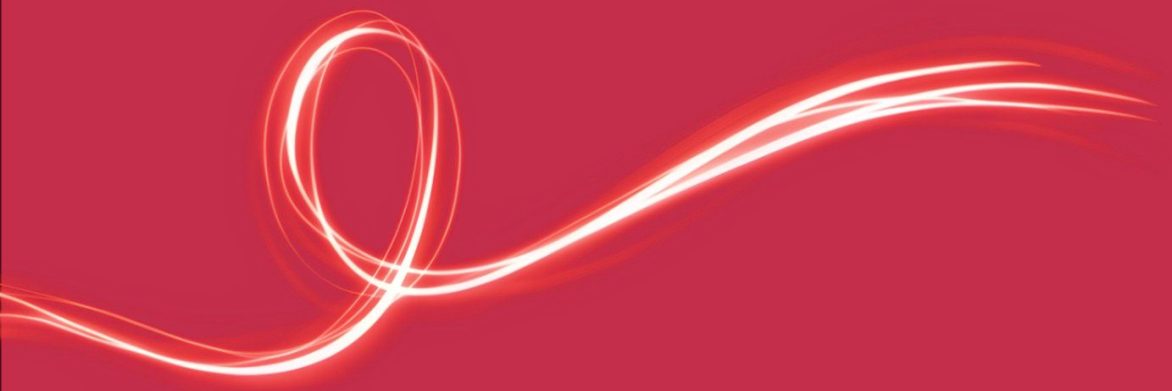
TalkTalk Business

TalkTalk Business Software Defined Networking (SDN)

Service Definition



Contents

1. Software Defined Networking (SDN)

TalkTalk Business' (TTB) Software Defined Networking (SDN) solution provides a modern, cloud-based approach to managing and optimising network efficiency. Public-sector customers gain greater control, visibility and performance across all sites, while reducing operational complexity and improving service resilience.

Our managed SDN solution uses centralised, software-driven control to intelligently route traffic, prioritise critical applications and optimise connectivity across multiple access types. It is designed to work seamlessly with TTB connectivity services, including Dedicated Internet Access (DIA), P2P circuits or Fibre Broadband.

This enables public-sector organisations to build a secure, high-performance network that supports cloud adoption, hybrid working, digital learning, telehealth, housing management platforms and emergency-service applications, and more.

Specialist consultancy ensures the solution is correctly designed, deployed and aligned to each organisation's operational needs. This includes:

- Network discovery and design
- Tailoring of SDN policies to support public-sector applications
- Installation, configuration and testing
- Seamless integration with existing networks and cloud environments

This scope is consistent whether customers choose reactive or proactive management.

We supply and configure all required customer-premises equipment, software licences and SDN devices. This ensures a complete, ready-to-use solution with consistent performance and security across every site.

<u>Ongoing Service Management</u>

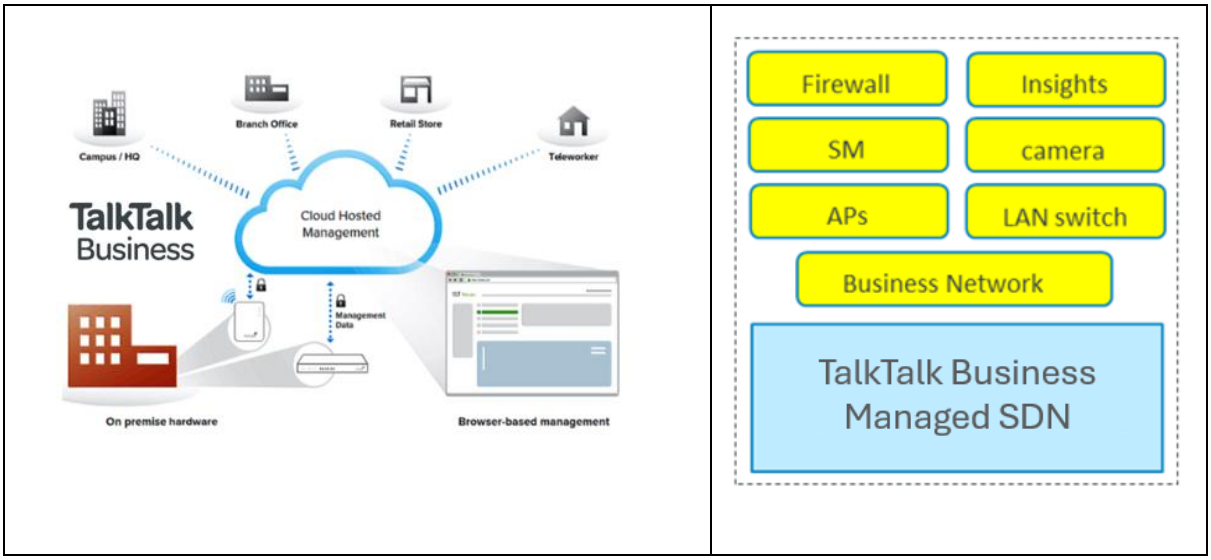
Customers can choose between reactive or proactive managed service options:

- Reactive Management:
  - 24/7 monitoring
  - Incident management and fault resolution
  - Hardware maintenance and replacement

- Proactive Management, including all reactive features, plus:
  - Daily health checks
  - Annual performance and policy reviews
  - Detailed service reporting
  - Change management support
  - Continuous optimisation of application and traffic policies

This ensures networks remain aligned to evolving public-sector needs such as new cloud services, increased bandwidth demand or changes in operational priorities.

SDN Overview



TTB Security & SDN Appliances:

- Simplest, cloud-managed, all-in-one UTM and SDN solutions including SDN , SD-LAN and SASE.
- Ideal for large, distributed organisations, datacentre VPN concentrator, and smaller office deployments.
- Robust feature set of security and VPN capabilities backed with centralised, cloud-managed dashboard.
- Allows customers to lower IT costs and reduce time spent deploying, monitoring, and troubleshooting gear.
- SDN appliances are self-provisioning.
- TTB has a 100% cloud-managed dashboard, saving time and money.

Removes the challenges of dealing with multiple solutions and reduces complexity.

Portfolio range

SDN portfolio includes multiple software-defined hardware and licenses across firewalls, security gateways, switches, access points, cameras and sensors.

Data backup and restore

The customer plan ensures the integrity and availability of SDN configurations and data by defining procedures for backup and restoration in case of system failure, disaster, or configuration errors.

Scope

Applies to:

- SDN Orchestrator/Controller
- Edge Devices (Branch Routers)
- Configuration Files, Policies, and Templates
- Certificates and Security Keys
- Monitoring and Log Data

Roles & Responsibilities:

- Network Administrator: Executes backup and restore procedures.
- IT Security Team: Ensures encryption and compliance.
- Disaster Recovery Team: Coordinates restoration during major outages.
- Vendor Support: Assists with troubleshooting and advanced recovery.

Backup Strategy

Frequency:

- Daily: Incremental configuration backups.
- Weekly: Full system backup.
- After Changes: Immediate backup after major configuration updates.

Backup Types:

- Full Backup: Entire SDN configuration and system state.
- Incremental Backup: Only changes since last backup.

Storage:

- Primary: Local secure storage.
- Secondary: Cloud-based encrypted storage.
- Tertiary: Offsite data centre for disaster recovery.

Security:

- Encrypt backups using AES-256.
- Use secure transfer protocols (SFTP, HTTPS).
- Implement role-based access control.

Restore Strategy

Trigger Events:

- Hardware failure
- Configuration corruption
- Cybersecurity incident
- Disaster recovery scenario

Procedure:

1. Identify affected component(s).
2. Retrieve latest verified backup.
3. Validate backup integrity.
4. Restore configuration to orchestrator and edge devices.
5. Test connectivity and policies.
6. Document restoration process.

Recovery Objectives:

- RTO (Recovery Time Objective): 1 hour for critical sites.
- RPO (Recovery Point Objective): Last 24 hours of data.

Testing & Validation:

- Perform quarterly restore drills.
- Validate backup integrity after each backup cycle.
- Document test results and improvements.

Monitoring & Alerts:

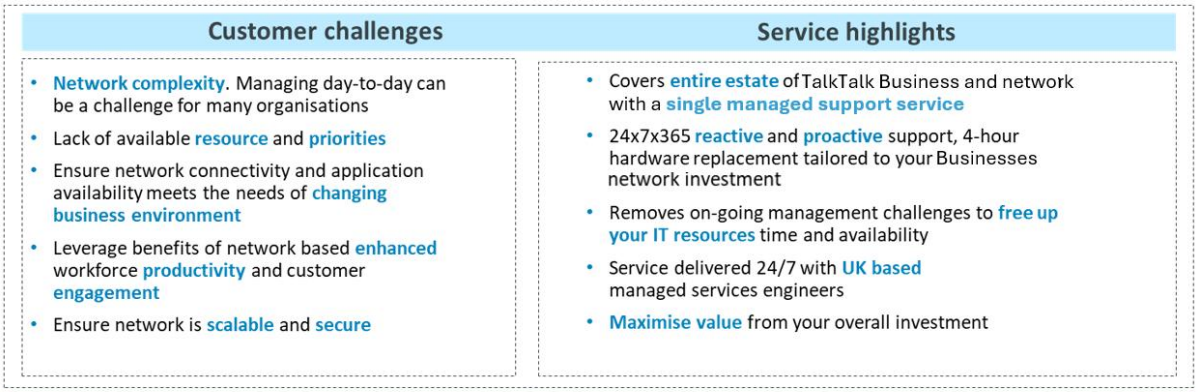
- Configure alerts for backup failures.
- Monitor storage capacity and encryption status

1.1 Managed Service Overview

This section provides an overview of the managed service and engagement offered to end-customers. It sets out all discrete ITIL based services that may be offered as part of the overall service.

The specific services that are to be provided to the company will be detailed in the associated Statement of Works.

Managed services



Business objectives	Service Benefits
Reduction in infrastructure operating day-to-day expenses	Our skilled operations team ensure we are consistently keeping pace with technology innovation and focused on high-quality service delivery
Reduction in infrastructure related capital expenditure	Integration of the Dashboard into our platform ensures service-affecting incidents are accurately and quickly detected and managed.
Enhanced end-user experience and productivity across the estate.	Our expert resources, tools, and processes are designed to ensure improved mean-time-to-restoration (MTTR) and consistent availability across your network.
Data-driven near real time management insight and graphical reporting available 24/7	We have a unified management view across LAN technologies and managed service.

The managed services scope will enable a customer to migrate their services to a TTB SDN solution. These services are offered flexibly, allowing the overall offer to be tailored to the customer's needs.

Managed Service Deliverables	**Level 1 - Reactive managed service**	**Level 2 - Proactive managed service**
Monitoring	√	√
Incident Management	√	√
Software Update and Validation	√	√
Hardware Maintenance	√	√
Proactive Technical Review		√
Daily Checks		√
Annual Dashboard Review and Familiarisation		√
Change Management		√
Flex Tokens		√
Service Reporting		

The managed service offers customers either a reactive or proactive managed service (shown above). Both services include the base service components below.

Base Service Components Optional	**Level 1 managed service elements**	**Level 2 managed service elements (in addition to Level 1)**
Service Transition	**Scope**	**Scope**
Service Transition – Planning and Support	Monitoring	Proactive Technical Review
Service Transition – Managed Component Activation	Incident Management	Daily Checks
Service Asset Inventory Management	Software Update & Validation	Annual Dashboard Review and Familiarisation
	Networking Update & Verification	Change Management
	Hardware Maintenance	Flex Tokens
		Service Reporting
		Problem Management

Service Transition

a) Planning and Support	
Summary: TTB and the customer will define a plan for establishing connectivity for the Managed Components.	
TTB Responsibilities • Single point of contact (SPOC) for the customer during the Service Transition • Compile and complete Transition Requirement Document necessary to transition the in-scope devices and assessing changes required to customer's platform, network, and processes to activate the Managed Components • Define the required inventory information and topology requirements necessary to activate the Managed Components • Creation of appropriate role-based access for the cloud login portal • Provide relevant fault reporting and escalation details	**Customer Responsibilities** • Identify a SPOC to engage throughout the Service Transition period • Provide the reasonably requested inventory and topology information by the dates agreed between TTB and customer • Provide all relevant address and contact details of all sites within the scope • Provide access levels for their internal IT team • Perform tasks specified as customer's responsibility by the date specified

Output:
- Transition Requirement Document
- Role-based access is created and assigned in the cloud-based portal for Managed Services and the customer

b) Managed Component Activation

Summary:
The Transition Manager will assist the customer's Transition Personnel to fulfil obligations by using information provided as part of the SoW.

The Transition period takes up to 30 days on receipt of the order; production of customer contract within the first 14 days of said period.

With customer assistance, TTB will connect the Managed Components, perform tests to confirm the Managed Components are ready for remote monitoring, management, and troubleshooting and activate the Managed Components onto the Managed Services Platform (MSP).

TTB Responsibilities	**Customer Responsibilities**
• Design, implement and test bidirectional management capabilities • Provide the customer with general guidance on stabilisation activities required to allow activation • Implement Monitoring Services • Activate Managed Components, per the applicable agreement • Implement MSP and conduct tests to confirm that the Managed Components are activated and ready for management • Provide notification to the customer that activation is complete • Create an Asset Inventory • Create Operational Service Manual	• Availability, access, agreement to plan **Transition is complete when:** • All processes and tools are in place for successful implementation • Documentation has been provided • Formal introduction and handover to Service Delivery Manager has occurred • Monitoring Service has been configured on all applicable devices

Output:
- Initial Managed Component Inventory
- Operational Service Manual

c) Service Asset Inventory Management

Summary: TTB will collect and maintain inventory information about the Managed Components and the associated environment.

Output: Managed Component List and Environment Details

1.2 Disaster Recovery

At TTB we undertake best ITIL practices throughout the business and technology teams. The Service Desk team has a problem management and change process to ensure that root cause and preventative actions are managed effectively, in line with service levels. In addition, root cause investigations are completed as part of our problem management process, where change and incident information is analysed and collected to suggest preventative actions. Reason for Outage (RFO) for network incidents are distributed to impacted customers within 10 working days from root cause following a Priority 1(P1) or Major Service Outage (MSO). Where the priority of a TTB Network Incident is MSO or P1, a Major Incident Manager is assigned to document and communicate the progress of an incident. A multi-disciplinary team will work collaboratively to resolve the incident as quickly as possible and with minimal impact on the business. The IT Service Management (ITSM) team record of the incident is updated throughout and resolved using defined metrics to drive post-incident analysis activities.

Major Incident notifications are distributed during the life of the incident via a dedicated Incidents Team. If the customer has any questions related to an RFO notification, or requires additional detail, these can be referred to the ITSM team via your Account Manager.

Business Continuity, Crisis Management and Disaster Recovery Plans are in place for all sites. Network resilience is assessed and monitored through testing on an annual basis. Continuous monitoring of network availability through the Technical Support Centre team will ensure any issues are identified in a timely manner.

Where an incident does occur, a robust incident response process is in place and is exercised to ensure an effective response, followed by a problem management review linked to service improvement. TTB recognises that network resilience is also reliant on Openreach for the last mile. If an outage was to occur on the Openreach infrastructure, we have agreed competitive SLAs with Openreach to mitigate risk. Other prioritised critical processes, systems and third parties are identified, and business owners are assigned accountability for assessing resilience and implementing business continuity plans to enable continuity of operations in the event of an incident.

TTB also continues to invest in supporting appropriate resilience of critical systems. Relationship owners are assigned accountability for requiring critical third parties to have adequate business continuity plans in place and obtaining third party assurance, where appropriate, that their plans have been reviewed and tested annually.

With usage consistently on the rise, we constantly monitor the network, forecasting and responding to the ongoing demand to maintain stability and minimise any congestion. Despite download usage increasing 40% year-on-year, our network has remained resilient. Additionally, due to Covid-19, further measures have been implemented to ensure the health and safety of our workforce and customers whilst

we successfully continue our provision of critical services, which involves enabling the remote working of both our workforce and third parties.

Service Components

The following service components are included:

1.2 Level 1 Managed Service

Monitoring
Summary: TTB Managed Services monitor a standard schedule of events and incidents.
TTB Responsibilities • Default alert types agreed with the customer • Alerts vetted and triaged In the event a Service Component is down the customer will be advised of the incident (email via ServiceNow) • The monitoring service will be configured according to the operational service manual • In the event of a discrepancy between the Supported Estate and the Statement of Work, the Supported Estate will take precedence. Both parties will meet as soon as reasonably possible to correct any potential differences in Supported Estate and Operational Service Manual.
Output: • Defined standard monitors (can be adjusted over time in dialogue with the customer)

1.3 Incident Management

Summary: TTB will help identify, troubleshoot, and restore standard operational functionality of the Managed Components if an incident is detected or reported by the customer.
When a Managed Service Incident occurs, the following takes place. On becoming aware of an incident, the End-Customer Service Desk will open a ticket. Each Managed Service Incident Request will include the following: • The End-Customer Service Schedule Number where applicable • The equipment details including serial number, hostname, IP address and description

- The priority of the incident;
- The relevant premises that the TTB Engineer may need to visit;
- Any special instructions to ensure remote connectivity;
- Details of the End-Customer contact; and
- Any other information End-Customer considers relevant

In the event that the Managed Service Incident request is opened upon receipt of an alert, elements of the information may be added to the Incident Request after the Managed Service Response has occurred.

TTB will use all reasonable endeavours to determine if the Managed Service Request is due to equipment failure or requires Vendor Support as soon as possible, but no later than 45 minutes after the Managed Service Request has been created in order to:

- Initiate the Support Services
- Request physical access to the End-Customer Premises.

The TTB Service Desk will acknowledge and accept each Managed Service Incident Request. The Service Desk will provide the unique company reference number applicable to that Managed Service Incident Request.

TTB will action all Managed Service Incident Requests for items identified on the Supported Estate.

For all Managed Service Incident Requests in relation to equipment not listed on the Supported Estate, the company shall use all reasonable endeavours to action such Incident Requests and the approach to payment in the Statement of Work shall apply in accordance with the Time and Material Charges.

If the Managed Service Incident Request is, in the sole opinion of the Company Engineer, not related to an equipment failure, the Service Level shall be measured as the Managed Service Response Time.

If the Company Engineer cannot ascertain with a degree of reasonable certainty if the incident is related the equipment failure, the parties shall discuss the appropriate way to progress the Managed Service Incident Request.

If no person can be contacted at End-Customer, TTB will place the Managed Service Incident Request on hold and pause the Service Level counters until contact has been established unless a specific process has been defined in the Operational Handbook.

The customer can cancel any Managed Service Incident Request at any time by giving notice to the Service Desk.

Where a TTB Engineer considers that the incident is fixed, they will:

- Contact the individual set out in the Managed Service Incident Request to confirm that the incident is fixed;
- The notice includes:

i. Date incident was fixed; ii. Time incident was fixed; iii. Confirmation that the equipment has returned to a normal state on the Monitoring Service; iv. Free text information if applicable; v. Details of the engineer who fixed the incident; and vi. Details of any follow up work that is required or charges which may apply.
Output: Incident Ticket, Change Request to resolve incident; Recommendation to resolve incident

SDN Software Update & Validation	
Summary: TTB oversees quarterly software updates, including the scheduling or postponement of updates based on impact. TTB will validate the success of the software updated.	
TTB responsibilities: Where the networking equipment has a native software update capability incorporated into a Cloud based dashboard – TTB will manage quarterly updates to the devices where they become available. For the service, which has a Cloud based Dashboard, we will construct device collections (target groups of devices to be patched together). Updates will be released in stages to the identified collection(s). After each staged release of the updates, we will validate the success of the release and verify that no related incidents have been caused before releasing patches to further collections. Where the release of patches have caused incidents, we will work to agree a rollback or work around.	Customer responsibilities: Assist in defining device collections Advise on success of patch rollout to collections
Output: Validation of successful software updates.	

1.4 Onboarding support

TTB has an onboarding model for all new customers, from SMEs through to major customers, undertaking the following process:

1. The customer order is received by the salesperson, along with a copy of the terms and conditions (signed using DocuSign)
2. All customer orders are verified, and credit checked and, once approved, put into the provisioning work in progress queue (WIP)
3. All orders are built within our Inventory Systems billing system by the Delivery team
4. All updates and communication on installation dates will be provided to the customer via email by the Delivery Team

5. Should a router be requested as part of the solution, TTB will provide engineering resource for onsite installation.

1.5 Offboarding support

If a customer chooses to cease their TTB service, clear timescales will be mutually agreed between TTB and the end customer. Any managed CPE provided as part of the managed service remains the property of TTB and must be returned to TTB unless otherwise agreed.

1.6 Service Constraints

For all planned notices and maintenance, the customer will be notified 10 business days in advance to allow them to make suitable arrangements. Emergency maintenance is rarely required and is typically not customer-affecting, as it is usually confined to one part of a resilient system. In the event emergency maintenance is required that is likely to be customer affecting, the planning and risk assessment we undertake will include making provision to minimise the impact in terms of scope and duration. Where it is possible, advanced notice will be given.

Service Levels

TTB's Managed SDN service is supported 24/7/365 with a target service availability of 99.9%.

NETWORKING PRODUCTS Software Update & Validation
Software Update & Validation
Summary: Field notices for core software applications and devices will be reviewed on a weekly basis. Where it is identified that an affected application version is in use on a customer's network, a deviation will be identified to the customer and recommendations provided to initiate the software update process. Application of software/ firmware updates is at the discretion of TTB and are related to individual technologies and devices. Software will be evaluated to minimise disruption to the stability of the current environment. Software updates will normally only be deployed as a resolution to an incident or as a result of a security notification and, as such, will be an inclusive service. TTB will attempt to apply the update remotely where possible. If the nature of the update requires on-site attendance, that will be scheduled with the customer as appropriate. Software updates that are customer-requested for the purpose of obtaining additional features or functions will be classed as COMPLEX and processed as COMPLEX changes. All software updates will be processed via the Change Management process. TalkTalk Business will validate the success of the software update.

Output: Notification to the customer on recommended software update actions Updated managed components to resolve incidents or security vulnerabilities Provide change documentation and updates to the customer Validation of successful software updates.

Managed Hardware Replacement	
Summary: Customer hardware must be maintained. Break-fix services will be carried out in accordance with priority level as per data product T&Cs	
TTB Responsibilities • To maintain CPE as per Data Product T&Cs	**Customer Responsibilities** • Customer will have hardware maintenance on their CPE via TTB.

1.7 Level 2 Managed Service

In addition to the reactive service elements, managed proactive services will provide the following:

8. Proactive Technical Review
9. Daily Checks
10. Annual Dashboard Review and Familiarisation
11. Change Management
12. Flex Tokens
13. Service Reporting

Proactive Technical Review
Summary: TTB will undertake a monthly proactive technical review of the customers' infrastructure, identifying issues before they become service affecting problems.
TTB Responsibilities • Review alert patterns and analyse trends • Check software and device versions for latest and/most stable release • Review capacity • Review availability • Make suggestions and recommendations to ensure optimal health and performance of the environment is maintained
Output: Proactive Technical Review Report

Daily Checks
Summary: Complement the monitoring and alerting service with additional checks, ensuring the environment is performing at optimum levels. Daily Checks are licence and feature dependant.

TTB Responsibilities

The service can include:

- Monitor Network – Make sure all devices are green and in an up state
- Monitor Events – look for critical errors in the last 24 hours to make sure nothing has been missed
- Main Dashboard – Check all controllers are up and healthy
- Main Dashboard – Check WAN Edge Health
- VPN Dashboard Check - Device Health
- Site Health and WAN Edge Health
- Dashboard Security – Check Firewall Enforcement, Signature Hits, URL Filtering and Advanced Malware
- Audit and ACL log check for suspicious activities
- Check health and availability

Annual Dashboard and Familiarisation	
Summary: An annual review, carried out once a year that can be requested any time during the 12 months.	
TTB Responsibilities • Conduct a demonstration with the customer at their request • Demonstrate current environment, including configuration set-up and business benefits	**Customer Responsibilities** • Customer to request dashboard and familiarisation when/ if necessary
Output: Dashboard and Familiarisation Session	

Change Management
Summary: Fulfilment of Change Management services as per a standard Managed Service, as covered in this document
Where the End-Customer requires a Managed Service Change, e.g. adding devices, changing firewall rules, policies, adding sites, web-site domain filters, actions to restore service. Categories are assigned to a Managed Service Change as a Standard Change, Complex Change or Emergency Change. • "Standard Change" - A standardised pre-approved Managed Service Change that is low risk and follows a pre-determined work instruction • Complex Change" - A Managed Service Change where no pre-determined work instruction exists which requires specific investigation and documentation to deduce the engineering required and mitigate risk to ensure seamless release. • "Emergency Change" - A Managed Service Change which needs to be implemented as soon as reasonably possibly to either restore End-Customer services or prevent significant risk to operation or security of the End-Customer Systems.

Authorised customer contact requests the Service Desk for the Request For Change (RFC).

The RFC will contain the following information:

- End-Customer unique RFC number;
- End-Customer Service Schedule Number where applicable
- Equipment details including serial number, hostname, IP Address and description
- Change Category of the RFC;
- The relevant premises that the Company Engineer may need to visit;
- Details of the Managed Service Change required;
- Details of End-Customer Contact;
- Details of required downtime or request date / time of implementation;
- Details of potentially impacted users;
- Any details of potential security risks; and
- Details of any known Back Out Plan.

A Change Manager will coordinate the Managed Service Change.

The Change Manager will contact the End-Customer to confirm the details of the RFC and to advise the unique Managed Service Change reference number.

If the Change Category has been confirmed as a Standard Change, no further approval will be required by the End-Customer.

If the Change Category has been confirmed as a Complex Change or Emergency Change, TTB will:

- Assign a Company Engineer to document the activity required for the Managed Service Change;
- Compile any scope documentation relating to design, work packages, process or procedures which may be required for the Managed Service Change; and
- Update the RFC with the expected Change Charge (flex point consumption).

The Change Manager will document Completed RFC which includes:

- Information captured within the RFC;
- Confirmed Change Category
- Scheduled Managed Service Change date;
- Scheduled Managed Service Change time;
- Company Engineer details who will implement the Managed Service Change; and
- The Change Charge.

Customer may request the RFC to be cancelled at any time. Change Charges may be applicable for any time already spent by the TTB Engineer.

In the event of an Emergency Change, the customer acknowledges in the interest to implement the Emergency Change as soon as practically possible, some

information and approvals may not occur, or a separate process may be defined within the RFC.

When the Completed RFC is approved, TTB will schedule the Managed Service Change as per the Completed RFC.

Upon implementation of a Managed Service Change, the TTB Engineer will advise the Change Manager of:

- The success or failure of the Managed Service Change;
- Any update to configurations, documentation or Asset Registers which may be required;
- How long the Managed Service Change took to implement; and
- Any further information which may be relevant.

Upon successful implementation of the Managed Service Change, the Change Manager will confirm closure of the Completed RFC, providing details of:

- The implementation activity which occurred;
- Any documentation or configuration changes which occurred;
- The impact of the Managed Service Change on other services;
- Any incidents which the Managed Service Changes was deemed the root cause of;
- Any follow up activity which will be required; and
- Where applicable (i.e. where the Work Order expressly notes the charges to be estimates or variable), Change Charges confirmation as per the Statement of Work.

Upon a failed implementation of the Managed Service Change, the Change Manager will provide details of:

- The success of the Back Out Plan;
- The current state of the End-Customer Equipment or systems; and
- Request information on proposed next steps.

Upon closure of the Completed RFC, TTB will advise all Change Charges (Flex tokens).

Product Field Notice Review

The managed service ensures that the overall solution is maintained within manufacturer's recommended support environment, including patch levels and configurations.

TTB reviews vendor notifications, which may the affect equipment, forming part of the Managed Service ("Field Notice Review").

Field Notices will be reviewed regularly.

Field Notices which would be categorised as a P1, result in a Managed Service Incident being created as soon as reasonable possible.

Only Field Notices on the equipment which forms part of the Managed Service shall be reviewed by TTB. In the event a Field Notice requires a change to be created, TTB will raise a RFC as part of the Managed Service Change process.	
TTB Responsibilities • All changes are scheduled events and are dependent on coordination with the customer's schedule	**Customer Responsibilities** • All changes are scheduled events and are dependent on coordination with customer's schedule • During any change, the customer must have an authorised representative available

Flex Tokens	
Summary: This service allows the tracking of resources required for changes. Upon initiation of a Managed Service contract, a finite number of Flex Tokens will be allocated on a per-device basis providing the customer with a 'Flex Token Fund'. Payment for requested changes utilises the 'Flex Token Fund'.	
TTB Responsibilities • Track and log Flex Token usage	**Customer Responsibilities** • None
Output: • Flex Token Fund Report	

Service Reporting

Summary: TTB Service Delivery Team will provide the customer with a standard monthly summary report, documenting the network's health, changes and availability.

Governance Reporting

This section of the Schedule identifies the regular reports and management meetings (This will be agreed for each customer with the TTB Account Manager

Report	Content	Period	Delivered by
Service Report	Performance review, details of previous month, reports on management of Specialist Third Party Suppliers and suggestions for continuous improvement.	Month	At least 5 Working Days before the Service Meeting
Quarterly Report	Performance review, End User satisfaction surveys and proposals for continuous improvement, Managed Service Specific Content	Quarter	At least 10 Working Days before the Quarterly Review Meeting
Annual Report	Performance review, End User satisfaction surveys, proposals for continuous improvement, strategy alignment, financial performance	Contract Year	At least 15 Working Days before the Annual Review Meeting

		and Managed Service Specific Content		

TTB Responsibilities	Customer Responsibilities
• Incident Review / Analysis • Service Level Performance • Problem Management Review / Analysis • Change Management Review / Analysis • Availability Review / Analysis • Flex Token/ Change Summary • Event Summary • Service Improvement Reporting	• None
Output: Standard Monthly Summary Report	

Problem Management	
Service Summary Problem Management is an ITIL process designed to help prevent incidents from happening, and to minimise the impact of incidents that cannot be prevented. Problem Management analyses Incident Records, and uses data collected by other IT Service Management processes to identify trends or significant problems. A 'problem' is caused by an unknown underlying cause of one or more incidents. Once the problem has been successfully diagnosed, it becomes a 'known error' for which either a work-around or a permanent resolution can then be identified. TTB will provide an impact analysis to the customer for consideration and authorisation, either to continue with the identified workaround, or to work on a permanent resolution	
The Service a) Analysing incident data to identify and record a problem. b) TTB will hold a database of all problems and 'known errors' once analysis has determined the cause. c) Managing the problem from acceptance to closure. d) Requesting support as necessary from Manufacturers/ the customer to investigate and resolve the Problem. e) Delivering effective and consistent communication between the company and the customer relating to Problem Management activities.	Customer Responsibilities j) Assisting TTB in the resolution of problems, where the problem is on technology/ platforms not in control of the company, e.g. 3rd parties/ suppliers. k) To ensure that TTB is made aware of any changes pertaining to the delivery of the Problem Management service. l) Participation in problem review at the service review meetings

f) Reviewing all active problem records during the service review meetings. g) Provide a full Root Cause Analysis report upon conclusion of each P1/ P2 incident record. h) Co-ordination, management and governance of problem activity spanning multiple manufacturers and resolving teams. i) Record the cause of all identified trends and corrective actions to prevent or reduce the impact of a repeat incident.	
Exclusions Problem Management of issues directly related to active projects or in early life support	

Escalations

Escalation Procedure
Summary: A Standard Escalation Procedure applies, which is detailed within the Customer Operational Service Manual (OSM) and described below
TTB Responsibilities • Escalations are 24/7 - Please note, if you do not receive an answer from one of the escalation level telephone numbers provided, call the telephone number in the next level of the escalation procedure • Escalation path can be altered depending on the customer's requirement Customer will be updated at each point of escalation in accordance with a provided escalation notification procedure from the customer

Complaints Procedure	
Summary: A Standard Complaints Procedure applies, which is detailed within the Customer Operational Service Manual. As a service provider, TTB needs to capture, review and act upon all customer complaints. TTB defines a Formal Complaint as something unsatisfactory or unacceptable, which would constitute a perceived or actual service failure impacting on an end-user.	
TTB Responsibilities • It is TTB' policy to acknowledge a customer complaint within 24 hours of its receipt during normal working business days (Monday – Friday excluding Bank and Public holidays) unless otherwise stated	**Customer Responsibilities** • Complaints can be raised via several channels; Service Delivery Meetings Escalations via relevant department Account Reviews

in the customer Service Level Agreement (SLA).	Written accounts to the business

Customers will be given an Operational Service Manual containing details of the service, and how to request a change in the service and for faults.

1.8 Service Levels

Incident prioritisation

Incidents are prioritised according to urgency and impact

	Impact				
Urgency		**Widespread** Entire Customer network is affected (more than 75% of individuals, sites or devices)	**Large** Multiple Sites are affected (between 50% and 75% of End Users, Sites or End User devices)	**Localised** Single Site, room or multiple End Users are affected (between 25% and 50% of End Users, Sites or devices)	**Individualised** A single user or group is affected (less than 25% of End Users, Sites or devices)
	High Primary business function of Customer is stopped with no redundancy or backup, immediate financial impact	Priority 1	Priority 1	Priority 2	Priority 2
	Medium Primary business function of Customer is severely degraded or supported by backup or redundant	Priority 1	Priority 2	Priority 2	Priority 3

	system, probably significant financial impact				
	Low Non-critical business function is stopped or severely degraded, possible financial impact.	Priority 2	Priority 3	Priority 3	Priority 3

1.9 Resolution Targets including Hardware

Where the Incident relates to an element listed in the Managed Data Service level (e.g. connectivity or hardware) then that Incident shall be covered by the applicable Service Level.

It should be noted that service levels and credits will apply to the network elements and equipment.

No Service Levels or service credits apply in relation to the Network Monitoring element of the managed SDN service.

Resolution targets

Priority level	**Updates (Business Hours)**	Target Fix (clock hours) SLO[2]	**Resolution Targets (Clock Hours) – Faulty Hardware**
1	1	4[2]	4.
2	2	8	By end of next Business Day.
3	24	24	As soon as reasonably possible.

1.10 Network Monitoring Service Availability

TTB uses its reasonable endeavours to achieve SDN Availability Target of 99.9%, measured monthly as calculated as the total minutes where the Network Monitoring Product is not available in a given calendar month divided by the total minutes of the calendar month, expressed as a percentage.

1.11 After Sales Support

Incident Reporting and Support Requests

Incident reporting and support requests should be raised by telephone on 0333 003 4333 or via email ttbenterpriseassurance@talktalk.business. Our team aims to diagnose faults within 30 minutes. Support requests which are less time sensitive should be raised by email.

1.12 Technical Requirements

Customer Responsibilities

- Identify a SPOC to engage throughout the Service Transition period
- Provide the reasonably requested inventory and topology information by the dates agreed between TTB and customer
- Provide all relevant address and contact details of all sites within the scope
- Provide access levels for their internal IT team
- Perform tasks specified as customer's responsibility by the date specified

1.3 Outage and Maintenance Management

For all planned notices and maintenance, the customer will be notified 10 business days in advance. Regarding all unplanned disruption or major failures, all TTB staff will receive email notification internally, informing them of the exact nature of the disruption and the details of the known failure. At this stage it will be the responsibility of the Assurance Desk to inform all affected customers via email and/or text message. Updates will be provided on a regular basis (every four hours) until fault restoration. For all Major Service Outages (MSOs) a full RFO report will be provided as part of the communication.

Reverting to a normal service in the event of a failure of MSO will follow a procedure whereby all necessary testing is completed within the Assurance and Technical Engineering teams. These teams will initially follow up through direct contact with named representatives within the customer's organisation. All relevant checks to ensure all connectivity and hardware is performing at full capacity in agreement and sign off from the customer.

1.13 Hosting Options

TTB currently has multiple Datacentre facilities, notably Corsham and Milton Keynes. We also have Data Centre space in 2 facilities - Virtus 2 in Hayes, and Virtus 5 in Stockley Park, both in west London.

Corsham

The functionality and operation of the TTB Corsham datacentre facility is designed to act as a single point of reference for customers to understand both the facilities provided and how to access/manage their services with TTB. The datacentre combines Tier 3 high-availability with very low additional energy used in the cooling and power system losses, resulting in an annualised power usage effectiveness (PUE) of less than 1.3 within an IL3 security environment. The systems employed ensure that Corsham is highly scalable, ensuring an unusually low PUE is achievable at low IT loads as well as when the facility is at its maximum capacity. This results in a carbon footprint that is nearly half the industry norm, providing customers with additional green credentials. Based in a multi-layered security complex with multiple levels of redundancy at both a power and network level, this facility ensures continuity of service delivery for customers hosting their equipment.

Milton Keynes

The Milton Keynes Data Centre consists of a purpose-built facility with N+1 redundancy throughout. Formerly the data centre for the Trustee Savings Bank (TSB), the Milton Keynes site has been built with attention focused on high availability. The Data Centre is secure and available 24x7x365. TTB provides a standard availability of 99.9% on all of the components of its co-location services: power, bandwidth, HVAC and fire suppression. Co-location services can be purchased as a standalone item, or as part of an IPVPN Service. These services may be used to extend service directly into a private MPLS cloud and/or to provide internet breakout.

Security

The facility provides a multi-layered physical security model to maximise security. The overall site is controlled and patrolled with no unauthorised access being permitted. The datacentre building has its own controlled security perimeter. Internally within the facility, all access is restricted and monitored using smartcard and pin, video surveillance and personal escorts.

The datacentre provides for a grading of security access. Personnel are only permitted to access the areas they require and only during the time periods agreed. In addition to standard physical access controls, photographic identification and biometric fingerprinting is required to access critical areas. The site has security and technical staff on-site 24/7, 365 days a year. Access to the building is controlled by an air lock which only allows one person through at a time. Access to all internal doors and

equipment aisles are controlled by card and pin code locks. The cards are configured to allow each individual access to only the areas they require and only for the length of time they require it. Access to the data room and build areas also have biometric scanners for additional security.

Access to the datacentre facility is covered by digital video surveillance both inside and out which records all movement and stores the data externally to the facility. This video data is stored offsite for three months. The physical building is covered by both passive and active sensors that are linked into local security response and emergency services. These sensors cover all areas with additional levels of coverage for critical zones. As additional security, all building alarm systems have built-in wireless notification systems as well as traditional telephone-based notifications to provide coverage in the event of physical links being tampered with.

The Data Centre is manned 24x7 and has 24-hour security at reception. The security desk is equipped with CCTV screens monitoring all access points, corridors and sensitive areas. All staff carry photo ID cards. Swipe cards are required to enter the Data Centre and to pass between rooms and enter hosting areas. Access to server rooms is only provided on a needs basis. All rooms, corridors and service areas are equipped with PIR detectors so that movement can be detected anywhere in the building. All external windows have “break glass” detectors, and all external doors including service areas trigger an alert when opened. The building is protected by an invisible fence which will detect motion around close proximity of the building. Client access to the Data Centre must be booked in advance and the booking confirmed by TTB . Any person arriving at the Data Centre without prior confirmation will be refused access. Anyone attending the Data Centre must show a valid legal form of photo ID. Using the “Authorised Contact Form” it is possible for customers to restrict access to a pre-determined group of personnel. Please note that it is the customer’s responsibility to ensure this form is kept up to data.

1.14 Access to Data (upon exit)

Data is stored in a secure and resilient N+1 environment and, where applicable, is subject to near real time replication/mirroring across diverse geographic locations. In the event of an incident, including loss or degradation of resilience, the incident will be managed in line with an established procedure to ensure customer SLAs can continue to be supported. Should the customer require access to data upon exit, a plan will be put into place for requesting the data via the customer’s Account Manager. The plan will contain a full inventory along with any contractual terms, expiry dates and any term fees. The Inventory list will be provided in CSV or Excel and will be sent directly to the main contact on the customer’s account.

At the end of a customer’s contract, TTB has a cease process in place. After the minimum term, the customer can end the contract or any connection forming part of a contract by giving 40 days’ notice. All cease requests must be received by email from the customer with a completed Cease Request Form, this will then create a case within Salesforce.

The Customer Service Team will query the address on the Cease Form to confirm that it matches the address held on our records. Once confirmed the cease process will begin.

The exit plan will be developed by the Account Manager with the customer 6 months prior to contract expiry to ensure a smooth handover. It will be provided by email and followed up with a phone call to answer any queries or highlight any missing information. The plan will cover:

- Options for asset acquisition by the customer
- Transfer of service/supply contracts
- Licence terms for IPR
- Data transfer
- TUPE
- Transition and handover planning
- Exit plan review and update

Provided the minimum contract term has expired and payment is up to date, no further charges or additional costs will be payable by the customer.

1.15 Security

Should intelligence or alerting indicate any potentially malicious activity, TTB operates a robust security incident management programme, and has deployed industry-leading endpoint protection technology through security solutions designed to protect endpoints—devices like laptops, desktops, servers, and mobile devices, defending against advanced threats as part of our incident response program.

TTB has implemented an Information Security Management System based on industry good practice (NIST CSF, PCI DSS) and is externally certified to ISO 27001. This covers a range of policies and procedures (e.g., IP/TLS) to ensure the confidentiality, integrity and availability of information. Standard security protocols, e.g., Transport Layer Security (TLS) and Internet Protocol Security (IPsec), are followed for private network connectivity. The DDOS service has no additional security requirements as the security elements lie within the private network. The TTB Security Operations Centre (SOC) facilities are manned 24x7x365, providing a near real-time response to security events with an escalation process to senior management as required. Our 24/7 SOC performs extensive monitoring, e.g., through centralised log collection and real-time threat detection endpoint monitoring, and of internal and external security controls, coupled with curated threat intelligence feeds, and real-time alerts are activated if suspicious activity is detected. Incidents are triaged based on risk and impact and playbooks have been developed to focus on containment, eradication and recovery activities in-line with NIST best practices. TTB conducts security scanning of all its infrastructure on a bi-weekly basis. We also conduct weekly threat and vulnerability scanning of all our network assets via InsightVM. Critical/high risk vulnerabilities patches are applied within 14 days. All other updates are applied as soon as possible using a monthly patching cycle. Security updates are assessed and prioritised based on threat level, likelihood of compromise, consequences of

compromise, environmental characteristics and regulatory or accreditation-based requirements. TTB gets its information about potential threats from InsightVM for scanning, Altiris Patch Management.

Version Control

Document Amendment History Log						
Document Owner	Warren Potts					
Created Date	20-01-26					
Author	Paul Ducklin					
Next Review Date	20-01-26					
Version Number	**Modified date**	**Amendment history**	**Reviewed by**	**Approved by**	**Approval date**	**Approval evidence**