Service Terms

IoT Connectivity

1 About this document

1.1 Where this document fits into our agreement with you?

(a) Thank you for choosing Telstra. Our Digital Services Agreement (**Agreement**) with you is made up of the following parts:

ⓘ If different parts of this Agreement conflict, the part listed earlier in the table applies to the extent of the inconsistency.

About the parts of this Agreement	
Overview	You sign this when you first agree to buy products and/or services from us. It includes your key Agreement details.
Price Schedule	Outlines the prices and pricing conditions of the products and Services you buy from us.
Service Order	A record of the orders you've submitted to us, including changes you've requested to your products and Services that have incurred a charge.
The following parts make up our standard form of agreement terms with our customers for the purposes of Part 23 of the Telco Act. We update these terms from time to time in line with our agreement with you.	
Service Terms	The specific conditions for each product and service you buy.
General Terms	The conditions that apply to all our products and services, available at telstra.com/digitalterms.

(b) This document, the Service Terms for Adaptive Mobility, has **6 sections.** At the top of each page, you can see which section you are in:

1. About this document | 2. Service summary | 3. IoT Data Plan | 4. Additional details | 5. Charges | 6. Support

2 SERVICE SUMMARY

2.1 What is IoT Connectivity?

(a) The IoT Connectivity Service allows you to establish machine-to-machine IP connectivity with a device over compatible Telstra mobile networks, as further described below (**IoT Connectivity Service**).

(b) Each IoT Connectivity Service comprises the following:

(i) connectivity to our network;

(ii) one SIM cards or SIM chips;

(iii) one IoT Data Plan (see 2.1(c) below); and

(iv) access to the IoT Connection Manager (or "**ICM**").

(c) When you order an IoT Connectivity Service, you must choose one of the IoT Data Plan available for that IoT Connectivity Service. The IoT Data Plans that are available with your IoT Connectivity Service are the data plans set out in section 3 below (**IoT Data Plan**).

2.2 Eligibility

To be eligible to acquire the IoT Connectivity Service, you must have a valid ABN, ACN or ARBN.

3 IOT DATA PLANS

3.1 Available IoT Data Plans

IoT Utilities Data Plan	
Mobile Network	CAT M1 and NB IoT (Narrowband IoT)
Monthly Data Allowance For use in Australia only **Error! Reference source not found.**	170 KB
Calls, SMS and MMS	Not available
Shared Data	Yes, your data is shared across all your IoT Connectivity Services. If you exceed your total Monthly Data Allowance, additional charges for excess data usage will apply.
International roaming	Not available. IoT Connectivity Services may only be used in Australia.

3.1 Specific exclusions

(a) The data plan included in your IoT Connectivity Service cannot be used for other calls or services including SMS (including Premium SMS), MMS, content subscription services, circuit switched data services, voice calls, video calls, voicemail or international roaming.

(b) The services, features and numbers mentioned in (a) above are not available with your IoT Connectivity Service.

3.2 Data volumes

In these Service Terms:

(a) 1000 bytes = 1 kilobyte (kB);

(b) 1000 kilobytes = 1 megabyte (MB); and

(c) 1000 megabyte = 1 gigabyte (GB).

4 ADDITIONAL DETAILS

4.1 Term

Each IoT Connectivity Service is a month-to-month service, which means you can terminate your IoT Connectivity Service at any time provided you let us know in advance.

4.2 Additional IoT Connectivity Services

You may order additional IoT Connectivity Services by completing a Service Order. If we agree to supply those IoT Connectivity Services to you, the terms of this Agreement (including these Service Terms) will apply in relation to those IoT Connectivity Services.

4.3 What connections and service types does your IoT Connectivity Service support?

(a) The IoT Connectivity Service supports the establishment of outbound connections from the relevant device to a server IP address reachable by the internet or via a Virtual Private Network ("**VPN**") (i.e. mobile-to-server connection establishment).

(b) Inbound connections from IP addresses reachable by the internet or via a VPN to a modem that forms part of your IoT Connectivity Service (i.e. server-to-mobile connection establishment) are not supported. However, server-to-mobile data connectivity is supported if a valid TCP session is first established.

(c) Direct data connections between two devices which are both linked to your IoT Connectivity Service (i.e. mobile-to-mobile data connection establishment) are not supported. However, mobile-to-mobile data connectivity via an external server is supported if a valid TCP session is first established.

4.4 General restrictions

(a) You must not use your IoT Connectivity Service to connect to the internet via another internet service provider in Australia. Global roaming services provided by us (if any) are permitted.

(b) If your IoT Connectivity Services use more than one modem device in a single location, you must ensure that data transmission from the modem devices is not synchronised, and that there is a minimum data transmission interval of 15 seconds between modem devices. If your IoT Connectivity Services uses more than 50,000 modem devices, you must provide a facility to control data transmission intervals in real time. We may require you to increase data transmission intervals during periods of network congestion.

(c) You acknowledge and agree that:

(i) while we will provide the IoT Connectivity Service in a manner that is consistent with prevailing industry standards and that endeavours to minimise errors and interruptions in the service, it may be temporarily unavailable for scheduled maintenance or for unscheduled emergency maintenance, either by us or by our suppliers, or because of other causes beyond our reasonable control; and

(ii) subject to non-excludable statutory guarantees, we do not promise that use of the IoT Connectivity Service will be uninterrupted or error free,

and as such, for any application that requires fail-safe or uninterrupted connectivity, you need to both implement a business continuity plan to address interruptions and to put in place separate backup services or arrangements to provide alternative coverage during any interruption.

4.5 FairPlay policy

(a) Our FairPlay policy is intended to ensure that our customers do not use our mobile network in an excessive, unreasonable or fraudulent manner, or in connection with equipment that has not been approved by us. Such usage may impact the reliable operation of our network and/or the quality or reliability of our services.

(b) You must not resell or commercially exploit the IoT Connectivity Service (or any part of it) or any of our mobile services or SIM cards. You must not re-route call traffic in order to disguise the originating party or for the purposes of resale.

(c) You may not use our mobile services in your capacity as a carrier or carriage service provider or as a party supplying services to a carrier or carriage service provider.

(d) You can only use a SIM card that we provide you with handsets or other devices that have been approved by us for use on our networks.

(e) You must not use, or allow others to use any part of your IoT Connectivity Service:

(i) as a point of interconnect for calls from overseas into Australia;

(ii) in connection with any machine-to-machine or internet-of-things applications (i.e. any automated telemetry, telematics or telemetrics application which links two or more systems or devices with a mobile data connection);

(iii) to establish any point-to-point connections with another modem; or

(iv) to send messages to any numbers that we reasonably believe have been set up to enable you or another person to commercially exploit our services.

(f) You must ensure that your end users comply with this FairPlay policy.

(g) If we reasonably believe you are in breach of our FairPlay policy, we may suspend or cancel the relevant IoT Connectivity Service (or any part of it) immediately.

4.6 Additional termination rights

In addition to any other termination or suspension rights we may have under the General Terms of this Agreement, we may terminate or suspend your access to our networks if:

(a) you use your IoT Connectivity Service to adversely impact the operation and/or other customers' enjoyment of our networks or if you commit a material breach. We will tell you before this happens.

(b) your use of the IoT Connectivity Service is polling the network more frequently than once every 60 seconds or maintains a continuous active radio connection to the network (other than for a voice connection). Continuous idle data connectivity to the network, in the form of PDP context establishment, is permitted.

4.7 Coverage

(a) The devices you use in connection with your IoT Connectivity Service can only access the Telstra Mobile Network where there is coverage within the relevant network.

(b) Although we will use reasonable care and skill in providing the IoT Connectivity Service, due to the nature of mobile network technologies, the network and devices may experience drop-outs from time to time.

(c) Some devices are also able to hand-over across different compatible Telstra Mobile Networks and maintain your connection during data transfers. Depending on the compatible Telstra Mobile Network, after handing over, the corresponding data rate may be altered.

4.8 Devices

(a) The devices you use in connection with your IoT Connectivity Service must have been certified with the RCM compliance mark administered by the Australian Communications and Media Authority.

(b) For optimum performance, we recommend you:

(i) comply with any user guides issued by the manufacturer or supplier of that device; and

(ii) comply with our guidelines for the devices, published by us from time to time, including the Wireless Application Development Guidelines (as amended by us from time to time and as currently available at https://insight.telstra.com.au/t5/Downloads/Download-Telstra-Wireless-Application-Development-Guidelines/ta-p/1209 (or at any other website advised by us from time to time)).

To the extent that our guidelines are inconsistent with the user guides, our guidelines should take precedence.

(c) We will only provide network support for devices that comply with clauses (a) and (b) above. If you connect a device that does not comply with those clauses, we provide no guarantee that that device will be compatible with our networks.

4.9 SIM Cards and SIM Chips

(a) For the purposes of this clause 4.9:

(i) a "**SIM Card**" means a subscriber identity module card that may be fitted to or removed from a device by hand via a slot or tray; and

(ii) a "**SIM Chip**" means a subscriber identity module chip that is soldered to a printed circuit board and then attached to a device.

(b) Any SIM Card or SIM Chip we provide you as part of the IoT Connectivity Service is unlocked. You must ensure that the SIM Card or SIM Chip is properly secured in your device in order to prevent any unauthorised use. You will be responsible for charges incurred as a result of any unauthorised usage of the IoT Connectivity Service (including as a result of fraud or theft of the SIM Card or SIM Chip).

(c) You must use the SIM Chips in accordance with the manufacturer's specifications, including that they must be stored in conditions up to a maximum of 40°C/90%RH, that they can only be used within 12 months of being packaged and within 168 hours after the package is opened.

(d) You must not:

(i) resell the SIM Cards or SIM Chips that we supply to you, unless expressly agreed otherwise by us in writing; or

(ii) use the SIM Cards or SIM Chips that we supply to you for any purpose other than for the purpose of using the IoT Connectivity Services.

(e) Subject to your compliance with this Agreement, if there is a manufacturing defect with a SIM Card or SIM Chip that we have supplied to you, we will refund to you the cost of that SIM Card or SIM Chip. Notwithstanding any other provision to the contrary, and to the extent permitted by law and subject to the Australian Consumer Law provisions in the General Terms of this Agreement, in respect of the supply of

SIM Cards or SIM Chips we limit our liability (including in relation to contract, tort (including negligence) or breach of any other law) to paying you the cost of the SIM Card or SIM Chip.

4.10 IoT Connection Manager

What is Telstra IoT Connection Manager?

(a) The Telstra IoT Connection Manager platform is a hosted SIM management service ("**ICM**") which allows you to view and manage your active Eligible Services on Telstra's mobile network via a portal ("**Portal**").

Licence

(b) We or our licensors (as applicable) retain all right, title and interest, including all intellectual property rights, in and to the ICM and Telstra Material. Other than as provided in clause 4.10(c), you do not receive any right, title or other interest in the ICM or Telstra Materials.

(c) We grant you for the term of your agreement with us for the ICM, a non-exclusive, non-transferable, revocable right to access and use, and allow your Authorised Users to access and use, the ICM and the intellectual property rights in the Telstra Material, in accordance with this Agreement and for your internal business purposes ("**Licence**"). You must not sub-licence or authorise any other person or party to use the Licence or the ICM except as expressly permitted in this Agreement.

(d) You own any rights (including intellectual property rights) in data or information you provide or make available to us in connection with the ICM ("**Your Data**") and grant us a perpetual, irrevocable, worldwide licence to use, reproduce, modify, sublicense, and communicate Your Data for the purposes of providing the ICM to you and for our internal business purposes.

Restrictions

(e) You may authorise individuals within your organisation to access and use the Portal ("**Authorised Users**"). However, you must not authorise a third party service provider to access and use the Portal on your behalf or otherwise.

(f) You must, and must ensure that your Authorised Users, comply with:

(i) all applicable laws and regulations in your use of the ICM; and

(ii) Telstra's reasonable information security policies and procedures as notified to you from time to time.

(g) You must not, and must ensure that your Authorised Users do not:

(i) use the ICM:

(A) to gain unauthorised access to or interfere with any online resources or systems of any third party, including by any form of hacking;

(B) in a way that infringes the intellectual property rights or any other rights of any person;

(C) in a way that damages, disrupts, misuses or excessively uses our (or our third party service providers) hardware, bandwidth access, storage space or other resources;

(D) in a way that could interfere with any other party's use of the ICMs;

(E) in breach of any licence relating to any open source software that forms part of the ICM (as notified or communicated by us to you from time to time);

(F) in breach of our Acceptable Use Policy (which is available at: www.telstraglobal.com/acceptable-use-policy);

(G) in any manner that would put us in breach of Mapbox's Terms of Service (available at www.mapbox.com/tos/); or

(H) for the purposes of accessing, storing, distributing, providing (including to us) or otherwise transmitting material or content that:

(1) is subject to specific government regulation (for example, health and other personal information);

(2) infringes the intellectual property rights of any third party;

(3) is unlawful, misleading, abusive, obscene, pornographic, defamatory, harassing, grossly offensive, vulgar, threatening malicious;

(4) aid or implement practices violating basic human rights or civil liberties;

(5) modify, obscure, circumvent, or disable any element of the ICM or its access control features;

(6) attempt to reverse engineer, decompile, disassemble or derive any part of the source code of the ICM;

(7) modify, translate or create derivative works based on the ICM; or

(8) use any robot, spider, retrieval application or other automated functionality to retrieve or index any portion of Telstra's data, products, or services for any unauthorised purposes.

Provision and Access to the Portal

(h) At your request, we will provide you with Authentication Credentials for each of your Authorised Users to access and use the Portal.

(i) You must:

(i) only give Administrative Access to the Portal to Authorised Users who are expressly authorised by you to have full access to the Portal and Your Data;

(ii) ensure that all Authentication Credentials are kept secure and confidential and each set of Authentication Credentials is used only by one Authorised User;

(iii) comply with any policies, guidelines or other requirements that we may notify you of from time to time in relation to Authentication Credentials; and

(iv) immediately notify us and take steps to disable an Authorised User's set of Authentication Credentials if:

(A) that Authorised User ceases to be authorised by you for any reason to use the ICM;

(B) those Authentication Credentials are lost, stolen, missing or otherwise compromised; or

(C) you become aware of any breach of this clause 4.10 by that Authorised User.

(j) We reserve the right to revoke or suspend Authentication Credentials by providing you with reasonable notice if:

(i) you or your Authorised Users breach this clause 4.10;

(ii) you fail to pay us any amounts owing to us under Agreement;

(iii) you provide us with a notification under clause 4.10(i)(iv);

(iv) you ask us to do this.

(k) You are solely responsible for:

(i) all use of the ICM by your Authorised Users;

(ii) determining which Authorised Users have Administrative Access to the Portal; and

(iii) maintaining and updating, if required, access levels for your Authorised Users.

(l) You must only use the ICM:

(i) for your internal business purposes;

(ii) with the latest industry standard virus and malware detection and prevention methodologies;

(iii) in accordance with this clause 4.10.

Very important information

(m) The ICM has the potential to be used by you or your Authorised Users in a manner which could breach Federal, State, Territory privacy laws and Federal, State and Territory surveillance device laws. **You and your Authorised Users must not use the ICM to determine or track the location of a person or an object in that person's possession without their express consent or other than as permitted by all relevant laws**. It is solely your responsibility to ensure that you use the ICM as permitted by all relevant laws. You indemnify us against any loss or damage we suffer or incur and that arises naturally (that is, according to the usual course of things) in relation to any claim by a third party against us arising from your breach of any law in connection with the ICM, except to the extent the claim is caused or contributed to by us. We will also take reasonable steps to mitigate any loss or damage we suffer or incur in relation to such claim.

(n) We may suspend or cancel your ICM without liability to you if you breach clause 4.10(m).

(o) In the event that any of the Eligible Services are personal devices, you warrant that you and any Authorised Users have made the requisite disclosures and obtained appropriate consents from the owner or user of that device for the collection, use and disclosure of the data obtained from that device, in accordance with the applicable state and territory legislation.

Map data

(p) The Portal allows you to view the location of the Telstra cellular tower the IoT Connectivity Service last connected to, plotted on a map. This does not provide, and must not be used to try to determine, the location of the IoT Connectivity Service.

Acceptable use

(q) You acknowledge and agree that the ICM is not suitable, and you must not use it, for:

(i) any application that requires guaranteed data or service availability (e.g. medical, nuclear, public safety or defence applications) without our prior written consent, and you must establish separate backup services for any such applications that require guaranteed data or service availability; or

(ii) any activity where use or failure of the ICM could result in death, personal injury or environmental damage.

Additional Features and Eligible Services

Additional Eligible Services

(r) We may allow you (or your Authorised Users) to order Additional Eligible Services on the Platform. Any such Additional Eligible Services will be provided to you on the terms set out under Part G – Data Services: Telstra Wireless Machine to Machine ("M2M") of Our Customer Terms or in your separate agreement with us (if any) for those Additional Eligible Services (as applicable).

(s) If you purchase an Additional Eligible Service via the Portal, you must pay us the charges that apply to that Additional Eligible Service as set out in your separate agreement with us for those Additional Eligible Services.

Termination

(t) We use open source software and services provided by our third-party service providers in order to provide the ICM to you. If those third party service providers terminate a service we rely on to provide the ICM or an aspect of the ICM to you, we may suspend or terminate your ICM or the affected part of your ICM (as relevant) or transfer you to a reasonably comparable alternative service after giving you as much notice as reasonably possible in the circumstances. If we transfer you to a reasonably comparable alternative service and this has more than a minor detrimental impact on you, you may cancel your service without having to pay any early termination charges for that service.

Indemnification

(u) You will indemnify us against any loss or damage we suffer or incur and that arises naturally (that is, according to the usual course of things) out of any claim by a third party against us in connection with your breach of clause 4.10(f) or the claim is caused or contributed to by us. We will also take reasonable steps to mitigate any loss or damage we suffer or incur out of such claim.

Definitions and interpretation

(v) Capitalised terms used in this clause 4.10 that are not otherwise defined in this Agreement have the following meanings:

(i) **Additional Eligible Services** are Eligible Services that we may (but have no obligation to) make available for you to purchase via the Portal.

(ii) **Administrative Access** is access to the Portal that allows the relevant Authorised User to order Additional Eligible Services and make changes to your Eligible Services.

(iii) **Authentication Credentials** are the usernames and passwords that we provide to you for use in accessing the platform by your Authorised Users.

(iv) **Eligible Services** means:

(A) the Services; and

(B) Additional Eligible Services;

(C) other data plans that we agree are “Eligible Services” under your separate agreement with us (if any) for those plans.

(v) **Telstra Material** means all software, data, information, components and other material that we provide or make available to you in connection with the ICM.

5 CHARGES

5.1 Charges for your IoT Connectivity Service

The applicable fees and charges for your IoT Connectivity Services are set out in the Price Schedule section of your Agreement with us.

5.2 Changes to the charges for your IoT Connectivity Service

(a) When you sign up for an IoT Connectivity Service, the pricing for that IoT Connectivity Service will not increase for the first 2 years after the Service Commencement Date (**Initial Service Period**).

(b) On or after the end of the Initial Service Period in relation to any IoT Connectivity Service, we may increase the applicable fees and charges for that IoT Connectivity Service.

(c) If we increase the fees and charges for your IoT Connectivity Service in accordance with clause 5.2(b) above:

(i) we will notify you of the new applicable fees and charges for your IoT Connectivity Service; and

(ii) the new fees and charges for your IoT Connectivity Service will apply from the end of the billing cycle during which we notify you of those new fees and charges, and we will invoice you and you must pay us those new fees and charges in connection with the relevant IoT Connectivity Service; and

(iii) if the change has more than a minor detrimental impact on you, you may cancel your IoT Connectivity Service in accordance with the General Terms.

(d) In this clause 5.2, "**Service Commencement Date**" in relation to an IoT Connectivity Service means the date on which we begin to provide that IoT Connectivity Service to you.

6 SUPPORT

6.1 Service desk

Engagement channel	Options
Online Support	You may visit **https://connectapp.telstra.com** (Telstra Connect) at any time to report an incident or to submit a service request in respect of your IoT Connectivity Service.
Phone support	You may call 1800 370 430 9am – 6pm AEST Monday – Friday (excluding national public holidays) to speak to the Service Desk about your IoT Connectivity Service, including to report an incident or to submit a service request. Availability may be impacted by unusual call volumes.
Email support	We will use our reasonable commercial efforts to provide e-mail support during Business Hours but do not guarantee any response or resolution times. Business Hours means 9am – 5pm AEST on days excluding weekends and public holidays in Victoria.

6.2 Service levels

(a) We will aim (but do not guarantee) to resolve faults with your IoT Connectivity Service within 5 business days of you reporting a fault.

(b) Please note shipping times for SIM delivery usually takes 3-7 business days, but may take longer depending on the circumstances.