Cloud 15 Service Listing.

Schedule 4 (Data Protection)

The contact details of the Customer's data protection officer will be provided by the Customer. Jisc's data protection officer details are:

- Email: dataprotection@jisc.ac.uk

Processing Personal Data – the Services

Description	Details
Identity of Controller for each category of Personal Data	The Parties acknowledge that in accordance with the Data Protection Legislation, both Parties are independent Controllers.
Duration of the Processing	The duration of the Agreement plus 7 years post Agreement expiry.
Nature and purposes of the Processing	In respect of the Customer's Personal Data for which Jisc shall act as an independent Controller, Jisc may: collect, collate, share, evaluate, use, store, replicate, and otherwise Process the Personal Data (subject to the terms of the Agreement) to enable it to administer and fulfil its obligations under the Agreement. This may include: ● complying with requirements under the Agreement to contact named individuals; and ● including Personal Data within reports. <u>Services Related</u> The Services provide the Customer with a communications service. Jisc Processes any information that is generated by the User's use of voice mail, voice recording, text messaging features and web browsing. Given that recordings can be made and stored, any type of Personal Data could be captured or provided inadvertently by the User. Any access to the content of such communications by Jisc is strictly in accordance with Applicable Law.

	Jisc's suppliers, including any sub-Processors of Jisc's suppliers, may from time to time use back-office support and system functions which are located or can be accessed by Users from outside of the UK and/or the European Economic Area. Any such Processing will be in accordance with Data Protection Legislation, including with respect to appropriate data transfer mechanisms. The Customer consents to the disclosure and transfer Personal Data, as required in order to provide the Services.
Type of Personal Data	name; gender; date of birth; email address; address; telephone number; associated persons; contact notes from calls; contact records; Personal Data traffic and communications records; Browsing time; IP address; Website history. This list is not exhaustive as the Customer will specify what Customer Personal Data is processed.
Categories of Data Subject	Users; Third party participants in voice calls or text messages to and from Users; Customer staff.
Plan for return and destruction of the data once the Processing is complete unless requirement under law to preserve that type of data for a different duration	Duration of the Agreement plus 7 years post Agreement expiry.

Schedule 5 (Subcontractor Acceptable Use Policy and EULA)

Part 1 – EULA
https://www.fortinet.com/content/dam/fortinet/assets/legal/EULA.pdf

Part 2 – Subcontractor Acceptable Use Policy

Use of the Service

1.1 You will not use the Service in breach of Applicable Law or your obligations in the contract to respect human rights, or otherwise in any way that BT reasonably considers to be:

1.1.1 fraudulent or dishonest;

1.1.2 detrimental to any person or in a manner which violates or otherwise encroaches on the rights of others (including rights of privacy and free expression);

1.1.3 detrimental to the provision of services to you or any other BT Customer; or

1.1.4 damaging to BT's brand or reputation.

1.2 You will not use the Service to take, or attempt to take, any action that is intended to:

1.2.1 transfer files that are, contain or are made up of viruses, worms, Trojans, distributed denial of service, any back door or time-bomb or other harmful programmes or software designed to violate the security of BT, any other person or company; or

1.2.2 prevent, block or obstruct access to any programme installed on, or data saved in, any computer or damage or harm the operation of any of these programmes or the reliability or accuracy of any of this data.

1.3 Unless agreed with BT first in writing:

1.3.1 you will only use the Services, and will ensure that your Users only use the Services, for the commercial and business purposes for which they have been designed (including as may be described in the Schedule to your Contract);

1.3.2 you will not, and will ensure that your Users will not, modify, amend, change, reconfigure or otherwise repurpose all or any part of the Services for uses other than those pursuant to Paragraph 1.3.1 above; and

1.3.3 you will only provide access to the Services to your Users. If BT consents to the provision of the Services to third party users in accordance with this Paragraph 1.3 you will ensure that any such third party users comply with the terms of this AUP.

Use of Materials

2.1 You will not create, download, receive, store, send, publish, transmit, upload or otherwise distribute any material, including information, pictures, music, video or data, that BT reasonably considers to be:

2.1.1 harmful, immoral, improper, indecent, defamatory, offensive, abusive, discriminatory, threatening, harassing or menacing;

2.1.2 promoting or encouraging of illegal, socially unacceptable or irresponsible behaviour, or that may be otherwise harmful to any person or animal;

2.1.3 in breach of the intellectual property rights of BT or any other company or person, for example by using, distributing or copying protected or 'pirated' material without the express permission of the owner;

2.1.4 in breach of the privacy or data protection rights of BT or any other person or company; or

2.1.5 in contravention of any licence, code of practice, instructions or guidelines issued by a regulatory authority.

2.2 You will ensure that all material that is derived from the machines or networks that you use in connection with the Service is not in breach of this AUP.

Systems and Security

3.1 You will not:

3.1.1 take any action that could:

damage, interfere with, weaken, destroy, disrupt, harm, violate, disable, overburden, overtake, compromise, hack into or otherwise adversely affect any computer system, network or the internet access of the BT Network or network of any other person or company; or

adversely affect or tamper with BT's security, the BT Network or any system or security network that belongs to any other person or company.
3.1.2 access any computer system or network belonging to any person or company for any purpose without permission, including to probe, scan or test the security of a computer system or network or to monitor data traffic;
3.1.3 connect the BT Network to machines, equipment or services that do not have adequate security protection or that are able to be used by others to carry out conduct that is not allowed by this AUP; or
3.1.4 collect, take or harvest any information or data from any BT services, BT's system or network or attempt to undermine any of BT's servers or systems that run BT services.

Communicating using the Service

4.1 When using any Service that allows you to communicate with others, including by phone, email or instant message, you will not:
4.1.1 communicate in any way that BT reasonably considers to be:
spam;
causing annoyance, inconvenience, distress, offence or anxiety to any person (for example, hoax calls);
likely to damage, harm, ruin or affect the enjoyment of any person; or
offensive on the grounds of race, sex, religion, nationality, disability, sexual orientation, age or any other similar categorisation;
4.1.2 impersonate or otherwise misrepresent another person, or help others to do the same, which includes faking, forging or hiding email headers, subjects, sender details or caller ID details;
4.1.3 send unsolicited communications such as unsolicited bulk emails or text messages, 'mailbombs', nuisance calls or advertising; or
4.1.4 send any emails, make any calls or communicate with any other person or company in any way that may suggest, indicate or imply that you are employed by BT.

Responsibilities of the account holder

5.1 Your use of the internet is at your own risk and you will be responsible for:
5.1.1 your use of the internet, including any material that you access through the internet, and any websites or pages that you own, run or control using the Service;
5.1.2 all material that is stored on, or accessed or distributed by the devices that you use in connection with the Service; and
5.1.3 making sure, when sharing the internet over a private network on your premises, that your network is secure and that any internet connection sharing software that you use does not permit access from outside of your network.
5.2 You accept that the internet is never completely private or secure and that any data or information that you send using the Service may be read or intercepted by others.
5.3 You will make sure that your computer systems, network and equipment have the appropriate security software installed, such as up-to-date virus protection and firewalls, so that they are protected against viruses, worms, Trojans and other risks and so that others cannot access them without your permission or interrupt your use of the Service and BT will not be responsible for any negative consequences that occur as a result of your failure to install appropriate security software.

BT's rights and responsibilities

6.1 BT may monitor:
6.1.1 material available on the internet or the activities of other internet users; or

6.1.2 any material that belongs to another person or company and that you may be able to access through the Service.

6.2 BT will not guarantee that all material accessed through the Service is free of illegal content or content that is otherwise considered unacceptable, inappropriate or offensive.

6.3 If BT is aware, or reasonably believes, that you have breached this AUP, BT reserves the right to take any action it deems appropriate including:

6.3.1 investigating the possible breach and using your personal details to contact you by email or phone to gather further information, discuss BT's concerns, or issue you with a formal warning; and

6.3.2 running network and computing systems to find and resolve issues covered by this AUP.

How to get in touch

7.1 If you have any questions about this AUP, you can contact BT using the methods set out at www.bt.com/contact.

7.2 If you suspect that someone has breached the terms of this AUP and you would like to report or make a complaint about their use of BT services, please email abuse@btbroadband.com.