JT Managed WAN

Service Description

1.0 Document Information

1.1 Legal Notices

1.1.1 Copyright

1.1.2 Terms

This document does not constitute an offer capable of acceptance by the Customer and is subject to agreement of a formal contract. No contractual relationship shall arise until a formal contract has been signed by both parties.

This document is provided in addition to and must be read in conjunction with the JT's Support Service Terms & Conditions, which are available online at https://www.jtglobal.com/global/terms-conditions/. Unless otherwise specified, terms used in this document shall have the same meaning as defined in the above Support Service Terms & Conditions.

2.0 Overview

2.1 Managed Service

The offer is available with three levels of service:

1. Support Services – these are the break-fix maintenance services. Hardware and software maintenance is undertaken by the JT engineering team and/or approved JT partners. The support services are underpinned by Service Level Agreements that are aligned to Customer's overall managed service solution.
2. Remote Monitoring Service – intended to support Customers by detecting, and managing the resolution of service issues, mitigating any impact to critical business operations. The managed service combines monitoring with incident, event and service management. This can be used where Customers do not have the resource, or do not wish to buy the tools to monitor their system.
3. Proactive Managed Service – this service is multifaceted – its main purpose is to ensure uninterrupted operation by resolving issues before they arise. It provides intelligence regarding network utilization and traffic visibility via a client access web portal.

The service provides 24x7x365 remote management and monitoring for Customers' solutions. JT manages the environment utilising our comprehensive ISO27001-cerfitied, Information Technology Infrastructure Library ("ITIL") aligned service management framework (the "Managed Service").

The proactive Managed Service includes proactive configuration, monitoring, performance and capacity management and access to JT's support capability, technical skills and vendor relationships. The table below shows the service elements available in each of JT's standard service offerings:

Service Element	JT Service Offering		
	Support Service	Remote Monitoring	Proactive Managed Service
Due Diligence	Yes	Yes	Yes
Service Transition	Yes	Yes	Yes
T2 Service Desk	Yes	Yes	Yes
Incident Management	Yes	Yes	Yes
Break/Fix Parts Maintenance	Yes	Yes	Yes
Problem Management	Yes	Yes	Yes
Change Management	Yes	Yes	Yes
Billing	Yes	Yes	Yes
Service Monitoring	No	Yes	Yes
Configuration Management	No	Yes	Yes
Partner Management	No	No	Yes
Patch/Release Management	No	No	Yes
Capacity Management	No	No	Yes
Service Level Management	No	No	Yes
Asset Management	No	No	Yes
Security Management	No	No	Yes
Service Catalogue Management	No	No	Yes
Remote management of applications	No	No	Yes
24x7 Performance, Availability, Capacity and Alert Monitoring	No	No	Yes
Experienced and vendor-certified engineers	No	No	Yes
Service based on ITIL Framework	No	No	Yes
ISO27001-certified operation	No	No	Yes
Managed monitoring, response, and incident management	No	No	Yes
Daily Configuration Back-ups and maintenance of system documentation	No	No	Yes
Ongoing Administration and Configuration	No	No	Yes
Comprehensive Monthly Service Reporting	No	No	Yes
Change/Release Management	No	No	Yes

2.2 Key Responsibilities

The table below shows the JT and Customer key responsibilities for the different services:

Activity	Support Service	Remote Monitoring	Proactive Managed Service
System Monitoring	Customer	JT	JT
Hardware Fix/ Replacement	JT	JT	JT
Configuration Backup and Restoration	Customer	Customer	JT
System Backup and Restoration	Customer	Customer	JT
Moves, adds and changes	Customer or JT on request	Customer or JT on request	JT
Firmware and Software Patches	Customer or JT on request	Customer or JT on request	JT
Incident Management & Problem Management	Customer	JT	JT
Reporting	Customer	Customer	JT

3.0 Service Description

3.1 Supported Platforms

The Wide Area Network ("WAN") Managed Service is delivered to the Customer's premises via a Customer Edge ("CE") device. The CE devices are provided and exclusively managed by JT. Customer monitoring access is evaluated on a case-by-case basis. The CE devices have the following features:

(a) Native Quality of Service ("QoS") support for up to 6 traffic classes;

(b) Two-factor authentication;

(c) Single global Virtual Routing and Forwarding ("VRF") per device. The deployment of more VRFs is at JT's discretion;

(d) Demarcation point – Customer-facing Local Area Network ("LAN") interface of the CE device;

(e) Off-site CE configuration backup; and

(f) Remote monitoring and management.

The table below outlines the supported network CE devices that JT can manage:

3.1.1 Supported Devices

Vendor	Model	Status
Cisco	All current production routers	Supported
Cisco	All current production switches	Supported
Versa Physical Appliance	Versa, Dell, OEM (e.g. Advantec)	Supported
Versa Physical Appliance	Supported hypervisors	Supported

3.2 WAN Managemens

3.2.1 Supported Configurations

Configuration	Status
Single Connected Site (Either Multiprotocol Label Switching (“MPLS”) or Direct Internet Access (“DIA”))	Supported
Hybrid Connected Site MPLS with DIA as back-up	Supported
Dual Connected Branch Site (Either MPLS or DIA)	Supported
Dual Connected Data Centre Site (MPLS)	Supported

3.2.2 Customer Requests

The table below outlines specific tasks that are included as part of the WAN Managed Service. All tasks are performed during business hours (08:30 – 17:00 Monday to Friday, excluding Bank Holidays in Jersey (“Business Hours”)). If the Customer requests an implementation outside of Business Hours, the changes will need to be communicated in advance and may be chargeable.

Task	Description
Circuit Bandwidth Upgrade	Change of bandwidth where the circuit upgrade can be achieved via a policy change and is not service affecting.
Creation and Management of Prefix or Access List	Creation, change and deletion of prefix or access lists configured in the device.
Management of LAN IP Addresses	Creation and changes on the CE LAN interface parameters (IP addresses, subnets, gateways)
Creation and Management of Static Route	Creation, change and deletion of static routes configured in the CE device.
Creation and Management of QoS	Creation, change and deletion of QoS class-maps or policy-maps.
Creation and Management of Simple Network Management Protocol, version 3 (“SNMPv3")	Creation, change or deletion of SNMPv3 community strings for Customer monitoring if agreed in design.
Hostname Change	Change of CE device hostname.
Log and SNMP system configuration	Management of the log information resending to a syslog server and SNMP alerts/traps
Output of commands	Provision of output from privileged exec commands or running configuration.
Management of manufacturer's guarantee	Management of hardware or firmware errors with the manufacturer. Customer needs to contract a valid manufacturer support for this management to be effective and Customer needs to require JT to open a support case.
Restore of data	Restore of device configuration from the backup.

3.2.3 Periodic Maintenance

Task	Frequency	Description
Firmware Review	Yearly	Notification to the Customer of the outstanding firmware patches that need to be applied to the device. In case the Customer wants to proceed and install the patches, a maintenance window will be agreed, and JT's team will install the requested patches.
Backup Review (Cisco devices only)	Following backup	Review of the correct execution of the associated configuration backup. In case there is an error with the execution, its handling will be considered an Incident and as such, it will be solved as soon as possible.

3.2.4 Availability Monitoring

Monitors are used to evaluate the condition of the host or virtual machine ("VM") and then perform an action when a threshold is reached. If the alerts are related to non-managed elements (such as the VMs or the physical devices if their management has not been contracted) these will be escalated to the Customer.

Monitor Name	Description	Default Alarm Threshold	Action
Ping / Network	Time taken for responding to a ping from a poller and packet loss	300ms round trip time or 25% packet loss error	Internal teams will solve the issue
CPU	CPU use of the device	80% total use	Internal teams will diagnose and try to solve the issue and escalate to the Customer if needed
Memory	Memory use of the device	90% of physical memory	Internal teams will diagnose and try to solve the issue and escalate to the Customer if needed with information about what processes are using the memory
Disk	Disk usage in %	85% Disk usage	Internal teams will investigate the issue
Interfaces	Check the device interfaces (virtual or physical)	Interface is down	Internal teams will solve the issue

3.2.5 QoS

All services provided over JT's MPLS network have the capability of supporting QoS. The below classes of service are configurable within a WAN Managed Service router, if a switch is used for the CE devices then there may be restrictions dependant on the device model. JT will work with the Customer to define their requirements during technical workshops.

IP Prec	Class Name	PHB Value	Application	
5	Voice	EF	• Real time data flows, low Jitter (SLA) • Low latency priority queuing • Burstable to subscribed limit	• Jitter sensitive applications, i.e. voice
4	Video	AF4	• Video applications/ priority applications • Class based weighted fair queuing • Burstable to port speed	• Video applications or business critical applications, i.e. SAP, POS, PeopleSoft, etc.
3	Critical Data	AF3	• Mission critical data flows • Class cased weighted fair queuing • Burstable to port speed	• Business critical applications, i.e. Citrix, SAP, POS, PeopleSoft, etc.
2	Interactive Data	AF2	• General data flows (latency sensitive) • Class based weighted fair queuing • Burstable to port speed	• Telnet, Extranet Web Apps, General Data Apps
1	Standard Data	AF1	• General data flows • Class based weighted fair queuing • Burstable to port speed	• FTB, database synchronisation, web surfing
0	Low Priority Data	Best Effort	• General Data Flows • Class Based Weighted Fair Queuing • Burstable to Port Speed	• Email

3.3 Network Device Patching

JT will apply patches to the Customer's environment in accordance with the Customer's change control procedure. JT will perform regular audits on the supported configuration items to identify which patches are available to be installed. JT will apply patches in accordance with vendor best-practice, subject to the agreed priority with the Customer and available maintenance windows. JT's technical management team will consider both the risk and benefits of applying patches or updates. Patches will only normally be applied if the following conditions are met:

(a) The patch is needed to resolve an incident or problem.

(b) The patch is needed to address a security vulnerability that the affected configuration item is exposed to.

(c) The patch is categorised as mandatory by the vendor.

(d) The patch is required to ensure supportability by the vendor.

Other updates and patches can be applied but are subject to additional charges and are agreed by the service delivery manager.

4.0 Management Requirements

4.1 Access

In order to provide the Managed Service, JT requires network link(s) into the Customer's infrastructure as necessary for JT's monitoring tools and the remote engineering management access. Unless access is available via a JT managed MPLS connection, the Customer is responsible for the installation of the access links and CE devices required to enable monitoring as well as providing all necessary authorisation for JT to manage the third party transport circuits on the Customer's behalf. All expenses (costs, fees, etc.) associated with the third-party providers are the Customer's responsibility.

CE devices – JT will supply CE routers from the JT-supported hardware matrix as part of the Managed Service, unless specified by the Customer; hardware installation and support will be JT's responsibility.

Monitoring – JT must have remote monitoring access to the WAN Managed Service CE devices. JT will install the monitoring access configuration required for the WAN Managed Service. Requests for Customer or third-party monitoring access is evaluated by JT on a case-by-case basis.

Management – JT retains exclusive management of all WAN Managed Service CE devices. All configurations are JT's intellectual property.

4.2 General Customer Responsibilities

For all three types of transport services (JT on-net, JT off-net and third party provided transit) the Customer is responsible for:

(a) The integration of the WAN with the LAN infrastructure – the WAN Managed Service demarcation point is the LAN-facing interface of the WAN Managed Service CE device.

(b) Customer Premise Equipment/LAN service incident resolution.

(c) Informing JT of any work or changes which may impact the operational status of the WAN Managed Service CE devices or remote access to the WAN Managed Service CE devices.

(d) Securing the operational environment to host the WAN Managed Service CE device on Customer premises (sufficient rack space, power, cooling, cabling, etc.) as per CE device manufacturer specification.

(e) Allowing in-band service access and management. Additional out-of-band management access will be reviewed on a case-by-case basis and will be at the Customer's expense.

(f) Accepting the JT-allocated WAN IP address space

(g) Providing JT with a user account with delegated administrative read-write permission to the CE device. SNMP v2 or v3 read-only credentials are required for standard monitoring and alerting.

5.0 Service Management

The following services are provided as part of the Managed Service:

(a) Incident management.

(b) Incident resolution and recovery.

(c) Incident closure.

(d) Hardware/software support*.

(e) Configuration management.

"Incident" means any event which is not part of the standard operation of the Managed Service and which causes, or may cause, an interruption to, or a reduction in the quality of, the functionality of the Managed Service.

*Third party support contracts must be in place but may be supplied by either JT or the Customer. Where the Customer owns the third-party support contract it must be on a 24x7x4hour on-site basis to conform to our standard JT Service Level Agreement **("SLA")**.

5.1 Service Desk

The JT Service Management Centre ("SMC") is the central, first point of contact for all incidents and enquiries related to the Managed Service. The JT service desk ensure that all calls are dealt with efficiently and professionally and are integrated into the highly experienced and dedicated team of engineers trained to industry recognised standards.

Customers have multiple ways to access the SMC. They can raise Incidents via the following methods:

(a) Send an email to a dedicated support address; or

(b) Call the service desk through a dedicated telephone number.

Regardless of the process that is used to raise an Incident, all calls are logged into our central service management tool and a unique reference number issued for ease of tracking).

5.2 Incident Management

JT's Managed Service enables Customers to leverage the industry best practice processes that are followed within JT's SMC to manage the resolution of Incidents as efficiently as possible.

Based on ITIL best practice processes, the goal of Incident management is to restore normal service operation as quickly as possible and minimise the adverse impact on business operations, thus ensuring that service quality and availability are maintained.

The SMC is responsible for managing the entire Incident life cycle until service has been restored and the issue completely resolved.

Incidents can be created automatically in response to monitoring system alerts or manually in response to issues detected either by the SMC or reported by the Customer.

Incidents are assigned a priority based on the impact and urgency of the issue, when an Incident is deemed a Priority 1 call, as defined by the priority matrix (in section 6.2.2 below); a call is raised and assigned to the relevant third line team.

A lead engineer is assigned to the call, and, if necessary, will call upon other third line technical specialists to assist in identifying the root cause, or issue a workaround whilst investigations continue.

Where an in-house resolution is not possible, third line engineers will liaise with the appropriate third-party support vendors/partners to ensure a fix or workaround is supplied and service restored as soon as possible, to minimise further disruption.

Once the Priority 1 call has been resolved, the JT service desk will update the Customer.

5.3 Incident Logging

All Incidents shall be logged with the JT service desk using the following contact information: By email:

globalsupport@jtglobal.com

By telephone:

Channel Island: **+44 1534 882345 option 1 option 1 (24x7x365)**

Please note JT recommends that the Customer logs any Priority 1 Incidents via telephone.

To enable a prompt response to a logged Incident, the service desk will require the following information:

(a) Company Name

(b) Circuit reference or Device ID or serial number.

(c) Any corresponding Incident reference.

(d) Name of person reporting the Incident.

(e) Technical site contact, if different from the person reporting the Incident.

(f) Contact information, direct dial, mobile and any alternative numbers.

(g) Affected configuration Item.

(h) Description of the symptoms

The Incident will be logged on the JT Incident management system and the JT service desk will provide the Customer with an Incident reference number. The Incident will then be assessed considering configuration item type, priority etc. and will be assigned to the appropriately-skilled engineer for investigation.

JT bases Incident recording on ITIL principles. JT will record the following information in order to best track the history of an incident from registration through to resolution:

(a) unique ID of the Incident;

(b) date and time of recording;

(c) service desk agent responsible for the registration;

(d) caller/user data;

(e) description of symptoms and priority level;

(f) product category (selected from a category-tree), e.g. server;

(g) Incident category (selected from a category-tree), e.g. database error, program error;

(h) links to related problem records;

(i) description of activities undertaken; and

(j) resolution and closure time and date

6.0 SERVICE LEVEL AVAILABILITY

There are two principal measures of service performance that are the foundation of JT's Managed Service:

1. Availability and performance of the technical infrastructure that underpins the Managed Service; and
2. Operational performance of the JT Managed Service teams, in particular the SMC.

6.1 Service Avaialbility

The availability of the Managed Service is dependent on the resilience inherent in the overall solution design. Where elements exist that are outside of JT's control and these impact the availability of the Managed Service, JT reserves the right to exclude these from the availability calculation. In the case of 3G/4G being used as backup connectivity, this is subject to the ad-hoc nature of cell tower signal conditions and other factors.

Site Availability	Availability
Single Connected Site DIA	95%
Single Connected Site MPLS	99.5%
Dual Connected Site DIA	99.5%
Hybrid Connected Site MPLS with DIA	99.9%
Dual Connected Site MPLS	99.99%
Dual Connected On-Net Data Centre Site MPLS	99.99%

Standard Avaialbility Table

Availability %	Downtime per year	Downtime per month	Downtime per week	Downtime per day
99% ("two nines")	3.65 days	7.20 hours	1.68 hours	14.4 minutes
99.50%	1.83 days	3.60 hours	50.4 minutes	7.2 minutes
99.80%	17.52 hours	86.23 minutes	20.16 minutes	2.88 minutes
99.9% ("three nines")	8.76 hours	43.8 minutes	10.1 minutes	1.44 minutes
99.95%	4.38 hours	21.56 minutes	5.04 minutes	43.2 seconds
99.99% ("four nines")	52.56 minutes	4.38 minutes	1.01 minutes	8.66 seconds
99.999% ("five nines")	5.26 minutes	25.9 seconds	6.05 seconds	864.3 milliseconds

6.2 Service Performance

6.2.1 Incident Response Times

The table below outlines the standard SLA for the Managed Service.

	Proactive Outage Notification	Response	Resolve (Target)	User Update Interval	Availability
P1	15 minutes	15 minutes	6 hours*	1 hour	**24 x 7 x 365**
P2	15 minutes	60 minutes	8 hours*	4 hours	**24 x 7 x 365**
P3	NA	120 minutes	12 hours	6 hours	**24 x 7 x 365**
P4	NA	240 minutes	5 days	1 day	**Business Hours**
MACD	NA	1 day	5 days	5 days	**Business Hours**

*These targets are Business Hours and dependant on the third-party support contracts being in place. To meet these resolution targets JT requires all infrastructure to have an associated 2-hour x 24 x 7 on-site hardware SLA.

6.2.2 Priority Levels

JT uses the following classification of priorities in the below Priority Matrix:

Priority 1 Major Disruption	Definition	Major Business Impact: outage with no workaround resulting in complete loss of core services to Customer. • Service unavailable to all users with no possible workaround; or • Vital business function(s) severely impacted
	Example	• *Data centre or office complete outage causing all critical business systems to become unavailable.*
Priority 2 Significant Disruption	Definition	Significant Business Impact: outage with no workaround resulting in significant loss or degraded system services to Customer; however, operations can continue in a restricted mode. • Service functionality or performance is severely impaired; • Majority of users are unable to access the service; or • Vital business function(s) impacted.
	Example	• *Site outage and failover to backup service causing degraded performance/access to critical business systems.*
Priority 3 Minor Disruption	Definition	Minor Business Impact: degraded system performance or issue with workaround. • Functionality or performance is degraded but the service is still usable; • More than 75% of users are able to access the service with no significant impact; or • Vital business functions are not impacted.
	Example	• High latency or Jitter on an MPLS service impacting application performance.

6.2.2 Priority Levels (cont.)

Priority 4 Superficial	Definition	Minor or No Business Impact: Minor or cosmetic fault (does not impact the capability, functionality or productivity of the system or service) or a Move/Add/Change. • Small number of users impacted
	Example	• *Transient high utilisation of a host CPU.*
Move, Add, Change, Delete ("MACD") Customer Request	Definition	No Business Impact: (does not impact the capability, functionality or productivity of the system or service). • No users impacted
	Example	• *Change of Description on a port, Change of a VLAN on a port.*

6.3 Operational Performance

6.3.1 Incident Response & Resolution Targets

The following target response and resolution times will be used as Key Performance Indicators ("KPIs").

Priority Level	Response Time	Status Updates	Availability	Target Resolution
Priority 1 Incident	15 minutes	Every 30 minutes	24 x 7 x 365	6 hours*
Priority 2 Incident	2 hours	Every 2 hours	24 x 7 x 365	8 hours*
Priority 3 Incident	4 hours	Every 24 hours	24 x 7 x 365	12 hours
Priority 4 Incident	8 hours	By request from customer	Business hours	5 days
MACD request	8 hours	By request from customer	Business hours	5 days

* These targets are based on Business Hours which will be further defined in the Customer Statement of Work and dependant on the third-party support contracts in place. To meet these resolution targets JT requires all infrastructure to have an associated 2-hour x 24 x 7 On-site hardware SLA.

6.4 Escalation procedure

An escalation shall be triggered when the Customer's representative expresses concern relating to the handling of one of more Incidents, changes or problems. JT shall log and track all escalations via the escalation team and assign each of them to an owner. In the event that the escalation level 1 representatives (as detailed in the table below) is unable to resolve the escalation satisfactorily, then the escalation shall be then promptly assigned to the escalation level 2 representatives (as detailed in the table below). Escalation shall continue through the hierarchical layers detailed in the table until resolution is achieved.

6.4 Escalation procedure

An escalation shall be triggered when the Customer's representative expresses concern relating to the handling of one of more Incidents, changes or problems. JT shall log and track all escalations via the escalation team and assign each of them to an owner. In the event that the escalation level 1 representatives (as detailed in the table below) is unable to resolve the escalation satisfactorily, then the escalation shall be then promptly assigned to the escalation level 2 representatives (as detailed in the table below). Escalation shall continue through the hierarchical layers detailed in the table until resolution is achieved.

Level	Business Hours	Outside of Business Hours
Escalation level 1	Service Desk Analyst	Service Desk Analyst
Escalation level 2	Assignment Group Team Leader	Duty Service & Problem Manager
Escalation level 3	Assignment Group Manager	On Call Duty Manager
Escalation level 4	Service Delivery Manager ("SDM")	On Call Senior Manager
Escalation level 5	Head of Service and Delivery Management	On Call Senior Manager

6.5 Service Credits

If JT fails to achieve the agreed service level, with no external or mitigating circumstances and a service credit is due in accordance with the terms of the applicable Statement of Work, the applicable service credit will be issued. Service credits are only applicable to the services provided by JT as detailed in the Statement of Work agreed between JT and the Customer.

7.0 Service Delivery

The Managed Service is delivered in accordance with industry best practice standards and leverages JT's highly experienced engineering teams. It includes:

(a) Problem Management;
(b) Change Management;
(c) Release and Patch Management;
(d) Configuration Management; and
(e) SDM*.

* Dependent on size of deployment

7.1 Problem Management

Problem Management helps to identify the underlying cause of Incidents and issues and commonly requires changes to be applied to a Customer's infrastructure to address a root cause.

The SMC will conduct a root cause analysis of all critical Incidents that affect Managed Service delivered by JT. Where underlying causes can be resolved by changes to a customer's infrastructure, such changes will be managed through the SMC Change Management process. Where underlying causes cannot be resolved, the SMC will maintain a known error log against such problems so that future Incidents can be managed more efficiently.

The Problem Management process enables the SMC to apply knowledge gathered across its entire customer base to be applied to individual customer infrastructure services. In this way, JT can proactively address potential issues with a customer's infrastructure in advance of incidents actually arising.

7.2 Change Management

The objective of Change Management within the SMC is to ensure that standardised methods and procedures are used for the efficient and prompt handling of all changes to a customer's infrastructure.

By following a standard process, JT is able to minimize the risks associated with making changes to the WAN Managed Service customer's infrastructure and therefore reduce the number of Incidents.

(a) Change requests may arise reactively in response to problems or through externally imposed requirements.

(b) Authorised representatives of the Customer can request changes under the scope of service contracted.

(c) All change requests are subject to technical review by the SMC engineering team.

(d) The SMC will agree priorities for all change requests with the Customer.

(e) All change requests have defined acceptance criteria and back-out plans agreed with the Customer before being executed.

(f) The SMC uses the service desk application to manage the workflow of change management.

Whilst the SMC operates its own Change Management Board, integration with the Customer's own change management process is critical to the successful operation of the Customer's infrastructure.

7.2.1 Change Control Process

JT initiated changes

JT's nominated contact will notify the Customer's nominated contact of any planned changes to the solution at least ten (10) Business Days (Monday to Friday excluding Bank Holidays in Jersey ("**Business Days**")) before changes are made.

Planned Works

JT will endeavour to perform maintenance (or non-emergency works) during maintenance windows agreed with the Customer. "Normal Maintenance" refers to: (a) upgrades of hardware or software; (b) upgrades to increase capacity; or (c) other scheduled network activity. JT will use reasonable efforts to perform all normal maintenance during a maintenance window mutually agreed with the Customer. JT will use its reasonable efforts to restrict service-affecting maintenance to a maximum of two (2) per month. To minimise Customer impact, JT will choose the most appropriate day to carry out this maintenance. JT shall endeavour to contact the Customer a minimum of five (5) Business Days prior to non-service affecting maintenance and a minimum of ten (10) Business Days prior to service affecting maintenance. Any outages that form part of Normal Maintenance activity will be excluded from the availability calculation.

The procedures for Change Control will be as follows:

(a) All changes to be initiated by JT to the Customer equipment that has the potential of changing user functionality or cause a risk to the operability of the service will be fully documented by JT using the change control form.

(b) A ticket is raised using a change ticket reference in JT's service desk system.

(c) JT will notify the Customer's nominated representative of plans to change the effected equipment and/or services.

(d) Any Customer reference should be documented in the change ticket.

(e) Once the change is complete, JT will confirm that the changes that were made successfully with the Customer's nominated representative. The service desk ticket will remain in a resolved state until the Customer confirms it can be closed or for a maximum of three (3) days.

Service Incidents

"Emergency Works" refers to efforts to correct certain network conditions that may be occurring that require immediate attention. Emergency Works, while being carried out, may degrade the quality of service and may result in total disruption of service. JT may undertake Emergency Works at any time it deems necessary in its sole discretion. JT shall provide notice where possible to the affected Customer as applicable in accordance with the section above.

The procedures for Change Control in the event of a service Incident will be as follows:

(a) A ticket is raised using an incident ticket reference in JT's service desk system.

(b) JT will notify the Customer's nominated representative of plans to change the effected equipment and/or services.

(c) Once the change is complete, JT will confirm that the changes that were made have restored service to agreed levels with the Customer's nominated representative. The service desk ticket will remain in a resolved state until the Customer confirms it can be closed or for a maximum of three (3) days.

7.2.2 Customer initiated changes

The Customer authorised representative will notify JT's service desk at least ten (10) Business Days before the changes are required. Emergency Works will be agreed between JT and the Customer as required. Planned outages will not count towards availability calculations.

The procedures for Customer-generated Change Control will be as follows:

(a) All changes required by the Customer or a contracted agent will be notified to JT by means of the Change Request Form which will be provided by one of the Customer's authorised representatives. The form will contain detailed instructions for JT staff to follow and execute the change. Confirmation of the change request will be made by email or telephone from the Customer's authorised representative.

The following actions will be taken upon receipt of an executed Change Request Form:

(b) A member of the JT team will return contact via telephone or email to the Customer's authorised representative. A JT service desk change ticket reference number will be given to the Customer. This will be the reference for all subsequent communications.

(c) JT will review the Change Request Form from the Customer and advise the Customer if a quote will be provided for the requested change. This will depend on the type of change requested and may be dependent on third party costs and support services being determined.

(d) If the change is chargeable this will be quoted and contained on a Change Request and the details also then stored in the ticket. The Customer may need to provide a Purchase Order ("PO") reference for the change to proceed.

(e) A member of JT's team will confirm the scheduled time and maintenance window with the Customer's representative.

(f) Upon completion of the change as scheduled, a member of JT's operations team will confirm the changes have been made by email to the Customer's authorised representative, quoting the date of request and service desk change ticket reference number. JT will retain all documentation relating to all changes requested by the Customer for twelve (12) months.

(g) The Customer's authorised representative will test the changes for completeness and provide confirmation via email that the change has been completed satisfactorily or whether issues exist.

Any further corrective action(s) will be taken with the agreement of the Customer's authorised representative and a member of the JT operations team and recorded against the original change ticket reference by JT. This process will be repeated until the change(s) are completed. The ticket is closed only once confirmation is complete and no further action is required.

7.3 Release & Patch Management

The SMC manages the process of Release and Patch management of WAN Managed Service Customer infrastructure.

Whilst the SMC Change Management process is responsible for approving and supervising the process as a whole, the Release and Patch Management process deals specifically with the task of designing, testing and implementing pre-defined changes within the Customer's solution.

The SMC engineering teams work closely with vendors to review and agree update schedules based on the criticality of released updates and the associated risks.

Device IOS and firmware are chosen for feature set and version stability and unless stated in the Service Description section

at 3.3 Network Device Patching above, their upgrade is not included in the service unless required by the vendor as part of Problem Management. Updates and patches can be applied but are subject to additional charges and are agreed by the SDM. All releases and patches are tested within a controlled environment prior to being scheduled for implementation within the Change Request process.

7.4 Configuration Management

Details of all managed devices are maintained within the Configuration Management Database ("CMDB") that also includes the configuration of all managed devices. The SMC ensures that the CMDB is updated to reflect all releases and changes.

7.5 Service Delivery Management

The SMC is responsible for all aspects of service delivery. In addition, a dedicated SDMr may be assigned who is responsible for ensuring service availability, capacity management and continuous service improvement.

The SDM, supported by JT's technical teams, will ensure that the infrastructure under JT management continues to support the Customer's evolving business objectives.

7.5.1 SDM

The SDM's role is the Customer's primary contact within JT to manage all elements of the WAN Managed Service within the JT support organisation. As such, the SDM is tasked with providing the highest level of care and is responsible for the following activities:

Transition into support

The SDM is the single point of contact for service stabilisation issues and defines the service operations manual and any required run-books.

Management of Business as Usual Support

The SDM is responsible for issuing reports for high priority incidents including any service improvement recommendations. The SDM provides regular service reviews on service availability and utilization.

Escalation Management

The SDM is the single point of contact for hierarchical escalations and is responsible for ensuring that SMC technical escalations are managed effectively.

Service Availability Management

JT's service management function is responsible for overseeing and driving on-going availability management. This service includes regular reporting, delivered by the SDM, providing detailed information relating to the WAN Managed Service. Typically, JT's regular service review meetings will include the following reporting:

(a) SLA performance;

(b) Incident management review;

(c) problem management review;

(d) utilisation and availability reporting of links and CE devices; and

(e) reporting on optional services will be addressed by JT on case-by-case basis.

Continuous Service Improvement planning and progress reporting

Through these regular reviews, the SDM will identify and jointly agree with the Customer a process for continuous service improvement, where applicable.

Capacity & Trend Management

(a) JT will capture and analyse data from the SMC monitoring systems to determine the performance and capacity of infrastructure components subject to the WAN Managed Service.

(b) JT will analyse this data and align it with evolving business requirements as communicated by the Customer during the regular service reviews.

(c) The SDM provides on-going performance and capacity management information.

(d) The SDM is responsible for advising the Customer regarding upgrades and changes required to the infrastructure in order to maintain availability

(e) The Customer is responsible for notifying JT of upcoming business events or other technical events that may have an impact on the solution infrastructure.

8.0 SERVICE TRANSITION

8.1.1 Site Requirements for WAN Managed Service

Any site that houses managed devices must comply with certain environmental parameters such as power, cooling and security. All sites will be assessed during site surveys conducted by JT or its partners prior to any implementation activity.

The Customer is responsible for ensuring that appropriate power sources are provided and all managed equipment must be installed in a secure and environmentally controlled environment.

8.1.2 Service On boarding

The following tasks will be performed as part of service on boarding.

(a) management user creation;

(b) deployment of monitoring access;

(c) system audit including:

  a. users and groups;

  b. patch baseline; and

  c. network configuration,

(d) configuration of the security policy;

(e) documentation of the device and

(f) monitoring setup

To find out more contact us at:

T **Jersey:** +44 (0) 1534 882 345
Guernsey: +44 (0) 1481 882 345
E business.solutions@jtglobal.com
W www.jtglobal.com/managed-wan