This Private Mobile Connection – Attachment ("Attachment") describes the Private Mobile Connection (PMC) services provided by AT&T to Customers. Private Mobile Connection 5G (PMC 5G) service is a subset of Private Mobile Connection service and collectively, or individually as applicable, is referred to as "Service". The provisions in this Attachment apply to both services unless expressly noted as applying only to PMC or PMC 5G. In the event of a conflict between other terms and terms in this Attachment, the terms in this Attachment will control.

1.0 SERVICE DESCRIPTION SUMMARY

PMC services, including PMC 5G where applicable, enable businesses to extend their WAN infrastructure more securely and reliably to mobile end points by providing standards-based connectivity options between the enterprise and cellular networks.

- The Service segments & isolates customer cellular data traffic within the AT&T Mobility core network via customized IP routing protocols.
- Customer's cellular data traffic is separated from public data traffic within unique network cores utilizing geo-redundant enterprise grade routers, firewalls, and other network elements.
- Cellular data traffic is routed between the mobile device and Customer's WAN or cloud via private or public secured internet or intranet connections via rules established in the custom design.
- Services are device agnostic, allowing virtually any AT&T certified mobile device to utilize.

2.0 PRIVATE MOBILE CONNECTION SERVICES

Pursuant to the terms and conditions of this Attachment, AT&T will provide PMC Services for the duration of the Service Term to requesting Customers possessing a separately obtained and AT&T qualified device, rate plan, and SIM. z

3.0 DEFINITIONS

The following definitions apply to PMC.

"APN" means "Access Point Name". A gateway enabling a data connection over a mobile network to another computer network. An APN contains the customization, rules and restrictions designed for use in 4G and earlier network cores.

"AT&T VPN Components" means the facilities and service components between Customer's FES and the AT&T network including, without limitation, the AT&T VPN port, the AT&T VPN MPLS VPN, and the MPLS Interconnect necessary to provide services.

"AT&T VPN" or "AVPN" means AT&T's Virtual Private Network service that can be accessed via wireline and mobile connections between devices and Customer FES. AVPN is an Intranet connection utilizing MPLS.

"Connection Right" means the conditional right to connect to AT&T's mobile network through Private Mobile Connection Services

"CPE" means customer premises equipment.

"CTN" means customer telephone number. Also referred to as line of service, subscriber line of service, or customer line of service.

"Custom" in relation to Service means a solution designed for and dedicated to Customer with customized attributes and features allowing Customer to specifically define the behavior of the Service.

"DNN" means "Data Network Name". A gateway enabling a data connection over a mobile network to another computer network. A DNN contains the customization, rules and restrictions designed for use in 5G network cores.

"EPL" means Enterprise Permit List which contains a best effort minimal set of firewall rules provided by AT&T to be used in the absence of Customer provided rules. This list identifies if and how addresses are allowed to traverse the AT&T mobile network when used with this "Service".

"FES" means Customer's fixed end system that includes, but is not limited to, Customer's host, server or gateway system that hosts Customer's enterprise applications and specialized databases.

"Firewall" means a network security system of hardware and software that allows or blocks IP traffic between networked devices on either side. This includes IP addresses, IP ranges, subnets, ports, and other IP protocols.

"GBL" means Global Block List which contains a best effort minimal set of network addresses known or considered by AT&T to be dangerous. These addresses are blocked from traversing the AT&T network to prevent various types of activities or data that may harm Customer, devices and networks to which they connect.

"Gbps" means gigabits per second

"Host Application" means a software or other enterprise application Customer intends to use in connection with the Service.

"IETF" means Internet Engineering Task Force. A standards organization for the Internet and is responsible for the technical standards that make up the Internet protocol suite

"Internet" means an open network connecting many computer networks based on a common addressing system and communication protocol that is generally accessible by any device with a connection to it.

"Intranet" means a closed loop network connecting specific computer networks and devices based on a common addressing system and communication protocol that is not generally accessible unless authorized and configured by an administrator accordingly. Intranet networks can be dedicated or routed securely over the Internet via tunneling solutions like AVPN.

"IP Charge(s)" means the monthly recurring charges payable by Customer to AT&T in connection with public IP addresses described in this Service Guide.

"IP" means Internet Protocol.

"IPsec" means IP Security or Internet Protocol Security, a secure data packet encryption protocol used in VPN connections over Internet connections as documented in the respective IETF RFCs.

"Kbps" means kilobits per second

"Mbps" means megabits per second

"Monthly Recurring Charge" (MRC) means charges that are billed for Services on a monthly basis for the duration of its use.

"MPLS" means multi-protocol label switching documented in the respective IETF RFCs.

"Non-Recurring Charge" (NRC) means charges that are billed for Services one time and do not repeat.

"Premises" means Customer's facility(s) where the FES is located.

"Private Mobile Connection" (PMC)," including as applicable **"Private Mobile Connection 5G" (PMC 5G),** means an AT&T network solution to customize IP data traffic routes and capabilities, utilizing separate, enterprise grade network hardware and software.

"Proxy Mobile IP" or (PMIP) means the service provided to wireless router devices utilizing the proxy mobile IP protocol as defined by RFC5213 and RFC5844 Internet standards.

"Set-Up Charge(s)" means the set-up charges for Professional Services, payable by Customer and related to a custom Service setup, as described in this Service Guide.

"Shared" in relation to Service means a common solution used by multiple Customers with specific fixed features and capabilities allowing Customers to utilize certain common features of the Service.

"VPN" means Virtual Private Network

4.0 CONNECTION RIGHT AND LIMITATIONS

4.1. Connection Right.

AT&T hereby grants Customer a revocable, limited Connection Right for use during the Service Term with one or more Host Applications, subject to the limitations set forth in §4.2.

4.2. Limitations

4.2.1. The Host Application must be used solely in connection with the transmission of Customer's data to and from Customer's End Users that are using the Service.

4.2.2. Customer must not offer, resell, or otherwise make the Connection Right available to third parties.

4.2.3. The Connection Right is not exclusive.

4.2.4. Traffic originating from Customer's network over the Service may only be addressed to the assigned IP address ranges of its Equipment on the AT&T network. Traffic addressed to any other IP destinations will be discarded by AT&T without notice.

4.2.5. The Connection Right must not be used to send SMS messages, and no data or other content may be passed via an SMS message, either from a Host Application to an End User's Equipment or from an End User's Equipment to a Host Application; provided, however, that Customer may use the Connection Right to send SMS messages solely as a signal to activate an End User's Equipment.

4.2.6. Customer must only use equipment that meets quality standards set by the Federal Communications Commission and is certified by AT&T in advance of use. Customer agrees that AT&T has the absolute right to approve or disapprove any equipment used.

4.2.7. Certain changes to an in production DNN may not be supportable. If AT&T determines that the changes required cannot be accommodated via the Change Order process, Customer will be advised. Such changes that cannot be supported will require a new DNN build.

4.2.8. For Custom AT&T VPN ("AVPN") configurations, not all AT&T VPN service capabilities, service level agreements, or features are available or interoperate with the Service.

4.2.9. Due to the nature of the Service, non-AT&T applications and services that require data connectivity may not operate unless specifically allowed in AT&T or Customer firewalls. As an example, Google RCS and Apple's iMessage IP-based messaging products require access to their respective host applications or servers and must be accounted for in both AT&T and Customer firewall rules during the design phase. Connectivity to and between applications, servers and/or hosts that were not defined within the AT&T firewall rules during the design and build of the custom Service will require a Change Order to modify the rules to allow IP traffic.

4.2.10. For custom VPN solutions, The Connection Right is for access to a single connection provided; however, Customer will receive, at no additional Set-Up Charge, a backup Connection Right for a second connection if Customer orders a backup Service connection together with the primary Service connection. If Customer (a) declines to order a backup Service connection when ordering the primary Service connection or (b) orders one or more Service connections to supplement its existing Service connection, then Customer must pay an additional Service Set-Up Charge. Customer acknowledges that if there is a failure or extended maintenance of the primary Service connection and Customer does not have a backup Service connection, Customer's End Users will not be able to connect to Customer's network or send data to, or receive data from, the Host Application. Both Primary and Secondary connections will be defined in a common custom APN or DNN, and both will connect to a single end point on the AT&T network.

4.2.11. Service Coexistence: PMC 5G is designed and hosted on AT&T's Next Gen 5G Standalone network core. Due to this advanced network architecture, products and services that depend on previous enterprise mobile cores are generally unavailable. To support both 5G Standalone services like PMC 5G and services hosted on previous network cores at the same time, when a 5G SA Customer requests non-5G SA products or services on their CTN, AT&T will place the device on the network capable of providing access to all the requested products and services. This may result in 5G SA subscription being placed on a 5G NSA or 4GLTE network. PMC 5G will still be accessible on these non-5G SA networks but it may be subject to slight performance degradation as it traverses the network cores from 5G NSA or 4GLTE to SA.

4.2.12. Decommissioning of Service by AT&T. AT&T reserves the right to decommission Customer's Service from the network due to cancelation/disconnection of account hosting the Service, or 12 consecutive months or more of non-utilization of the Service on purpose or due to suspension. If decommissioned, Customer may be required to restart the Service onboarding process, including paying the applicable Set-up Charges, to reestablish Services specific to its requirements and needs. Decommissioning of the Service removes the solution attributes defined in the APN or DNN from all relevant network elements and releases any public IP address pools or assignments back into available inventory. This activity may result in any specific IP address assignments or pools as well as the APN or DNN name may not be available to Customer in the future.

5.0 CUSTOMER RESPONSIBILITIES

5.1. FES Premises Solutions

5.1.1. Install Router and Related Hardware. Prior to Test and Turn-Up of the Service, Customer must install, at Customer's sole expense: (a) a router with applicable serial interface card; and (b) in the case of AVPN, the inside wiring between the demarcation point of AT&T VPN transport termination to Customer's router at its Premises.

5.2. Host Applications.

5.2.1. Host Application Responsibility. Customer must, at its own expense, develop, procure, implement and/or operate any and all Host Applications.

5.2.2. Host Application Approval. Customer acknowledges and agrees that deployment of Service is subject to AT&T's review and approval of Customer's Host Applications. Customer must submit a written request for approval by AT&T prior to any modification of the network traffic profile or the addition of a new Host Application. In the event Customer modifies a Host Application without AT&T's prior written approval or adds additional Host Applications or features to existing Host Applications without an AT&T approved Customer order for such modifications or additions, AT&T may immediately suspend or terminate the Connection Right.

5.2.3. Host Application Testing. AT&T reserves the right, but is not obligated, to test any Host Application prior to the initial connection or any time during the term to confirm that such Host Application is in compliance with the terms and conditions of the Service.

5.3. IP Addresses.

Customer acknowledges and agrees that it must have either public static IP addresses, private static IP addresses, public dynamic IP addresses, or private dynamic IP addresses in connection with the Service.

5.4. Network Use

The Service operates over AT&T's enterprise-grade network and shared enterprise infrastructure, which is designed to support standard, commercially reasonable business usage patterns at scale. Certain unique, atypical, high-intensity usage, traffic patterns, or implementations of the Service may create conditions that adversely affect the operation, stability, security, or performance of AT&T's network or the services provided to other customers. Customer is responsible for ensuring that its use of the Service does not create such conditions. Upon AT&T's request, Customer shall cooperate with AT&T and provide relevant technical or operational information relating to Customer's use of the Service as necessary for AT&T to evaluate the impact of such use on the network or other customers. AT&T reserves the right, but not the obligation, to monitor, evaluate, and audit Customer's use of the Service to determine whether such use is, or could reasonably be expected to be, detrimental to AT&T's network, infrastructure, or service levels experienced by other customers. If AT&T determines that Customer's use of the Service is causing or may cause material degradation, disruption, or instability to the network or to other customers' services, AT&T may suspend, with advance notice to the extent practicable under the circumstances, all or a portion of the affected Service to the extent necessary to protect network operations and restore normal service levels. AT&T will work with Customer to identify and implement, at Customer expense, modifications to Customer's use of the Service, so that service may be resumed in a manner consistent with network requirements. Service may remain suspended until such modifications are implemented to AT&T's satisfaction.

5.5. Security.

Customer is solely responsible for maintaining security for connectivity between Customer's network and AT&T's mobile network. Customer must comply with all security requirements and procedures established by AT&T and provided to Customer and must use an industry standard virus protection program on all networks that Customer maintains that may be accessed by the Service. All corresponding interconnections are subject to and will go through the appropriate AT&T firewall. If AT&T believes that a connection is insecure, a logical or physical audit may occur. AT&T will gather information relating to Customer's access to AT&T's mobile network, systems, or applications. This information may be collected, retained, and analyzed to identify potential security risks. Customer understands and agrees that AT&T may in its reasonable judgment suspend or terminate without notice the Service **if its construct or usage is determined to pose a security concern for AT&T and/or its customers**.

5.6. Customer Contact; Test and Turn-Up of Custom solutions.

Customer must designate a customer representative ("Customer Contact") with responsibility for assisting AT&T, during a mutually agreeable time and upon reasonable prior notice from AT&T, in the testing and deployment of the Custom Service (the "Test and Turn-Up"). Customer Contact's responsibilities with regard to Test and Turn- Up include but are not limited to the following: (a) validating that the custom Service APN or DNN works properly and permits access to Customer's network and the Host Application(s), and (b) authorizing the final deployment of the Service APN or DNN. The Service may not be operational until Test and Turn-up is complete.

5.7. Changes to service. Once a Custom Service APN or DNN has been deployed in the AT&T mobile network for use by Customer, changes to the Service configuration may be requested by Customer by contacting its respective AT&T account manager. Changes are subject to a Change Order professional service fee as described in this Attachment.

5.8. Decommissioning of Service. Upon termination or suspension of the Service, for any reason, Customer must disable service on their mobile devices, end points, server(s) and/or Host Applications by removing the configuration parameters that enable the Service connection.

5.9. Terms and Conditions for Public IP Addresses. The services provided under this Attachment are subject to the following terms and conditions:

5.9.1. IP Address Best Practices. Customer must maintain end point software and hardware updates, utilize strong passwords, implement least privileged firewall rules, and audit usage.

5.9.2. Public IP Address Security Risks. An AT&T public Internet Protocol (IP) address is a static or dynamic IP address number assigned to an eligible AT&T mobile device that is visible to the open Internet without any masking or translation. If required by the design, a mobile device assigned to a public IP address can access, and be exposed to, the public internet via the Service. Devices with public IP addresses are vulnerable to data mining and increased security risks, including malware and DDoS attacks.

5.9.3. Firewall rules. Custom solutions are designed to allow establishing the least privileged set(s) of firewall rules for the Service design and provisioning that afford only the necessary data routes to operate between the mobile device, Service and the Host Applications**.** In the event

Customer does not have or is unable to produce a valid list of least privileged IP Ranges for the Service firewall configuration, AT&T will offer an optional best effort set of firewall rules (EPL) to limit mobile terminated activity over the Service being used. Shared solutions will utilize the AT&T EPL unless specified otherwise.

5.9.4. Firewall Expectations. The increased risks associated with Public IP addressing and mobile termination necessitates the utilization of firewall rules with the fewest necessary IP ranges and ports defined to afford only required connections over the Service. Requests to abstain from using firewall rules in any Service solution is not recommended, and Customer assumes all risk and is fully responsible for the security and financial impacts associated as described in §5.9.11.

5.9.5. SIM Activation. The SIM on a mobile device must be activated before the device can be assigned to a public IP address.

5.9.6. Limited Resource. Public IP addresses are a limited resource. Accordingly, AT&T reserves the right, in its sole discretion, to limit the number of public IP addresses available to Customer and/or deny any requests for public IP addresses.

5.9.7. No Ownership Right. Customer does not own, nor has any property interest in, an AT&T provided public static or dynamic IP address - assigned to any mobile device. AT&T shall have an unrestricted right to reclaim and/or reassign any public static or dynamic IP address if the SIM on an associated mobile device is deactivated or if the public static IP address remains unused for 12 months.

5.9.8. No Usage Alerts. Due to systems limitations, Customer device(s) assigned to a public static IP address will not receive data usage alerts. Customer is solely responsible for tracking all data usage on mobile devices assigned to a public static IP address and remains responsible for any data overages.

5.9.9. Modification. AT&T reserves the right to modify or discontinue the provisioning of public static IP addresses without prior notice to Customer.

5.9.10. Customer support to AT&T. Customer shall provide any information and assistance as may be requested by AT&T related to the set-up, maintenance, and termination of any public static IP addresses.

5.9.11. Public IP Responsibility and Liability. In all cases, Customer assumes all responsibility for the security of its mobile devices assigned with a public IP address, including compliance with any security recommendations made by the device manufacturer as well as the following security requirements established by AT&T: (i) All devices assigned to a public IP address must be able to accept and implement software and security upgrades over-the–air. (ii) Customer must change all default passwords and UUIDs for all devices assigned to the public IP address after initial provisioning. (iii) All unnecessary services and network protocols (e.g., Telnet SSH, etc.) must be disabled. (iv) Customer is responsible for continuously monitoring the security of its devices and must remove any infected or compromised devices from the AT&T network immediately. In the event that AT&T determines in its reasonable judgment that one or more of Customer's devices may be infected or compromised, AT&T shall have the right, but not the obligation, to disconnect the device from the AT&T network with or without notice to Customer. (v) Customer is hereby advised that devices using mobile terminate on a Public IP address may increase usage substantially, cause unanticipated overage charges, cause damage to connected systems, software or hardware and have financial impacts to Customer. ALL SUCH CHARGES AND DAMAGES ARE THE RESPONSIBILITY OF CUSTOMER AND AT&T SHALL NOT BE REQUIRED TO REIMBURSE, COVER COSTS, ISSUE ANY CREDITS OR REMOVE ANY SUCH CHARGES FROM CUSTOMER'S INVOICE.

6.0 AT&T RESPONSIBILITIES

6.1. AT&T will establish and facilitate the Service(s) in accordance with the terms and conditions of this Attachment. Once Customer requests Custom Service(s) from AT&T, AT&T will commence the process to consult, design, build, test and deploy the Service(s). AT&T will notify Customer in writing of the corresponding timelines for each stage, including collaborative stages such as design and Test & Turn-Up.

6.2. For Custom AT&T VPN solutions, as part of the service order, AT&T will establish and facilitate the MPLS Interconnect(s) that will connect Customer's AT&T VPN to AT&T's mobile network in accordance with the terms and conditions of this Attachment.

7.0 SUPPORT

AT&T will provide Customer Custom Service support through a toll-free number to the applicable Customer Care representative 24 hours per day, 7 days a week.

8.0 PRICING

Listed charges are standard rates for professional services and product charges only. The listed pricing does not include prerequisite and separately obtained: AT&T qualified device(s) with corresponding AT&T Mobility SIM(s) and mobile service on AT&T rate plan(s). Service pricing should be confirmed with an AT&T representative or Customer's account manager to ensure it corresponds with Customer's business needs. Products and pricing may vary between PMC and PMC 5G solutions and are described accordingly by Service name.

8.1. Set-Up Charges - Professional Services - Non-Recurring, one-time Charges (NRC) are determined and identified in the design confirmation communication from AT&T to Customer. Invoiced amounts are due once design and associated Charges are approved by Customer and invoiced by AT&T at completion of Test and Turn-Up.

PMC Set-Up Charges	
PMC Set-Up Type	**NRC**
Custom Internet or Intranet APN Design, build and provisioning	$500.00
APN Change Order	$500.00
APN Design and Build Prioritization	$250.00
Public IP Address Pool(s) Setup/Change Fee	$500.00
Transport Setup (MPLS and/or IPsec) per APB	$1,995.00

PMC5G Set-Up Charges	
PMC 5G Set-Up Type	**NRC**
Custom Internet Type DNN Design, build and provisioning	$1,000.00
Custom Intranet Type DNN Design, build and provisioning	$2,500.00
DNN Design and Build Prioritization	$500.00
DNN Change Order	$500.00

8.2. Monthly CTN PMC Service Charges – Per Customer Telephone Number (CTN) charge for access, usage, and maintenance of the Service. Invoicing commences when applied to CTN.

PMC Monthly Charges by CTN	
Custom APN	$5.00
Shared APN	$6.00
Public Static IP Address *(Legacy solutions only. Replaced by IP Pools)*	$3.00

PMC 5G Monthly Charges by CTN	
Custom DNN	$5.00
Shared DNN – Includes 1 Public Static or Dynamic IP address	$10.00

8.3. Monthly Service Charges by Account. These Charges are at the account level, sperate from any CTNs on the account or CTNs using the Service. Charges begin at the completion of Test and Turn Up of the Service build or change order. These are only applicable to the Service on the PMC platform.

PMC Monthly Charges for MPLS Logical Connection by Bandwidth				
Bandwidth	**MRC**		**Bandwidth**	**MRC**
2 Mbps	$250.00		100 Mbps	$1,400.00
5 Mbps	$437.00		250 Mbps	$1,600.00
10 Mbps	$610.00		500 Mbps	$1,950.00

PMC Monthly Charges for MPLS Logical Connection by Bandwidth			
Bandwidth	**MRC**	**Bandwidth**	**MRC**
20 Mbps	$750.00	1000 Mbps	$3,000.00
50 Mbps	$1,000.00	2000 Mbps	$9,000.00

PMC Monthly Charges for AT&T VPN Access by Bandwidth			
Bandwidth	**MRC**	**Bandwidth**	**MRC**
512 kbps	$166.00	70 Mbps	$2,124.00
1 Mbps	$193.00	80 Mbps	$2,287.00
1.5 Mbps	$195.00	90 Mbps	$2,494.00
2 Mbps	$250.00	100 Mbps	$2,683.00
3 Mbps	$310.00	150 Mbps	$3,983.00
4 Mbps	$351.00	200 Mbps	$5,140.00
5 Mbps	$437.00	250 Mbps	$6,047.00
6 Mbps	$463.00	300 Mbps	$6,660.00
7 Mbps	$499.00	400 Mbps	$7,886.00
8 Mbps	$540.00	450 Mbps	$8,499.00
9 Mbps	$580.00	500 Mbps	$9,112.00
10 Mbps	$610.00	600 Mbps	$10,336.00
20 Mbps	$839.00	700 Mbps	$13,029.00
30 Mbps	$1,114.00	800 Mbps	$14,224.00
40 Mbps	$1,344.00	900 Mbps	$15,497.00
50 Mbps	$1,605.00	1000 Mbps	$16,723.00
60 Mbps	$1,873.00		

8.4. Public IP Charges. For Custom Service configurations designed to use IP Pools for public IP addresses, either dynamic or static, the following rates apply and are charged at the account level monthly, separate from active subscriber lines. Pools may be stacked to meet or exceed the total IP addresses required by the Service design. Invoicing commences at completion of Test and Turn-Up of the Service build or Change Order.

Public IP Address Pools[1]	Assignable IP Addresses[2]	MRC Per Pool
/30 POOL	2	$6.00
/29 POOL	6	$18.00
/28 POOL	14	$42.00
/27 POOL	30	$90.00
/26 POOL	62	$186.00
/25 POOL	126	$378.00
/24 POOL	254	$762.00

Public IP Address Pools[1]	Assignable IP Addresses[2]	MRC Per Pool
/23 POOL	510	$1,530.00
/22 POOL	1,022	$3,066.00
/21 POOL	2,046	$6,138.00
/20 POOL	4,094	$12,282.00
/19 POOL	8,190	$24,570.00
/18 POOL	16,382	$49,146.00

1. For PMC 5G, each pool is dual stack supporting IPv4 and IPv6. PMC is either IPv4, IPv6 or dual stack based on APN design.
2. Each IP pool consists of two additional IP addresses. A HOST and BROADCAST IP address are part of each subnet mask containing the POOL. These are not assignable to a mobile end point.