Service Definition

Managed Networks

G-Cloud 15

Contents

Managed Network Services Overview

Fujitsu provides a set of comprehensive Managed Network Service solutions for clients.

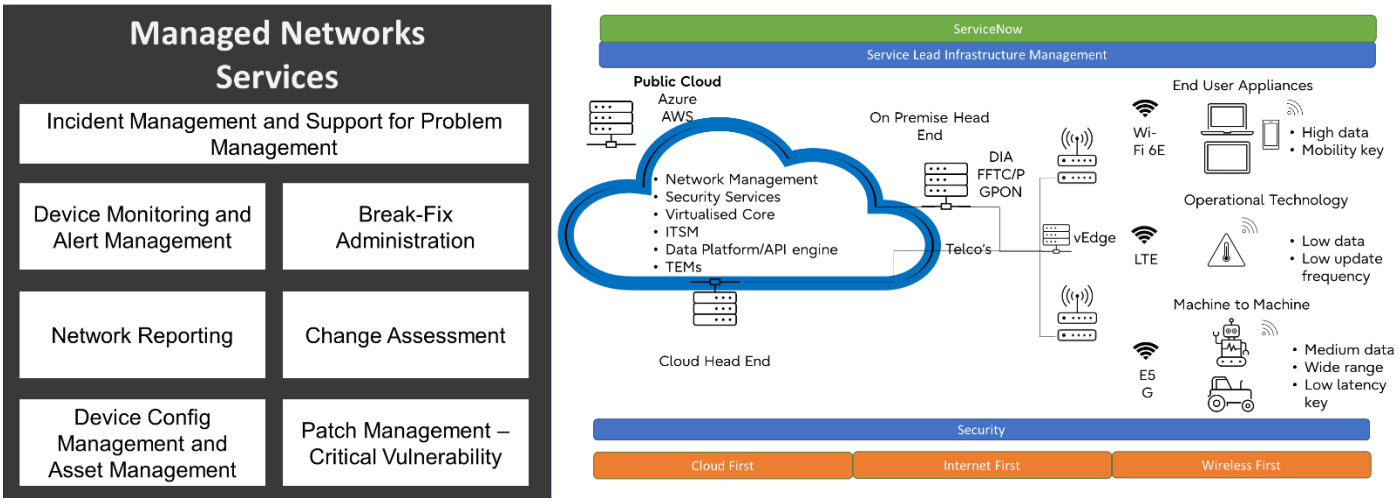

Figure 1: Managed Network Services Overview

OT-IT, Cloud, Hybrid IT, Artificial Intelligence, and Virtualisation have made the network the critical component to achieve these key organisational strategic objectives.

Fujitsu Managed Network Service provides the ability to support our customers' key objectives by offering:

- A standardised offering to offer the same tangible results and deliverables no matter what the strategy and technology used.
- Differentiated offering because only Fujitsu can offer a true "end to end" solution, which can include IoT, Cloud, Hybrid IT, Big Data, Artificial Intelligence, and infrastructure virtualisation utilising Fujitsu technologies and know how.
- True Customer Transparency because Fujitsu's toolsets allows our customers to understand in real time how IoT, Cloud, Hybrid IT and virtualisation is affecting their networks.
- Automation & Orchestration because Fujitsu's toolsets offers complete operations and customer automation including assets defined in the CMDB & Service Catalogue to become availability and delivered in real time.
- Critical Network Analytics Fujitsu's toolsets can also provide instant Capacity Management (ITIL aligned) and control utilising real time data from the network.
- Truly agility platforms for:
  - Legacy & new virtualised networks – no matter what the technology, Fujitsu can offer the ability to manage transparently a client's infrastructure in new & exciting ways
  - ITIL capabilities – it isn't about "it's aligned to ITIL", it's about "how does my Managed Network enable me a competitive advantage"

Fujitsu's key resources and capabilities can offer our prospects, clients and customers a unique offering into the market, by mixing our unique skills, knowledge and understanding of the IT and Communications environment for all verticals. This is because during our interaction with our clients, we gain knowledge and understanding of how technologies can enable our clients to achieve a Competitive Advantage. Examples of these capabilities are illustrated where Fujitsu has leveraged network technologies for IoT capabilities within the Utilities vertical; enabling these organisations to achieve both a price leadership position in connectivity; whilst utilising the technology to provide an agile infrastructure that can adapt within hours to environmental

changes; and as a platform for IoT devices to understand the analytics behind Telemetry data and as a platform for the evolution of SCADA technology– which will be key to their strategic direction. Enabling our clients to stay ahead of the pack and achieve a significant Competitive Advantage.

The aim of Fujitsu's Managed Network service is to maintain high-quality network connectivity and performance whilst offering the ability to response to competitive pressures. Fujitsu also offer innovate solutions, for example, Fujitsu's new Managed Service for Software-Defined WAN (SD-WAN) which offers the ability to virtualize your Wide Area Network. Enabling the ability to rapidly deploy new applications, services, and offering to the market. Whilst at the same time reduce costs by removing hardware and support costs by the virtualization of your network.

In summary, the Fujitsu Managed Network service provides:

- 24-hour by 365 days monitoring and incident management from our secure UK Network Operations Centres (NOC)s
- Escalated network issues managed by Fujitsu's Network Operations Centres (NOCs) technical & operational specialists.
- Proactive incident management and response; restoring service in accordance with Fujitsu's committed Service Level Agreements.
- Order Management for end-to-end service provision
- Customer dashboard providing near real-time network status data to help customers understand how well their network and surrounding IT is performing. With Network reviews, planning and consultancy to optimize the network performance and proactive identify possible future issues, utilizing knowledge of how applications are impacting the network.
- Routine Service Management and maintenance modifications
- Change Management – expert assessment of non-routine service modifications
- Out-tasked and outsourced operations – for customers wishing to retain ownership of their existing or new network assets Fujitsu can provide the skills that professionally and economically deliver the right Managed Network operation.
- Public Cloud Access – Fujitsu's core networks are already extended to Fujitsu's and the mainstream public clouds, allowing effortless integration of cloud-based applications into your private network. Enabling secure access to public Cloud offering between Amazon Web Services and Microsoft Azure.
- Ability to monitor and manage key WAN metrics such as Availability, Latency, Jitter and Packet Loss for critical application support.

Fujitsu Managed Network Service: Our service provides seamless management of end-to-end networks when combined with our best-in-class Managed service product portfolio:

- Managed Network WAN - wide area network access services including SD-WAN, MPLS and Broadband
- Managed Network LAN - building secure corporate, public and private network including guest access networks across retail, leisure and corporate office markets.
- Managed Network Private 5G - offers secure, high-speed, and reliable private 5G network solution

Fujitsu's Network & Security Operations centres: Our UK-based NetSec operation centres manage our wide range of connectivity components for the Managed Network service. These two centres operate under strict security controls to ensure the management of the network connectivity is not compromised. The NOCs are where our expert engineers operate the services through the deployment of our standard tools, capabilities and methodologies. They confirm impact and engage third parties if needed using integrated workflows and escalation paths. In addition, we utilize Fujitsu's in house skills and services to deliver a network solution which will drive the value from your investment in IT, whether extending the life of existing assets, investing in new infrastructure, or making the transition to new hybrid IT architectures.

Why Choose Fujitsu?

- The complete network service from design to operate – from committed professionals
- Dedicated UK and offshore Network Operations centers – serving you wherever you are
- Network monitoring 24 hours a day, every day – resolving issues before they can impact your operations
- The strength of a world class systems integrator – our network solutions deliver seamless support for your operational processes
- The power of partnership – Fujitsu work with innovative partners to create the best network experience for your operation.

Fujitsu offer comprehensive and bespoke Managed Network services addressing all matters relating to the set-up and operation of highly efficient corporate & campus networks, from planning through to maintenance and security. Whatever the complexity of your requirements, Fujitsu can provide a single source of expertise and experience. From managing your migration to Voice over IP (VoIP) to deploying high quality LAN, WAN, SAN or MPLS VPN environments, Fujitsu offer the levels of performance your business expects, while driving down cost.

Fujitsu will meet your network demands by:

- Delivering constant network availability and high performance
- Ensuring flexibility and scalability to meet future requirements
- Reducing operating and administrative costs
- Minimising risk and maximising security
- Supporting data centre consolidation
- Increasing application performance.

Fujitsu can offer expertise in all of the following areas, building on the network infrastructure to enhance and develop a network and security solution:

- Design, Implementation and Support for network and security platforms from leading vendors
- Design, implementation, and support for Centralised Infrastructure Management Platforms
- Enhanced proactive security support services for Security Auditing and Accounting
- Identity and Access Management
- Network Monitoring and Management, including Single Pane of Glass Dashboards on any user device showing traffic levels, with options for advanced analytics on flows (netflow/jflow/sflow etc) and applications, Enhanced SLA monitoring and reporting, BOXI alert analysis, SSH, SSL VPN and proprietary software clients
- Network Diagnostics.

Scope

Managed Network Service Deliverables

The service consists of the following service elements:

- Device Monitoring and Alert Management (Standard)
- Incident Management and Support for Problem Management (Standard)
- Break-Fix Administration (Standard)
- Network Reporting (Standard)
- Patch Management – Critical Vulnerability - Standard
- Change Assessment (Standard)
- Device Config Management, Device Backup & Restore and Asset Management (Standard)

The Service will comprise all Service Elements and be the full scope of the services.

Unless provided for within this Contractual Service Description, any variation to the Services will be managed as a Change, in accordance with the Change Control Procedure.

The performance of these Services will be delivered during the Support Hours unless stated otherwise in this Contractual Service Description. The delivery of the Network Managed Service shall commence on the completion of Acceptance of the Service by the Customer and by Fujitsu.

Please request a copy of the Fujitsu Managed Network Services Contractual Service Description for the full set of terms and conditions associated with this service.

Device Monitoring and Alert Management

The Supplier shall Monitor the Customer Network Devices as defined and agreed by The Supplier and the Customer. Fujitsu will monitor the following data point on in scope devices where the device enables the information to be collected using SNMP.

- Device Availability derived from Internet Control Message Protocol (ICMP) and/or Simple Network Management Protocol (SNMP) events, traps or signals.
- Data packet errors in
- Data packet errors out
- Data latency
- Network Device memory utilization
- Network Device CPU utilization
- Temperature status
- Netflow/IPSLA- This service is available for an additional charge. The number of flows required shall be agreed with the Customer via the approved Change Control Procedure
- Wi-Fi data – where the technology deployed enables this.

The Services contained herein shall be delivered to the Customer from the Supplier's remote locations. The Supplier shall use its current Network Management infrastructure to facilitate the remote monitoring and management of the Customer Network Devices.

Incident Management and Support for Problem Management

The Supplier shall perform Incident Management against the reported or Monitored Incident during the Service Hours set out in this service definition.

In the event of a Customer Network Device being reported in an error state, the Supplier shall attempt to resolve the Incident by following the Supplier's current Incident Management process. The Supplier shall undertake some or all the steps below in order to attempt resolution of the Incident:

- Incident Triage against current known errors log.
- Remote diagnosis.
- Refer the Incident to non-network teams in the Supplier.
- Refer the Incident to the Suppliers support teams and partners of the Supplier or the Customer (in the event of the Customer holding circuits directly)

The Supplier shall restore the Customer Network Device to the last known working state; this shall include any Connected Communication Services that are included in the CE Schedules for which the Supplier is responsible.

The Supplier shall appoint an engineer resource from a shared support team who shall have reasonable awareness of the Customer Network Solution and shall be available to support the Incident and Problem Management process the Supplier will provide Firmware upgrades as part of Incident management

For this Service Element, the Supplier shall only undertake Firmware or Software upgrades to The CE if required in order resolve an Incident.

Any charges associated with a Firmware or Software upgrade to The Customer Equipment, such as but not limited to:

- Hardware upgrades
- Memory upgrades
- Licence upgrades

These shall be referred to the Customer prior to the charge being incurred for approval, this process shall be carried out through the current Supplier Change Control Procedure.

If Firmware or Software upgrades are not possible due to limitations of The CE such as, but not limited to:

- Insufficient memory available.
- It is deemed by the Supplier that the Firmware or Software upgrade represents a significant risk to The Customer's service.
- The CE is no longer supported by the manufacturer.

In such a case, the Supplier shall suspend or reject the Incident and refer the matter to the Customer Representative

Failure to resolve incident – follow up actions:

If after Incident or Problem Management work has been completed but the Incident remains unresolved. the Supplier shall pass the Incident Record and therefore ownership of the resolution of the Incident to the responsible service organisation For onward progression and resolution

Break-Fix Administration (Standard)

The Supplier shall include Break-Fix Administration which is the management of the invocation of the Break-Fix provision. For the avoidance of doubt, the operation of Break-Fix provision, which is the physical attendance to interrogate, replace, store, or recover Network Devices, is not included in this Service or its charges.

The Supplier shall perform Break-Fix Administration against the reported or Monitored Incident during the Service Hours set out in the Service Hours section of this document.

The Supplier shall manage the Break-Fix Administration of the Customer Network Devices defined in the CE Schedules.

If a Customer Network Device hardware failure is identified by the Supplier, the Supplier will manage the replacement of the Customer Network Device in accordance with the Customer's Break-Fix agreement.

The Supplier's Break-Fix Administration shall include:

- Verification with the Customer contact of the access details for the Customer Site where the failed Customer Network Device is located. This shall include site address, health and safety requirements, escorting requirements for the engineer, access time and date.
- Obtain details of a Customer Representative on the Customer Site where the failed Customer Network Device is located. This shall include name, contact telephone number, email address.
- The arrangement of an engineer to visit the site with the engineering team supporting the Customer.
- The arrangement of a replacement part to replace the failed Customer Network Device.
- Once the failed Customer Network Device has been replaced or returned to service and the Supplier can remotely access and manage the replacement Customer Network Device, the Supplier shall attempt to restore the last known working configuration.
- On successful restoration of the failed Customer Network Device the Supplier shall verify with the Customer Contact that Service has been restored.

Network Reporting (Standard)

The Supplier shall provide the Customer with access to the Reporting Portals. This shall include:

- Web addresses or IP Addresses for the service.
- Account information including usernames and passwords.
- Any training requirements – the charge for this is a factor of location, duration and frequency required and may be charged separately, a price for which shall be made available on request.

The Supplier shall provide the Customer with read only access for one Customer User to a report dashboard, so that the Customer may view the Supplier defined reports. The data reports available via the dashboard shall not be presented in real time.

All and any of the items below that feature in a report shall only be made available providing all aspects of the Customer Network Solution support such features and functions.

The Reporting of the Customer Network Devices (where available) shall provide the following event and Threshold reports:

- CPU Utilisation
- Memory Utilisation
- Device reachability (availability)
- Interface utilisation/Traffic volume
- Traffic volume aggregated (all interfaces' volumes aggregated)
- IPSLA reporting (where service is taken by customer): Highest IPSLA Jitter, Highest IPSLA Jitter Response Times, Worst IPSLA response time, Worst IPSLA MOS (Mean Opinion Score), Worst IPSLA ICPIF (Calculated Planning Impairment Factor)
- Flow reports (when Netflow service is taken by the customer): Top Client, Top Talker, Top Conversations plus direction, Type of service plus direction, Top Flow plus next hop.

Patch Management – Critical Vulnerability (Standard)

The Supplier shall provide two levels of Patch Management. Firmware upgrades are included as part of Incident management within Service Element 2. Service Element 5 consists of:

- Patch Management – Critical Vulnerability (Standard)
- Patch Management – Recommended Baseline (Optional)

Service Element Patch Management – Critical Vulnerability (Standard)

In the event of a notification being received from a Vendor of a critical vulnerability, devices may be required to be patched to maintain the recommended security of the Network.

- In the event of a notification being received from a Vendor of a critical vulnerability, the Supplier will perform an impact assessment and inform the Customer of any required remedial activity.
- If the impact assessment determines that this is a critical vulnerability, then the patch shall be deployed by the Supplier using the Patch Management process.

Service Element 5B Patch Management – Recommended Baseline (Optional)

The Customer will be advised of this as part of the impact assessment. The Customer may purchase the Supplier Patch Management – Recommended Baseline Service to keep the devices at a suitable level or they may purchase upgrades on an adhoc basis as a project as part of the Change Control procedure.

The Supplier will provide a recommended baseline for the network estate based on a Vendor approved patching cycle. This will be defined at the transition stage of the contract as part of due diligence.

Change Assessment (Standard)

The Supplier shall provide:

- Impact assessments for Service Changes raised on the Supplier's managed change system during the Service Hours stated in the Service Levels / Service Hours table below.
- Supplier originated Requests For Change shall be communicated to the Customer using the Change Control Procedure.

Where a Request For Change is deemed by the Supplier to be too complex for the Change Assessment process, then the Supplier shall contact the Customer Representative to progress elsewhere and reject the original change. Requests For Change that may be rejected as too complex may include but not be limited to:

- Changes to the attributes of the network solution or devices that is deemed by the Supplier to add risk to Service.
- Changes that the Supplier deems are significant to require project management to implement.
- Changes to the Approved Network Design.

Device Config Management, Device Backup & Restore and Asset Management (Standard)

The Supplier shall provide the following.

Device Config Management, Backup and Restore:

- Implementation of Changes to the Customer Network Devices configuration as listed and approved in the Supplier's managed change system during the agreed implementation hours listed for the change.
- Daily automated backup of the device configuration state (changes) to the Supplier's configuration management platform.
- Initiate manual backups as part of post change activities, as requested via the Supplier's managed change system.
- The ability for the Supplier to view, access and compare the latest and historical backed up device configuration state from the Supplier's configuration management platform.
- The restoration of a historical configuration under either a Change listed and approved in the Supplier's managed change system or under an Incident being managed in line with Service Element 2 Incident Management

Asset Management: Supplier shall hold a database of the identifying characteristics of a Customer Network Device, such as Vendor, Model and serial numbers, Firmware versions etc.

Service Delivery

Service delivery shall commence on the completion of Acceptance of the Service by the Customer.

Service Management

Fujitsu shall provide the Customer with performance and capacity management reports monthly by email for the Network Devices that are subject to the Network Managed Service and where such reports are available.

Fujitsu shall provide the Customer with one 30-minute phone conversation or online web-based session per month to assist the Customer understand the performance and capacity management reports.

Fujitsu shall provide the Customer with ability to escalate problems and incidents, the escalation process shall be requested via a Service Desk service which must be separately procured if required.

Security and Information Assurance

ISO27001:2017: The Fujitsu NOC Facilities are certified to ISO27001:2017, certificate number UK002399,

As a trusted organisation, Fujitsu holds the following certifications:

ISO9001:2015 certificate number: UK 011583 Version 18 Dated 12/04/2022 (this supersedes the below)

BS EN ISO 9001 Quality Management

- ISO 9001:2008 Certificate - Fujitsu UK & Ireland
- ISO 9001:2008 Certificate for Defence & Security

ISO/IEC 20000 Service Management

Multi-site certificate across Europe ISO/IEC20000-1 2018 V3 3/3/2022

ISO/IEC 27001:2013 Information Security Management

Certificate No. IND.21.736/IS/U Version: No.1 Issue date: 6-Jan-2022 this is now a multi-site certificate which supersedes the below:

- ISO/IEC 27001:2013 Certificate - Fujitsu UK & Ireland
- ISO/IEC 27001:2013 Certificate - Fujitsu DPS (Document Processing Solutions)

Cyber Essentials Scheme Specification

- Cyber Essentials Scope whole of organisation dated 4/03/2022 Certificate ref IASME-CE-037570
- Cyber Essentials Plus Scope whole of organisation dated 1/04/2022 Certificate ref IASME-CEP-008648

PCI Certificates: PCI DSS version 3.2.1 on 16/12/2021

ISO 14001: 2015 Environmental Management: Certificate No.: UK012503 Version: 2 Issue date: 15-12-2021

BS OHSAS 18001 Occupational Health & Safety Management: superseded by ISO45001 2018

BS 10500 Anti-Bribery Management (ABMS)

ISO 22301 Business Continuity Management: ISO 22301: 2019 Issued 11/04/2022

CAS(T) - CESG Assured Service (Telecommunications)

HMRC Authorised Economic Operators (AEO): Certificate GB/AEO/C/00032/14

IIP Gold (Investors In People)

Operational Sustainability (Tier III Data Centres)

CESG Pan Government Accreditation Certificates

PSN Connectivity Service Compliance

PSN Service Provision Compliance certificate: Fujitsu Services Ltd - SRV_0405

EMEIA Wide ISO/IEC 27001 Information Security Management

- EMEIA ISO 27001 Statement of Applicability
- EMEIA ISO27001 Detailed Scope Document

Business Continuity

The specific Offering does not directly deal with customer data and does not include business continuity support. Fujitsu will engage with customers regarding their data needs and dependent on the stated requirements propose appropriate solutions. Fujitsu offers a range of Framework Offerings including Backup As A Service and Managed Infrastructure Services which include the ability for customer data to be backed-up and restored.

Training and Consultancy

Training is not applicable to this Service.

Consultancy services covering aspects such as design, due diligence etc. may be provided by Fujitsu at the Customers request. Fujitsu shall provide a quotation for such services, the price for which shall be calculated using the rates displayed in the Managed Network Service Professional Services Days Rates table in this Service Definitions Pricing section, plus any other reasonable expenses.

Additional Service Options

The options associated with this Service are as follow, a price quotation for which shall be made available on request:

- Design
- Implementation
- Service Desk
- Break/Fix Engineer and part to site
- Equipment specification and procurement
- Telecommunications provider management, order and ongoing support for WAN products such as Wholesale Ethernet, Business DSL, MPLS, Wavelength Networks, Internet Service Provision.

Service Levels

Service Hours

Service Element	Service Hours
Device Monitoring and Alert Management	24 hours per day, 7 days per week by 365 days per year
Incident, Service Request and Support for Problem Management	Incident Severity 1: 24 hours per day, 7 days per week by 365 days per year Incident Severity 2,3,4,5: 08:00 to 18:00, Monday to Friday excluding weekends and public holidays
Break-Fix Administration	Incident Severity 1: 24 hours per day, 7 days per week by 365 days per year Incident Severity 2,3,4,5: 08:00 to 18:00, Monday to Friday excluding weekends and public holidays
Network Reporting	08:00 to 18:00, Monday to Friday excluding weekends and public holidays
Patch Management – Critical Vulnerability	08:00 to 18:00, Monday to Friday excluding weekends and public holidays
Change Assessment	Emergency Change Assessment: 24 hours per day, 7 days per week by 365 days per year Change Assessment: 08:00 to 18:00, Monday to Friday excluding weekends and public holidays
Device Config Management, Device Backup & Restore and Asset Management	Device Configuration Management, Backup and Restore: 24 hours per day, 7 days per week by 365 days per year Asset Management: 08:00 to 18:00, Monday to Friday excluding weekends and public holidays

Table 1: Service Hours

Incident Severity Definitions

Severity Level	Description	Target First Response Time	Resolution Times
1	Network Incident resulting in the failure of multiple Customer Sites (total loss of data transmission for the affected Sites) or complete loss of service for 100+ users.	30 minutes	4 hrs.
2	Network Incident resulting in the failure of a single Site or total loss of service for multiple users.	1 hour	8 hrs.
3	Network Incident resulting in the total loss of service for a single user.	4 hours	2 days
4	Non-total loss of service, including loss of resilience that is not service affecting.	1 day	5 days
5	This is used to cover change, Service Requests, advice & guidance requests, where a client does not have a separate formal toolset to record such activities. No Service Level applies to this severity.	N/A	N/A

Table 2: Incident Severity Definitions

Note:

1. Performance measurement against the Resolution Time begins at receipt of Incident by the Supplier Service Management System (inclusive of all Incident Information) and until it is recorded as Resolved on the Supplier Service Management System
2. No Service Levels apply to a Service Request. The Supplier will support it on a reasonable endeavours' basis
3. The Service Level clock for measuring performance against the Resolution Time will only operate during the Service Hours and will be subject to the stop the clock principle where the time required to Resolve an Incident extends beyond the Service Hours

Commercials

Minimum and Maximum Terms

The minimum term for an ordered Managed Network service shall be 12 months from the date of Customer Acceptance.

The maximum term for an ordered Managed Network service shall be 60 months from the date of Customer Acceptance. Thereafter the Managed Service shall be renewed monthly, or re-ordered subject to the minimum term.

Customer Responsibilities (Specific to Service Elements)

Please request a copy of the current Fujitsu Managed Network Service Contractual Terms for details of Customer Responsibilities.

Customer Dependencies (Specific to Service Elements)

Please request a copy of the current Fujitsu Managed Network Service Contractual Terms for details of Customer Dependencies

Customer Obligations (Specific to Service Elements)

Please request a copy of the current Fujitsu Managed Network Service Contractual Terms for details of Customer Obligations.

Customer Dependencies (Specific to Service Elements)

Please request a copy of the current Fujitsu Managed Network Service Contractual Terms for details of Customer Dependencies.

Service Constraints

This service is subject to a minimum order quantity of 50 devices.

About Fujitsu

As one of the world's leading IT companies, Fujitsu is at the forefront of pioneering technology in the UK since we made our initial investment over 40 years ago. As a key strategic partner we deliver essential services, from our secure hybrid IT which underpins critical national infrastructure to our investment in emerging technologies to boost national capability. Drawing on our Japanese technology expertise we provide bespoke digital transformation solutions. This unrivalled expertise has allowed us to specialise in emerging focus areas; Hybrid IT, AI & RPA, Data analytics, Agile application development/transformation and Security. Together, we offer a full package of solutions to support the UK as a long-term industry supplier.

We believe in realising the significant alignment between the UK and Japan in emerging technologies and in creating a UK-Japan 'Innovation Bridge' to support the UK's science and technology superpower objectives. We are committed to investment in UK skills and research and development, driving customer outcomes and promoting social value. We employ 124,000 people around the globe, including around 8,000 people across the UK, promoting diversity and inclusion as a DWP Disability Confident Leader. We are recognised as a Times Top 50 employer for Women since 2017, a Stonewall Top 100 Employer for 2023 and were awarded an EcoVadis Silver Rating, the world's largest provider for sustainability ratings.

Contact: government.frameworks@fujitsu.com