SERVICE TERMS

SERVICE OPTION: OPTUS MACHINE TO MACHINE (M2M)

This Service option forms part of the Optus IoT Services.

The Optus M2M Service Description comprises the following Parts:

- Part 1: Service Family Terms (applicable to all Optus IoT Services); and
- Part 2: The Service Terms.

The Service Terms are to be read in conjunction with both the General Terms and the Service Family Terms.

Optus has announced that it will be repurposing its 3G technology from September 2024. If you use 3G only devices, your services will be impacted and will no longer work from Sep 2024. For further information please visit: https://www.optus.com.au/support/mobiles-tablets-wearables/important-changes-3g

1. DESCRIPTION OF THE SERVICE OPTION

1.1 The Optus Machine to Machine Service (also referred to as the 'Optus M2M Service") is a carriage and service management solution. The Service allows your SIM-enabled M2M Device (such as a connected vehicle, meter, or payment device), to connect to your private enterprise IP data network or to the public internet and to manage the lifecycle of your mobile data carriage service via a web interface.

1.2 Optus M2M Service includes the following components:

(a) Optus M2M mobile data connectivity;

(b) Optus M2M access connection

(c) SIM card or SIM chip; and

(d) Access to the Optus IoT Control Centre

2. SERVICE PRE-REQUISITES

2.1 Access Connection

(a) M2M Access connection is the establishment of outbound connections from your M2M Device to a server IP address reachable by the internet or via a Virtual Private Network ("VPN")

(b) The Optus M2M Service supports the following Access Connection types:

(i) M2M VPN access via IPSEC

(ii) M2M VPN access via Optus Evolve

(iii) Public internet access

(iv) IoTFlex

(c) For M2M VPN Access Connection types, you must establish and maintain one of the below Access Connections, that meet the minimum bandwidth requirements as determined by Optus from time to time.

(i) M2M VPN access via an IPSEC connection requires you provide at your own expense an IPSEC capable router and an internet connection to use the Service.

(ii) M2M VPN access via Optus Evolve IP VPN requires a M2M VPN Port which is purchased as part of this service, and an Optus Evolve IP VPN Service which must be purchased separately to the Optus M2M Service.

(d) For IoTFlex Access Connection type, if you are to build private network connectivity via Akamai VPN Network Connector Gateway or Secure Edge – IPSec Gateway, you must meet the below requirements as determined by Optus from time to time.

(i) Private Network access via Akamai VPN Network Connector Gateway has the following requirements:

(A) Is “always-on” (i.e., not a desktop or laptop) physical machine or virtual machine (VM) with the following minimum configuration:

(I) CPU: 2-core, 2Ghz;

(II) RAM: 4GB; and

(III) Storage: 1GB.

(B) Runs one of the below versions of Microsoft Windows operating system:

(I) Windows Server 2022, 2019, 2016, 2012 R2, 2012; or

(II) Windows 10, 8.1.

(C) Has Internet access:

(I) To be able to connect to the devices and establish a secure VPN, the server or computer must be able to reach the internet (via outbound connections to both port 80 and 443)

(II) If DNS is needed in the private network, the server or computer must have access to the DNS server (usually on port 53, both TCP and UDP)

(III) The network connector might conflict with other VPN applications installed on the same host, even if not enabled at the same time.

(D) Either hosts (or has network connectivity to) the services and applications the IoTFlex services need to connect to.

(E) Does not have any other Network Connector already installed;

(F) The CPU and network requirements will vary depending on the use case. If an Akamai VPN Network Connector is running on a VM, the physical machine the VM is on needs to have enough resources to provide the connector with what it needs. If multiple VMs on a physical machine, the physical machine must have the processing power, RAM, and network capabilities to support the connector VM at peak usage.

We reserve the right to update the requirements at any time without notice.

(ii) Private Network access via the Secure Edge IPSec Gateway observe the following requirements:

(A) IPSec Per Tunnel Appliance, Connectivity and Protocol Requirements:

(I) Physical or Virtual Router or Firewall Appliance:

1) Is “always-on” (i.e., not a desktop or laptop) physical machine or virtual machine (VM).

2) Has Internet access and is reachable via a Public Static IPv4 Address.

3) Either hosts (or has network connectivity to) the services and applications the Corporate Flex mobile services need to connect to.

(II) IPSec Tunnel Protocol Support:

1) Internet Exchange Key (IKE) Version 2.

2) Encryption Algorithm equal to or greater than 256 bits, ie: AES-256.

3) Integrity Algorithm equal to or greater than SHA-2.

4) Diffie Hellman Group equal to or greater than 2.

We reserve the right to update the requirements at any time without notice.

2.2 Equipment / M2M Devices for use with the Service

(a) Your M2M Device must be an Approved Wireless Device.

(b) The Approved Wireless Device must be certified with the Regulatory Compliance Mark (RCM) compliance mark and must be:

(i) an external device such as a PC Data Card, USB modem, wireless router or tethered modem that connects to your machine to machine asset; or

(ii) an embedded mobile network compatible module within your machine to machine asset.

(c) As part of the Service, you may choose to purchase an Approved Wireless Device from Optus or one of its partners.

(d) You can request a list of Approved Wireless Devices from your account executive or by contacting Optus Customer Care.

(e) Alternatively, if you have your own wireless modem or mobile device capable of connecting your machine to machine assets and that meets the requirements in these Service Terms, you may choose to use it with the Service. You are responsible for the configuration, operation, maintenance, and repair of any equipment that you provide for use with the Service.

2.3 SIM Card(s)

(a) You must purchase a compatible Global M2M SIM Card or a compatible Local M2M SIM Card from Optus, to use this Service. The charge for the relevant SIM Card(s) will be included in your Application form.

(i) A Global M2M SIM Card allows you to send and receive SMS to and from, the M2M Device and the Optus IoT Control Centre.

(ii) An Optus Local M2M SIM Card allows you to send and receive an SMS to and from, any mobile network service provider that holds an inter-carrier agreement with Optus, inclusive of interconnection arrangements for SMS traffic.

(iii) When applicable and requested by you, an Optus Local M2M SIM Card allows you to send and receive voice calls to and from, any mobile network service provider that holds an inter-carrier agreement with Optus, inclusive of interconnection arrangements for voice traffic. You must have compatible devices to use the service.

(iv) Please note that if you use voice service and your device does not support VoLTE, your voice service will be impacted and will no longer work from Sep 2024 due to the Optus 3G switching off.

(v) When applicable and requested by you, an Optus Local M2M SIM Card allows you to send and receive VoLTE calls to and from, any mobile network service provider that holds an inter-carrier agreement with Optus, inclusive of interconnection arrangements for VoLTE traffic. You must have VoLTE compatible devices to use the service.

2.4 SIM Cards are available in the following formats and types:

(a) Triple Punch SIM Card (2FF/3FF/4FF) with temperature range of -40 to 85 degrees Celsius

(b) 2FF form factor (Standard) with temperature range of -40 to 85 degrees Celsius.

(c) 3FF form factor (Micro) with temperatures range of -40 to 85 degrees Celsius.

(d) 4FF form factor (Nano) with temperature range of -40 to 85 degrees Celsius.

(e) 2FF form factor (Standard) with temperature range of -40 to 105 degrees Celsius.

(f) 3FF form factor (Micro) with temperature range of -40 to 105 degrees Celsius.

(g) 4FF form factor (Nano) with temperatures range of -40 to 105 degrees Celsius.

(h) MFF2 form factor with temperature range of -40 to 105 degrees Celsius.

2.5 Optus will, from time to time, determine which format and type of SIM Card that is required for the Service.

3. SERVICE FEATURES

3.1 Optus IoT Control Centre access

(a) The Optus IoT Control Centre is a cloud-based software platform that provides you with self-serve functions enabling you to manage the M2M Devices in your Optus M2M Fleet.

(b) Features of the Optus IoT Control Centre include:

(i) Multi-tiered access and privileges

(ii) Automated provisioning of SIMs

(iii) Real-time usage data of all SIM Cards

(iv) network diagnostics that allow users to interrogate the status of SIM connections

(v) Rules-driven automation of actions and alerts based on the behaviour of SIMs Web-services API.

(c) You may access the Optus IoT Control Centre via the Control Centre online portal or API access.

(d) The Optus IoT Control Centre and associated user portal is a Third Party Service Provider Licenced Product powered by Cisco. Optus may change the Third Party Service Provider from time to time and will advise you of this change. Your use of the Service is subject to your acceptance of the Third Party Usage Terms.

3.2 Optus Radius access

(a) The Optus Radius feature is only supported and available for private network access connections via IPSEC or Private network access connection via Optus Evolve.

(b) Access on request to the Optus Radius Platform to:

(i) Manage Portal Administrator account access.

(ii) View Service details.

(iii) Manage your Optus M2M VPN mobile services status, authentication, and connectivity options.

(iv) Access mobile service connection and usage reporting.

4. OPTIONAL SERVICE FEATURES

4.1 You may select the following optional service features in your Application. The optional service feature is subject to the relevant additional charges set out in your Application /statement of work.

4.2 IoTFlex

(a) Optus IoTFlex provides an enterprise-grade connection to the public Internet, helping to reduce an end-customer's exposure to potential cyberthreats. Through the intuitive web-based interface, customers can provision their unique secure network requirements in real time, enabling faster and secure IoT service roll-outs, reducing deployment cost and improving operational efficiency.

(b) IoTFlex is one of the access connection types you can select when you order your M2M service. By selecting the IoTFlex option, you will be provided access to Optus IoT Control Center for SIM connectivity management and IoTFlex solution for service network and security management.

(c) The IoT Control Center and IoTFlex are integrated. IoTFlex will synchronize with IoT Control Center every 5 minutes via API integration, to retrieve and provision services automatically in the corresponding IoTFlex account.

(d) You may access the IoTFlex solution using one of the two available options:

(i) Access via the IoTFlex Online Adminstrator Portal to manage administrator user access, set up groups, define data access policies, secure users, control group and user data access, access reports and insights, view critical events, access audit logs, setup notifications on mobile data usage across the fleet, setup and manage access to Public Internet and or Private Networks and enable integration with UEM platforms; and

(ii) Access via the IoTFlex API Gateway to manage administrator user access, set up groups, define data access policies, secure users, control group and user data access, access reports and insights, view critical events, access audit logs, setup notifications on mobile data usage across the fleet and setup and manage access to Public Internet and or Private Networks.

(e) IoTFlex includes the following service features:

(i) Self-service capability to create private wireless networks on-demand via Akamai VPN Network Connector Gateway

(ii) Private Static IP.

(iii) Self-service capability to connect to multiple data clouds.

(iv) Enable SIMs to connect to the Internet and private networks.

(v) Manage and control network security policies in real time.

(vi) Block unwanted data flows with IP ACLs.

(vii) Control access to public domains with DNS security lists.

(viii) Data rate limiting of devices.

(ix) Flexible route table configuration.

(f) IoTFlex Secure Edge IPsec Gateway:

You may also select additional IoTFlex Secure Edge IPSec Gateway licence for your IoTFlex service Private Network Access.

(i) The licence will allow the ability to setup, configure, and manage eligible M2M service fleet access to a Private Network via an IPSec Gateway. The IPSec Gateway can be configured with up to 4 IPSec tunnels (2 per site) for mobile data traffic capacity and redundancy flexibility.

(ii) A single IoTFlex Secure Edge Gateway and corresponding licence can only be enabled on a single IoTFlex account and only be usable by the IoTFlex Services enabled on that account. A single Secure Edge Gateway cannot be enabled on more than a single IoTFlex account. If multiple IoTFlex accounts require access to a single Private Network via IPSec, then each of those accounts will need to be setup and enabled with its own Secure Edge IPsec Gateway licence.

(g) When you select IoTFlex you will also have access to IoT Control Centre for SIM connectivity management. IoT Control Centre is integrated with IoTFlex.

(h) The IoTFlex platform and associated user portal is a Third Party Service Provider Licenced Product provided by Akamai. Optus may change the Third Party Service Provider from time to time and will advise you of this change. Your use of the Service is subject to your acceptance of the Third Party Usage Terms.

5. SERVICE REQUIREMENTS AND LIMITATIONS

5.1 Optus as a Carrier and Carriage Service Provider must comply with all relevant Industry Codes, Australian Standards, and laws, including Industry Codes registered by the Australian Communications & Media Authority (ACMA). Optus has issued you with mobile phone numbers for use with the Service for originating and receiving phone calls using the associated SIM. The use of these numbers is regulated by the ACMA and in particular via the CA C661:2020 Reducing Scam Calls Industry Code. This Code requires Optus to detect and block certain call types that may be associated with scam activity, including calls displaying Australian Mobile Service Numbers as the A-Party Calling Line Identifier (CLI) information on phone calls received by Optus. Accordingly, if you use an Optus provided Australian Mobile Service Number to make a call that is not supported by the Service, that call may be blocked.

5.2 Global M2M SIM Card

You acknowledge and agree that:

(a) The Global M2M SIM Card does not support sending or receiving of SMS messages to or from, any other mobile service or voice access.

(b) Where you select a Global M2M Sim Card, you will not be issued with a MSISDN (Mobile Subscriber Integrated Services Digital Network-Number) for use with the Service and, as such, any service number allocated will not be available for mobile number porting.

5.3 Local M2M SIM Card

You acknowledge and agree that:

(a) The Local M2M SIM Card may only be used for:

(i) originating mobile traffic or other mobile services, on the Optus Mobile Network; and

(ii) terminating mobile traffic or other mobile services, on the Optus Mobile Network, which originate on our networks or on the network of another supplier with which we have a current interconnection arrangement.

5.4 We may monitor your use of the Optus Global M2M SIM Card and Optus M2M Local SIM Card to ensure that it is for the Permitted Purpose, is not in breach of these Service Terms and is compliant with all relevant laws and any directions of Regulators in connection with the Service.

5.5 If you use the Optus Global M2M SIM card and Optus Local SIM Card for anything but the Permitted Purpose or breach any other term of the Agreement, and we consider that the impact of this is materially detrimental to Optus, we may immediately suspend, Downgrade, cancel, terminate or limit the Service or impose conditions on the continuance of the Service.

5.6 Service restrictions

(a) The Service cannot be used for M2M Devices in your M2M Fleet that are overseas unless you have:

(i) the option of international roaming included in your pricing plan; and

(ii) the M2M Device and the relevant SIM Card has roaming activated; and

(iii) the M2M Device is compatible with the network availability in your roaming location.

5.7 Optus cannot guarantee that the Optus M2M Service can be used successfully with M2M Devices that are overseas. International roaming is not available in all countries or in all areas of countries. The countries in which international roaming is available may change from time to time. Furthermore, some wireless modems or modules only operate with the networks of certain countries. For further information, please contact your account executive or Optus Customer Care.

5.8 The Service is only available for use with new SIM connections. The Service does not include and does not support the migration of existing mobile data services to the Optus M2M Service.

5.9 The Optus SIM Card must not be used (even if used for the Permitted Purpose):

(a) with SIM cards/chips that have been on-sold to third parties;

(b) to transit, refile or aggregate domestic or international traffic on the Optus Mobile Network; or

(c) in connection with a device that switches or reroutes calls to or from the Optus Mobile Network, or the network of any supplier.

5.10 Your obligations, and our rights, under the Agreement are additional to those obligations and rights in the Fair Go Policy.

5.11 Connection Speed

(a) The speed of the Service will depend on, among other things, the data transfer speeds and factors including:

(i) The type of Optus Mobile network used to connect to the Service. For example, you may obtain faster data transfer speeds on the Optus 5G Network compared to the Optus 4G Network;

(ii) The type of M2M Device (wireless modem or mobile) used to connect to the Service;

(iii) The location of the M2M Device when using the Service;

(iv) The number of users sharing the Optus Mobile network at the location;

(v) The speed of the connection chosen between the Optus Mobile network and your private enterprise IP data network;

(vi) general private enterprise IP data network activity;

(vii) the speed and capacity of the server or application you access within your private enterprise IP data network; and

(viii) the speed and capacity of your internet connection.

(ix) Whether any speed throttling has been applied to the M2M Service.

5.12 IoTFlex Service limitation or restriction

(a) For the Private Network Gateway connectivity options (Akamai VPN Network Connector, Secure Edge - IPSec Gateway:

(i) The Internal IP Address range 10.128.0.0/10 is reserved for internal usage by the platform and can not be used by the Customer or exist in the network the service is intended to be linked with.

(ii) LAN Subnets (i.e., Subnets behind the connecting mobile device) are not supported.

(iii) Dynamic Routing (i.e., RIP, BGP) is not natively supported by the underlying mobile data connection, IP tunnelling technologies (such as GRE) can be used to provide this capability ontop of the underlying mobile data connection if required.

(b) Certain Reporting, Quota and Time Access Control is enforced based on the customers IoTFlex Account time zone. This time zone cannot be changed by the Optus Customer themselves and is defined at the initial account setup.

(c) A single Customer IoTFlex account can only have a maximum of 8 Networks enabled.

(d) The Secure Edge – IPSec Gateway Licence is chargeable as soon as the licence has been applied to the IoTFlex account regardless of whether the IPsec Gateway has been enabled and configured or not.

(e) The Secure Edge – IPSec Gateway Licence can be configured with up to 4 IPSec Tunnels (2 per site) for capacity and redundancy flexibility.

(f) The Secure Edge – IPSec Gateway Licence can only be enabled and configured via the IoTFlex Online Adminstrator Portal, it cannot be enabled or configured via the IoTFlex API Gateway.

(g) A maximum of 16,384 devices can be supported per Network.

(h) If a M2M service is suspended or moved to another Customer Account (i.e., CHOWN), the M2M service will be removed from the IoTFlex account and all reporting usage, events, Group and Access Policies will be reset to defaults upon re-enablement of the service.'

(i) The following data available on the solution is retained for a maximum:

(i) Account & Service Internet, Data and Blocked usage Reporting: 6 months;

(ii) Account Audit Logs: 90 days;

(iii) Service Events Logs: 48 hours.

(j) The maximum reporting data export period is 1 month (1 cycle) at a time.

(k) Reporting data update frequency is as follows:

(i) Account and Service Data Usage: Updated in near-real time when device ends their mobile data session;

(ii) Service Event Logs: As soon as the event occurs;

(iii) Account Audit logs: As soon as an audit event occurs.

(l) The IoTFlex Account quota and usage period is based on a Calendar month which may differ from your Billing / Invoice cycle or period.

(m) Audit and Events logs cannot be exported from the IoTFlex Online Adminstrator Portal, however can be extracted, and stored via the IoTFlex API Gateway access option.

(n) Any changes made to a IoTFlex Group, Access or Zone Policy or if a device is moved to a new IoTFlex Group Policy the updated or new Group, Access or Zone Policy will come into effect the next time the device attachs to the Mobile network (i.e. if the device is attached at the time the Policy is updated, the updated policy will only take effect when the device discounts and re-attachs to the Mobile Data network).

(o) Update to more than 50 devices at a time would be deemed as a bulk update. It is not possible to make bulk updates to the Device information in the IoTFlex Online Adminstrator Portal itself, this however can be done via the IoTFlex API Gateway access option.

(p) Enabling certain end user data cut-off restriction policies may result in the end user device being unable to access 4G Voice Call capability (also known as VoLTE or Voice over LTE). It is recommended that if a service must have voice call access that these data restriction policies are only applied with caution. These policies include:

(i) Device cut-off due to exceeded data usage within the calendar month, in this scenario suggest that a "throttle" (check if correct) policy is used instead;

(ii) Data Access Time restriction if certain times are set to restrict data access;

(iii) Roaming / Zone restriction if a user attempts to use the service in a data restricted Zone (Country / Carrier).

(iv) Device has its Interfaces manually disabled either via the IoTFlex Online Administrator Portal or API Gateway.

(q) The IoTFlex Online Administrator Portal login process in addition to an Email Address and password uses a two factory Authentication (2FA) Login security challenge via a Mobile/Phone number (i.e., SMS sent Code or Call) to authenticate

the Administrator user login request, two factor authentication via email or any other form is currently not possible.

(r) For Devices associated with a “Private Network” Gateway, the Devices assigned Internal Static IP Address, which is assigned at device creation from the next available IP Address in the Networks Device IP Address range, cannot be changed once the device has been created.

(s) A Policy Group can either have a Daily or Monthly Usage quota’s defined, it is not possible to set both Daily and Monthly Quota’s on a Policy Group at the same time. If this option needs to be changed after being initially set the Zone will need to be removed and re-added again.

(t) An Access Policy which can be associated with one to many Policy Groups and can enforce data speed throttling on the device(s) that meet the conditions the Access Policy is configured with, the speed throttle options when applied range from 20Mbps to 100Kbps when throttling is to be applied.

(u) If an end user attempts to access a blocked site / resource it will not show a custom or blocked access message, it will just not load or connect to the page or resource, this is by design due to the way secured access to Websites works on the Public Internet (SSL / HTTPS), i.e. cannot act as a middle man in a secured connection to show a ‘custom / error’ message to the end user.

(v) All IoTFlex account and service Data is stored in Amazon Web Services (AWS) within Australia.

(w) IoTFlex is a “Network” based solution, meaning it provides control at a “Mobile Network Layer”. Its capabilities do not apply to SIM connectivity management, such as SIM provisioning, SIM state change, rate plan management etc. These functions are managed in the Optus IoT Control Center.

(x) The Optus IoT Control Center and IoTFlex are integrated. IoTFlex will synchronize with the IoT Control Center every 5 minutes via API integration, to retrieve and provision services automatically in the corresponding IoTFlex account. Any newly added SIMs will be displayed under the default network in the customer IoTFlex account.

5.13 Fault Reporting

(a) As soon as you become aware of any Incident in the Service, you must report that Incident to Optus by either logging an incident on the self service portal or telephoning the number notified to you by Optus from time to time. The number will be available 24 hours a day, 7 days a week.

(b) Before reporting an Incident to Optus, you must take all reasonable steps to ensure that the Incident is not attributable to a Service Exclusion. If Optus determines that the Incident is attributable to a Service Exclusion, Optus may charge you for reasonable costs incurred in the investigation of the Incident (including any professional or other services as required).

(c) If you require Optus to respond to and resolve Incidents, your Authorised Representative must report the Incident to Optus via the Service Desk or Self Service Portal. All Priority 1 and Priority 2 Incidents must be reported via telephone to the Service Desk.

5.14 General

(a) The Service does not include remediation works required to ensure that your network or systems are sufficient to run the Optus M2M Service.

(b) You are responsible for ensuring that M2M Devices and facilities are compatible for use with the Service and continue to be compatible with subsequent revision levels of Third Party Service Provider provided equipment, software, and services.

(c) [Not used]

(d) Where the Service is accessed via a third party carriage or internet service, the service Delivery Point, which is the demarcation point for Optus responsibility, is the last router managed by Optus.

(e) Where the Service is delivered over the Internet, it may traverse networks and equipment that Optus has no control over. Optus will use reasonable endeavours to ensure the Service is delivered in accordance with this Agreement but will not be responsible for the performance and functionality of those components.

(f) Optus is not able to guarantee data network quality of the Service, where your Access Connection is interrupted.

(g) You will comply with, and you will use all reasonable endeavours to ensure each End User complies with, all directions of a Regulator and all reasonable directions of Optus.

(h) Optus may subcontract with one or more Suppliers to provide on its behalf any or all Services.

6. CHARGES

6.1 The charges for the Service are set out in your Application and are incurred from the Service Start Date. The Service Start Date is defined in the Optus General Terms and deemed to be, the date on which the SIMs ordered under your Application have been dispatched and loaded by Optus into your Optus IoT Control Centre inventory.

6.2 The charges for the Service consist of:

(a) once off charges, including:

(i) SIM ordering charge;

(ii) IoTFlex platform onboarding fee, where applicable;

(iii) configuration charge for the M2M VPN access via Evolve IP VPN or IPSEC via Internet;

(iv) configuration charge for the IoTFlex Secure Edge IPsec Gateway licence, where applicable;

(v) Professional services, where applicable;

(b) recurring charges, including dependent on the relevant service feature:

(i) Monthly service subscription charge with the following options:

(A) Stand-Alone;

(B) Flexi-Pool;

(C) Fixed-Pool.

Depending on the Service Option you select, your service subscription charge may have included usage allowance to use each month for services such as data, SMS or voice. Unless specified otherwise, all included service usage and usage charges are for use within Australia.

(ii) Monthly recurring IoTFlex charges, with the following options, where applicable

(A) Stand-Alone;

(B) Flexi-Pool;

(C) Fixed-Pool.

(iii) Monthly access charge for IoTFlex Secure Edge Gateway licence(s), where applicable.

The Secure Edge IPSec Gateway Licence is chargeable as soon as the licence has been applied to the IoTFlex account regardless of whether the IPSec Gateway has been enabled and configured or not.

A Secure Edge IPSec Gateway Licence can be configured with up to 4 IPSec Tunnels (2 per site) for capacity and redundancy flexibility. You can order multiple licences. The monthly access charge is calculated as the sum of all monthly access charges for the relevant IoTFlex Secure Edge Gateway licences.

(iv) Monthly access charge for the M2M VPN private network access via Evolve IP VPN or IPSEC via Internet, where applicable.

(c) Excess usage charge.

(d) any other charges as specified in the relevant M2M Service Terms or Application.

7. CUSTOMER OBLIGATIONS

7.1 In using the Service, you must comply with Optus' Fair Go Policy and any rules imposed by any third party whose content or services you access using the Service or whose network your data traverses.

7.2 The Service does not include, and Optus is not responsible for, any configuration of the equipment that you use in connection with the Service. This includes the configuration of any wired or wireless connectivity that may be supported by the equipment that you use in connection with the Service.

7.3 You are responsible for ensuring that:

(a) the equipment you want to use with the Service is correctly configured; and

(b) you have compatible web browsers to access the Optus IoT Control Centre and/or IoTFlex.

(c) You may only authorise named administrators and/or end users to use the Service. You must keep an up-to-date register of these authorised personnel and make it available for Optus' inspection at all times on request.

7.4 In relation to Optus IoT Control Centre and/or IoTFlex platforms, you undertake that:

(a) You will not allow any account profile to be used by any other unregistered user unless it has been reassigned in its entirety to another individual, in which case the prior individual shall no longer have any right to access or use the account;

(b) You shall keep a secure password for the use of the account/s, that such password shall be changed as frequently as is required by us in our absolute discretion, and that you shall keep the password confidential;

(c) You shall permit us to audit the accounts in order to establish compliance with this Agreement; and

(d) If any of the audits referred to above reveal that any password has been provided to any individual who is not registered to an Optus IoT Control Centre and/or an IoTFlex platforms account, then without prejudice to Optus's other rights, you shall promptly disable such passwords and Optus shall not issue any new passwords to any such individual.

(e) You are responsible for the conduct of your Personnel while using the Optus IoT Control Centre and/or IoTFlex platforms. You must not, and must take all reasonable steps to ensure your Personnel do not, use Optus IoT Control Centre and/or IoTFlex platforms for any of the following:

(i) violating intellectual property rights;

(ii) any illegal or criminal activities;

(iii) depicting sexually explicit images;

(iv) promoting unlawful violence;

(v) the storage, distribution or malicious distribution of any viruses or any material during the course of your use of Optus IoT Control Centre and/or IoTFlex platforms;

(vi) threatening, obscene, harassing, defamatory, discriminatory, racially, or ethically offensive or other objectionable behaviour;

(vii) causing damage or injury to any person or property;

(viii) sharing IoTFlex with other users who are not licensed;

(ix) using, displaying, mirroring or framing Optus IoT Control Centre and/or IoTFlex platforms or any individual element within the platforms, Optus's name, any Optus trademark, logo, or other proprietary information;

(x) altering, tampering, or circumventing any part of Optus IoT Control Centre and/or IoTFlex platforms;

(xi) providing services to third parties;

(xii) attempting to obtain, or assist third parties in obtaining access to Optus IoT Control Centre and/or IoTFlex platforms, other than as provided under this Agreement;

(xiii) attempting to reverse compile, disassemble, reverse engineer or otherwise commercially exploit, or otherwise make Optus IoT Control Centre and/or IoTFlex platforms available to any third party;

(xiv) attempting to copy, modify, duplicate, create derivative works from framing, mirroring, republishing, downloading, displaying, transmitting, or distributing all or any portion of Optus IoT Control Centre and/or IoTFlex platforms, except to the extent expressly permitted under this Agreement;

(xv) accessing all or any part of Optus IoT Control Centre and/or IoTFlex platforms in order to build a product or service which competes with Optus IoT Control Centre and/or IoTFlex platforms;

(xvi) licensing, selling, renting, transferring, assigning, distributing, displaying, disclosing, or otherwise commercially exploiting, or otherwise making Optus IoT Control Centre and/or IoTFlex platforms available to third parties; and

(xvii) testing the vulnerability of any part of Optus IoT Control Centre and/or IoTFlex platforms or for breaching any security or authentication measures.

(f) You agree not to access your Optus IoT Control Centre and/or IoTFlex platforms account and the platforms through the use of any mechanism other than through the use of an authorised connection.

7.5 Optus is not liable for any costs, expenses, liabilities, losses, or damages caused by your failure (or the failure of anyone in your organisation) to maintain the confidentiality of your Optus IoT Control Centre and/or IoTFlex account credentials. It is your responsibility to keep your account information up to date in your account settings.

7.6 Optus reserves the right, without liability to you, to disable your access to your account or to any material as a result of any breach of the provisions of this clause.

8. THIRD PARTY USAGE TERMS

8.1 The Service includes the on-supply of third party products by the Third Party Service Provider.

8.2 You may be required to agree to the Third Party Usage Terms and any warranty, support or other terms referenced within those terms, or provided with or embedded within the Product.

9. PRODUCT OR SERVICE RIGHT OF USE

9.1 Subject to your acceptance of and compliance with the Service Terms, the Third Party Service Provider will grant you a non-exclusive, non-transferable direct licence for the term of the Agreement to use the Licensed Product for your internal operation and maintenance purposes and not for commercial distribution, re-sale, or other trade dealing.

9.2 You acknowledge and agree that the Third Party Service Provider of the Licenced Product is a third party beneficiary of your right of use and may seek to enforce the terms of your rights of use directly.

10. SPECIAL CONDITIONS

10.1 **Offshore Access To Information**. The Service relies for its operation on services supplied by third parties who are not controlled by Optus. Components of the Service utilise infrastructure hosted in the United States of America and Singapore, and as such information relating to you and your use of the Service may be hosted on servers outside of Australia. This information may include your company name and address, administrator

name and email address, Service usage details and billing data. In using the Service, you, and your personnel consent to Optus or our third party disclosing this information to the relevant third parties at locations outside of Australia where reasonably necessary to provide the Service.

10.2 You will indemnify and hold harmless Optus and its affiliates, employees, agents and/or distributors, from and against any claims, disputes, demands, liabilities, damages, losses, and costs and expenses including, without limitation, reasonable legal fees arising as a direct result of (i) your access to or use of your Optus IoT Control Centre account and/or your IoTFlex account (ii) your access to or use of your Optus IoT Control Centre and/or IoTFlex platforms , or (iii) your breach of any of your responsibilities or any other provision of this Agreement, each of which are not within Optus' reasonable control. Optus reserves the right to assume control of the defence of any third party claim that is subject to indemnification by you, in which event you will cooperate and assist Optus as required. Optus will use its reasonable efforts to mitigate the extent of liabilities, damages, losses, and costs and expenses incurred by it with respect to this indemnity.

10.3 You agree that your obligations are neither contingent upon the delivery of any future functionality or features nor dependent upon any oral or written comments made by us with respect to future functionality or features. Optus is not liable to you or to any third party for any update, change, suspension, discontinuance of any feature or component of Optus IoT Control Centre and/or IoTFlex platforms. Optus reserves the right to determine the timing and content of software updates, which may be automatically downloaded and installed without your notice.

11. RELEVANT APPENDICES

11.1 Optus M2M Standard Pricing Table

11.2 The Fair Go Policy, for more information see optus.com.au/fairgo.

12. DEFINITIONS – SERVICE TERMS

Terms not defined in these Service Terms are as defined in the Service Family Terms or the General Terms (in that order).

Term	Definition
Access Connection	means a telecommunications data service between your nominated equipment and our provider edge routers in an Optus exchange.
ACL	means Access Control List.
Approved Wireless Device	means a wireless modem or a wireless module, tested and approved by Optus for use with the Service and that meets the requirements set out in these Service Terms.
Data Allowance	means the maximum amount of data usage (the sum of uploaded and downloaded data) able to be used with the Service without incurring excess usage charges.
DNS	means Domain Name System.
Fixed Pool	means a Shared Data Plan that shares a single pool of predefined, fixed usage across all services on the plan.
Flexi Pool	means a Shared Data Plan that aggregates usage incrementally across all services on the plan. The size of the pool depends on the number of devices activated in the same Flexi Pool data plan. If a customer has multiple Flexi Pool data plans, the usage is aggregated across the services on the same rate plan, not across multiple rate plans.

IoT Control Centre	has the meaning given to it in these Terms.
IoTFlex	means cloud-based software platform that provides you with self-serve functions enabling you to manage the network in your Optus M2M Fleet.
Incident	means an unexpected event which is not part of the standard operation of the relevant Service and causes disruption or degradation to that Service.
IP	means Internet Protocol.
IPSEC	means Internet Protocol Security.
Licenced Product	means the Third Party Service Provider software and/or platform or other services specified in the statement of work.
Maintenance	means maintenance conducted on the Service, Optus Equipment, or the Optus Network (including upgrades to maintain Products used by Optus to provide the Service, at vendor supported versions), including the maintenance activities referred to in this Service Description
M2M Device	means an Approved Wireless Device.
M2M Fleet	means a group of SIM connections with a Shared Data Plan.
Optus Radius Platform	means the Optus network components used to provide authentication, authorization, and accounting (AAA) services and the customer management interface (CMI) web portal.
Permitted Purpose	means the M2M Device approved for use on the Optus Mobile Network.
Pricing Plan	contains information about the terms and conditions and prices of the plan (including services and features) you have selected in your Application for the Service and are set out in the Application.
RCM (Regulatory Compliance Mark)	is a compliance label produced by the electrical regulator (Regulatory Authorities (RAs)) and Australian Communications and Media Authority (the ACMA). It indicates that an item is compliant with electrical safety, EMC, EME & telecommunications requirements, as applicable to each product. For more information on RCM see: www.acma.gov.au
Related Service Option	means other Optus services that are pre-requisites to obtaining the relevant Service and must be acquired separately for use with the Service.
Service Exclusion	means where the In-Scope Service is affected by: (a) Maintenance; (b) an Excluded Event; (c) a Force Majeure Event; (d) insufficient bandwidth of the Access Connection used to connect to the Service; (e) any carriage service provided by Optus under another agreement or by a third party service provider; or (f) an Incident raised prior to the Service start date.
Service Family Terms	mean the terms applicable to each Service option as set out in Part 1 of this Service Description
Service Terms	means these product/service specific terms.
Shared Data Plan	means a shared Data Allowance applicable to a group of SIM connections, amalgamated under an approved Pricing Plan.

SIM Card	means a subscriber identity module (card or chip) embedded in, or used with, a device that identifies and authenticates the device as a user on a mobile telecommunications network.
SMS	means short message service of up to 160 characters in length.
Stand-Alone	means a pricing plan that allocates usage to a single SIM connection service only.
Target Service Start Date	means the date requested by you and/or estimated by Optus and agreed between the parties, as the target date on which the service is intended to be activated and supplied to you, as specified in the statement of work.
Third Party Service Provider	means each of Asavie Technologies Limited and Jasper Technologies LLC.
Third Party Usage Terms	means, in addition to any terms and conditions referred to in the corresponding definition set out in the applicable Service Family Terms, the terms and conditions set out in: (a) the Akamai/Asavie Acceptable Use Policy located at https://www.akamai.com/legal/privacy-and-policies/acceptable-use-policy; and (b) the Cisco end user license agreement, available at https://www.cisco.com/c/en/us/about/legal/cloud-and-software/end_user_license_agreement.html
VPN	means virtual private network.