

TalkTalk Business
Pangea Mobile Data back up
Service Definition



Contents

1.	Introduction	3
1.1	Service level constraints	6
1.2	Data backup and restore	6
1.3	Onboarding support.....	6
1.4	Offboarding support.....	7
1.5	After sales support.....	8
1.6	Technical Requirements	8
1.7	Outage and Maintenance Management.....	8
1.8	Hosting options.....	9
1.9	Access to data (upon exit)	9
1.10	Security	10
	Version Control	12

1. Introduction

TalkTalk Business (TTB) offers high speed mobile data connectivity to provide highly effective solutions to address customers' overall networking requirements of being always online, highly available and secure.

TTB can provide data connectivity services utilising 4G/5G mobile data networks delivering robust, resilient backup data service if the primary WAN circuit(s) and/or primary hardware device fails.

Low Power WAN (NB-IoT, and LTE-M) Mobile Data Connectivity addresses low power and continuous application environments such as for delivering Internet of Things (IoT).

The service can also be used to meet use cases where customers want a fast immediately available connection whilst waiting for lead times for fixed service installation

The service has been designed to provide primary or resilient connectivity for Standalone Internet, Private MPLS Network and SD-WAN services that a customer may wish to deploy.

The services are available to customers on an Opex basis or combined Capex/Opex.

Service Highlights

- Can be used as back-up or as main connection
- Unsteered multi-network SIMs choosing the best network coverage in areas where individual service provider coverage is poor
- Single network SIMs for cost effective coverage in areas of known coverage
- Choice of 4G or 5G speeds
- Hardware to accommodate wired or wireless premises connections
- Choice of IP addresses if offered: Public or Private Static, or Dynamic
- Secure connectivity

Main Service components

A choice of router hardware is offered to address LAN or WAN use

- Ultra-high **5G** speeds with **ultra-low latency**, to meet mission-critical infrastructure with high data throughput.
- 5G and **backward compatible with 4G** (LTE CAT 20) and 3G network technologies
- Delivers **up to 3.3 Gbps** speeds (4x4 MIMO)
- **Advanced security** features such as bespoke APNs, private Static IPs, VPNs

Pooled or single data usage

We provide a choice of shared, pooled or unlimited data across several devices to give the most optimal solution for performance, cost control, site coverage, business continuity and throughput.

Data Packages and speeds

A choice of 4G or 5G data packages are available, dependent on customer requirements, coverage and availability. Tariffs are flexible and designed to align with each customer's deployment needs, usage patterns, and device count. This means data packages are custom-built rather than pre-set. Included within the packages are:

- Small-usage IoT plans (e.g. sensors, telemetry)
- Medium-usage plans (e.g. retail, CCTV alerts)
- High-usage plans (e.g. streaming CCTV, AI cameras, vehicle tracking)
- Unlimited or high-cap plans for 4G/5G routers

Single network coverage

A choice from EE, VMO2, Vodafone and Three are available.

When: typically, where there is known, reliable and strong coverage in a location.

- Advantage: This can typically provide the most cost-effective solution
- Disadvantage: It can leave the service dependent on the provider and a higher likelihood of failure compared to unsteered multi-network

Unsteered multi-network

SIM allows the device access to all UK MNOs in an unsteered fashion. Unsteered means that there is no preference to any specific network.

When: Typically for use as a back-up or replacement to the primary that would use DSL or FTTC. The device can be configured to search for the strongest available network when called on for use

- Advantage: overcomes reliance on a single MNO
- Advantage: is typically better for vital back-up solutions as it gives the ability to utilise any available network.
- Disadvantage: can be more costly

Additional Value-adds

- IP Addresses (supports more secure corporate networking)
- Public Static IP Address

- Private Static IP Address
- Dynamic IP Address
- Pooled Data:
- The Unsteered network SIM data allowance is pooled across all users, providing additional peace of mind in cases where individual sites across estates require back-up and the others do not.

Provision

TalkTalk Business will set-up each customer in the in the portal for nominated users to oversee their use of the service

TalkTalk business proposition includes:

- + Supply of the SIM(s)
- + Supply, Installation and configuration of the 4G/ 5G router
- + Supply and installation of additional accessories such as external antennas
- + SIM Management for controlling/ limiting data costs for SIM estate
- + Project management or co-ordination

Customer service management

White label IOT management portal is available. Customers can use to view usage, set thresholds, see session details understand usage across an entire estate and receive alerts.

The portal can be set to send alerts when data usage thresholds are reached and when breached, together with recommended actions to be taken.

The portal can:

- show usage per SIM
- add multiple unique searchable descriptions for every connection
- monitor usage against customer set thresholds
- check that SIM is visible on the mobile network. This check confirms the customers mobile device is live and available should it be required
- Diagnostic tools to understand SIM session and configuration
- Report against above which can be downloaded

All the devices can be managed and maintained by TalkTalk Business.

1.1 Service level constraints

Services may be affected by local terrain (e.g. trees, hills and buildings), weather, electromagnetic interference, arrangement of and number of users accessing a base station, and compatibility and availability of any equipment, systems and third-party services used by Customer.

For this reason, in common with all providers of mobile based solutions, TalkTalk Business strives to provide uninterrupted services through the unsteered mobile service which access all the main mobile service, but we cannot guarantee 100% uptime. We provide uptime availability of around 99.9%.

1.2 Data backup and restore

The IoT architecture includes a Data & Cloud middleware layer, responsible for processing, managing, and securely storing the data flowing from connected devices.

The Mobile solution provides a single-pane-of-glass IoT management portal that stores and manages information related to:

- SIM lifecycle (active, suspended, terminated)
- Usage statistics
- Alerts and diagnostic information
- Network behaviour
- [pangea-group.net]

This portal effectively maintains the state and configuration of IoT deployments and means configuration data is stored reliably.

This is a connectivity solution that helps customers deliver improved back-up and restore to their IT environment.

WRT to Customer data held on the management portal. This is backed up in multiple instances so can be restored by TTB and used if needed.

1.3 Onboarding support

TalkTalk Business will provide the following support during onboarding:

- Agree sites that need connectivity and mobile coverage availability at a site level.
- Confirming Mobile at location
- Coverage checks at the point of sale and order is performed to ensure appropriate coverage is available at the required site(s). This coverage

checker is an industry-wide used, government managed checker and assesses coverage across all major UK networks.

- Where a known strong coverage location exists, the solution has options to choose from, with a single network solution possibly providing the most cost-effective option.
- Additional antennas if required can ensure more robust signal strength.

1.4 Offboarding support

Upon Notice to cease TalkTalk Business will remove Customer access to the management portal.

Service levels

Fault services operate 24 hours a day.

Care Levels impact the target fix SLA when a fault is raised. At the point of order, customer must elect the level of care they wish to subscribe to

Target Service Levels will depend upon the Care Levels chosen by the Customer at point of order as shown below

Fault Priority Level	Care Level 2 (Standard)	Care Level 3 (Enhanced)
P1 Target Fix	48 Hours	24 Hours
P2 Target Fix	48 Hours	24 Hours
P3 Target Fix	72 Hours	48 Hours

All Target Fix times exclude Parked Time. Parked Time occurs whenever we ask you for information and/or site access and await such information and/or until our engineer arrives at your site.

Where Priority is defined as follows:

Priority	Description	Definition
P1	Total Loss of Service	Total loss of service existing for five minutes or more before logging.
P2	Severe Intermittence	Significant degradation or materially intermittent connectivity that has high degree of service impact and where the intermittence can be demonstrated repeatedly within an hour interval.
P3	Degradation	Incident has low service impact.

1.5 After sales support

Helpdesk function allows customers to raise queries or faults with a specific site's service. If the issue is confirmed, TalkTalk Business will work to resolve the issue. Queries and faults may include:

- Reporting services that are not working
- Reporting services that are degraded
- Seeking advice how to utilise a service

Allocated Service and Account Managers can assist with overall service change or service queries, such as billing queries, service upgrades or service performance.

1.6 Technical Requirements

Mobile data services can either be delivered as SIM only, or inclusive of 4G/ 5G routers. Technical design will determine agreed interworking with customers fixed line connectivity, and with selected CPE.

Design considerations and options

Firewalls can be used to terminate the VPN connections made by the mobile routers and to privately connect to the customers MPLS. Dedicated firewalls allow segregation of traffic for a security.

At each customer's premises, a 4G/ 5G Router can connect to the network.

When deployed, both the fixed and 4G/5G back-up Routers can work either in a main/standby mode to provide an automated solution, or under firewall control.

Upon failure of the primary router, standby protocols (e.g. VRRP) can automatically failover, and the Mobile router will advertise itself as the default gateway for the network. All traffic will route via a virtual IP address which is owned by the active router. This solution can be used regardless of LAN architecture as long as the existing devices support the standby protocol.

1.7 Outage and Maintenance Management

From time-to-time TTB or its underlying providers may require to work on any part of the network or its IT infrastructure to support growth and maintenance. For any network change TTB will give 8 business days' notice of the planned work and also provide a start and target finish time. TTB will keep the customer updated of all progress and when the maintenance window is closed.

Emergency Maintenance may take place outside of this window but is only used where there is an immediate threat to the availability of the service.

For Core Functions – impacting multiple users

Where there is a network outage that impacts multiple users, TalkTalk Business will seek to inform the customer (where practicable) in advance as soon as possible if after the event. Multiple user issues include:

- Core network or routing issues
- Regional infrastructure issues with TalkTalk Business Supplier
- Planned or Emergency Works

On site Engineering Access – Single User issue

Where an engineer has to visit site, the customer may elect the day of week and time period for the visit. Note the SLA clock will stop for any visit selected that is outside of the SLA window below.

The response time for an on-site visit is related to the care level selected at point of order.

1.8 Hosting options

As a SIM delivered service, mobile data can be provisioned at premises or at data centres, always subject to the mobile signal strength.

1.9 Access to data (upon exit)

Upon termination the customer will receive a final invoice containing any unbilled rentals, any outstanding call charges (and any early termination fees if notice served whilst in contract).

Customer can extract their data usage information from the mobile management portal before exit. The portal will be cleared of customer data at exit.

1.10 Security

Secure Connectivity can be provisioned as an overlay based on customers' own secure architectural related preferences.

The mobile data **advanced security** features, such as bespoke APNs, private Static Ips and VPNs support highly secure connectivity environments.

Secure Connectivity is provided through a **comprehensive API-based security platform** designed for developers building cloud, mobile, and AI-driven applications. Its security model focuses on embedding protection directly into the app stack rather than relying on external tools.

Below is a breakdown of the major security components:

Core Security APIs for Mobile/App Developers

Pangea offers modular APIs that allow mobile and web applications to integrate critical protections such as:

Authentication & Authorisation

- Secure user login, session handling, and access control to protect mobile app user accounts.
- Secure Audit Logging

Tamper-proof, compliance-friendly audit logs help monitor user and system actions—critical for regulated mobile environments:

- Vault & Secrets Management
- Secure storage for API keys, tokens, and other sensitive secrets needed by mobile or backend systems

Threat Intelligence & Protection:

- Mobile apps often interact with external networks; Pangea's security platform includes:
- Detection of malicious files, IPs, domains, and URLs

Useful for mobile apps that upload files, pull external content, or handle user-generated data:

- Malware Scanning & Content Sanitisation

- This ensures uploaded files/images from mobile devices do not introduce malware.

AI-Focused Security (If the Mobile App Uses AI/LLMs):

Provides industry-leading guardrails for AI features embedded in mobile apps:

- AI Guard – Sensitive Data & Content Filtering
- Blocks PII leaks, profanity, malicious content, harmful URLs, and malicious input/output in AI workflows.
- Prompt Guard – Prompt Injection / Jailbreak Defense

Prevents direct and indirect prompt-injection attacks with 99% detection efficacy:

- Ideal for mobile apps using on-device or cloud AI assistants.
- AI Visibility & Governance (Enterprise Mobile Deployments)

For companies distributing mobile apps with AI features:

- Unified AI visibility across browsers, apps, cloud, and gateways
- Consistent data and access policies across AI systems
- Detection of shadow AI usage and risky behavior

End-to-End AI Detection & Response (AIDR)

Pangea's AIDR provides:

- Real-time monitoring of AI usage and behavior in apps
- Threat detection for jailbreak attempts, data leakage, and indirect attacks
- Automated response actions

Version Control

Document Amendment History Log						
Document Owner	Jay Bhickhabai					
Created Date	26-01-26					
Author	Jay Bhickhabai					
Next Review Date	26-01-27					
Version Number	Modified date	Amendment history	Reviewed by	Approved by	Approval date	Approval evidence