APPENDIX OSS-CELLULAR/PCS NUMBER PORTABILITY

TABLE OF CONTENTS

APPENDIX OSS NUMBER PORTABILITY
(ACCESS TO OPERATIONS SUPPORT SYSTEMS FUNCTIONS)

1. INTRODUCTION

1.1 This Appendix sets forth terms and conditions for access to Operations Support Systems (OSS) "functions" to "WSP" (Wireless Service Provider), for pre-ordering, ordering, and provisioning of Wireline to Wireless Number Portability (WNP) consistent with FCC Order #95-116 and related Orders. The OSS interfaces to be used by the WSP for WNP are the same interfaces that AT&T-13STATE provides to Competitive Local Exchange Carriers ("CLECs") for Wireline Local Number Portability (LNP). AT&T-13STATE is in the process of making necessary LSR enhancements to enable acceptance, recognition, and processing of Wireline to Wireless Number Portability requests. These enhancements will be the subject of a future OSS release consistent with the industry obligations for WSPs to offer WNP capabilities per the FCC Order #95-116. Following this release, AT&T-13STATE will provide a mechanized means for placing Wireline to Wireless Number Portability requests. The interfaces described herein have certain features which are not related to number portability, but which are inherently available via the interface. Such non-LNP features shall not be accessed nor used by, through, or on behalf of WSP pursuant to this Appendix. WSP hereby warrants and represents that it will not access such non-LNP features. The WSP is authorized by this Appendix to use only the Pre-Order, Ordering, and Provisioning functions identified herein and only for essential number portability functions.

1.2 AT&T Inc. (AT&T) means the holding company which directly or indirectly owns the following ILECs: Illinois Bell Telephone Company d/b/a AT&T Illinois, Indiana Bell Telephone Company Incorporated d/b/a AT&T Indiana, Michigan Bell Telephone Company d/b/a AT&T Michigan, Nevada Bell Telephone Company d/b/a AT&T Nevada, The Ohio Bell Telephone Company d/b/a AT&T Ohio, Pacific Bell Telephone Company d/b/a AT&T California, The Southern New England Telephone Company d/b/a AT&T Connecticut, Southwestern Bell Telephone, L.P. d/b/a AT&T Arkansas, AT&T Kansas, AT&T Missouri, AT&T Oklahoma and/or AT&T Texas and/or Wisconsin Bell, Inc. d/b/a AT&T Wisconsin.

1.3 AT&T-2STATE - As used herein, AT&T-2STATE means AT&T CALIFORNIA and AT&T NEVADA, the applicable AT&T-owned ILEC(s) doing business in California and Nevada.

1.4 AT&T-7STATE - As used herein, AT&T-7STATE means AT&T SOUTHWEST REGION 5-STATE, AT&T CALIFORNIA and AT&T NEVADA, the applicable AT&T-owned ILEC(s) doing business in Arkansas, California, Kansas, Missouri, Nevada, Oklahoma and Texas.

1.5 AT&T-8STATE - As used herein, AT&T-8STATE means AT&T SOUTHWEST REGION 5-STATE, AT&T CALIFORNIA, AT&T NEVADA, and AT&T AT&T CONNECTICUT the applicable AT&T-owned ILEC(s) doing business in Arkansas, California, Connecticut, Kansas, Missouri, Nevada, Oklahoma and Texas.

1.6 AT&T-12STATE - As used herein, AT&T-12STATE means AT&T SOUTHWEST REGION 5-STATE, AT&T SOUTHWEST REGION 5-STATE and AT&T-2STATE the applicable AT&T-owned ILEC(s) doing business in Arkansas, California, Illinois, Indiana, Kansas, Michigan, Missouri, Nevada, Ohio, Oklahoma, Texas and Wisconsin.

1.7 AT&T-13STATE - As used herein, AT&T-13STATE means AT&T SOUTHWEST REGION 5-STATE, AT&T SOUTHWEST REGION 5-STATE, AT&T-2STATE and AT&T CONNECTICUT the applicable AT&T-owned ILEC(s) doing business in Arkansas, California, Connecticut, Illinois, Indiana, Kansas, Michigan, Missouri, Nevada, Ohio, Oklahoma, Texas and Wisconsin.

1.8 AT&T CALIFORNIA - As used herein, AT&T CALIFORNIA means Pacific Bell Telephone Company d/b/a AT&T California, the applicable AT&T-owned ILEC doing business in California.

1.9 AT&T CONNECTICUT - As used herein, AT&T CONNECTICUT means The Southern New England Telephone Company d/b/a AT&T Connecticut, the applicable above listed ILEC doing business in Connecticut.

1.10 AT&T MIDWEST REGION 5-STATE - As used herein, AT&T MIDWEST REGION 5-STATE means Illinois Bell Telephone Company d/b/a AT&T Illinois, Indiana Bell Telephone Company Incorporated d/b/a AT&T Indiana, Michigan Bell Telephone Company d/b/a AT&T Michigan, The Ohio Bell Telephone Company d/b/a AT&T Ohio, and/or Wisconsin Bell, Inc. d/b/a AT&T Wisconsin, the applicable AT&T-owned ILEC(s) doing business in Illinois, Indiana, Michigan, Ohio and Wisconsin.

1.11 AT&T NEVADA - As used herein, AT&T NEVADA means Nevada Bell Telephone Company d/b/a AT&T Nevada, the applicable AT&T-owned ILEC doing business in Nevada.

1.12 AT&T SOUTHWEST REGION 5-STATE - As used herein, AT&T SOUTHWEST REGION 5-STATE means Southwestern Bell Telephone, L.P. d/b/a AT&T Arkansas, AT&T Kansas, AT&T Missouri, AT&T Oklahoma and/or AT&T Texas the applicable above listed ILEC(s) doing business in Arkansas, Kansas, Missouri, Oklahoma and Texas.

2. DEFINITIONS

2.1 "LSC" means (i) the Local Service Center (LSC) for AT&T-10STATE and AT&T-2STATE; (ii) Local Exchange Carrier Center (LECC) for AT&T CONNECTICUT.

2.2 "WSP" or Wireless Service Provider means a provider of cellular, broadband Personal Communications Services ('PCS')or SMR CMRS.

2.3 "Service Bureau Provider" - For purposes of this Agreement, Service Bureau Provider (SBP) is a company which has been engaged by a Wireless Service Provider (WSP) to act on its behalf to access AT&T-13STATE's OSS application-to-application interfaces via a dedicated connection for the purpose of transporting multiple WSP's Wireless Number Portability (WNP) transactions.

3. GENERAL CONDITIONS

3.1 The Parties agree that electronic order processing is more efficient than manual order processing. During implementation of this Wireless Interconnection Agreement the WSP will migrate to electronic processing within six (6) months from the Effective Date of this Agreement. Electronic processing is available via AT&T-13STATE's Application to Application Interface or via AT&T-13STATE's Graphical User Interface (GUI). After the six-month (6) transition period, WSP will no longer submit Wireless Number Portability orders manually and AT&T-13STATE shall not be required to accept and process manual orders, except when the electronic interface is unavailable for a substantial period of time.

3.2 Proper Use of OSS interfaces:

3.2.1 For AT&T-13STATE, WSP agrees to utilize AT&T-13STATE electronic interfaces, as described herein, solely for the purposes of pre-order and order activity necessary for Wireless Number Portability. In addition, WSP agrees that such use will comply with AT&T-13STATE's Data Connection Security Requirements as identified in Section 8 of this Appendix. Failure to comply with such security guidelines or misuse of OSS interfaces may result in forfeiture of electronic access to OSS functionality. In addition, WSP shall be responsible for and indemnifies AT&T-13STATE against any cost, expense or liability relating to any unauthorized entry or access into, or use or manipulation of AT&T-13STATE's OSS from WSP systems, workstations or terminals or by WSP employees, agents, or any third party gaining access through information and/or facilities obtained from or utilized by WSP and shall pay AT&T-13STATE for any and all damages caused by such unauthorized entry.

3.3 Within AT&T-13STATE regions, WSP's access to pre-order functions described in 4.2.1 will only be utilized to view Customer Proprietary Network Information (CPNI) of another carrier's End User where WSP has obtained an authorization for release of CPNI from the End User and has obtained an authorization to become the End User's WSP.

3.3.1 In AT&T-13STATE regions, WSP must maintain records of individual customers' authorizations in accordance with section 3.3 above, and release of CPNI which adhere to all requirements of state and federal law, as applicable.

3.3.2 This section applies to AT&T CALIFORNIA ONLY. For consumer End Users, prior to accessing such information, WSP shall, on its own behalf and on behalf of AT&T CALIFORNIA, comply with all applicable requirements of Section 2891 of the California Public Utilities Code and 47 USC 222 (and implementing FCC decisions thereunder), and, where accessing such information via an electronic interface, WSP shall have obtained an authorization to become the End User's local service provider. Accessing such information by WSP shall constitute certification that WSP is in compliance with applicable requirements of Section 2891 and Section 222 (and implementing FCC decisions thereunder) and has complied with the prior sentence. WSP shall receive and retain such information in conformance with the requirements of 47 USC 222 (and implementing FCC decisions thereunder). WSP agrees to indemnify, defend and hold harmless AT&T CALIFORNIA against any claim made by a consumer End User or governmental entity against AT&T CALIFORNIA or WSP under Section 2891 or Section 222 (and implementing FCC decisions thereunder) or for any breach by WSP of this section.

3.3.3 Throughout AT&T-13STATE region, WSP is solely responsible for determining whether proper authorization has been obtained and holds AT&T-13STATE harmless from any loss on account of WSP's failure to obtain proper CPNI consent from an End User.

3.4 By utilizing electronic interfaces to access OSS functions, WSP agrees to perform accurate and correct ordering such that no other WSP, CLEC, IXC, ILEC, or any of their end users are harmed by the WSP's preorder or order use of AT&T-13STATE's OSS. WSP is also responsible for all actions of its employees using any of AT&T-13STATE's OSS systems. As such, WSP agrees to accept and pay all reasonable costs or expenses, including labor costs, incurred by AT&T-13STATE caused by any and all inaccurate ordering or usage of the OSS, if such costs are not already recovered through other charges assessed by AT&T-13STATE to WSP. In addition, WSP agrees to indemnify and hold AT&T-13STATE harmless against any claim made by an End User of WSP or other third parties against AT&T-13STATE caused by or related to WSP's use of any AT&T-13STATE OSS.

3.5 In the event AT&T-13STATE has good cause to believe that WSP has used AT&T-13STATE OSS in a way that conflicts with this Agreement or Applicable Law, AT&T-13STATE shall give WSP written notice describing the alleged misuse ("Notice of Misuse"). WSP shall immediately refrain from the alleged misuse until such time that WSP responds in writing to AT&T-13STATE's Notice of Misuse, which shall be provided to AT&T-13STATE within twenty (20) days after receipt of the Notice of Misuse. In the event WSP agrees with AT&T-13STATE's allegation of misuse, WSP shall refrain from the alleged misuse during the term of this Agreement.

3.6 In the event WSP does not agree that WSP's use of AT&T-13STATE OSS is inconsistent with this Agreement or Applicable Law, then the parties agree to the following steps:

3.6.1 If such misuse involves improper access of pre-order applications to obtain CPNI in violation of this Agreement, Applicable Law, or involves a violation of the security guidelines contained herein, or negatively affects another OSS user's ability to use OSS, WSP shall continue to refrain from using the particular OSS functionality in the manner alleged by AT&T-13STATE to be improper, until WSP has implemented a mutually agreeable remedy to the alleged misuse.

3.6.2 To remedy the misuse for the balance of the agreement, Parties will work together as necessary to mutually determine a permanent resolution for the balance of the term of the agreement.

3.7 In order to determine whether WSP has engaged in the alleged misuse described in the Notice of Misuse, and for good cause shown, AT&T-13STATE shall have the right to conduct an audit of WSP's use of the AT&T-13STATE OSS. Such audit shall be limited to auditing those aspects of WSP's use of the AT&T-13STATE OSS that relate to AT&T-13STATE's allegation of misuse as set forth in the Notice of Misuse. AT&T-13STATE shall give ten (10) days advance written notice of its intent to audit WSP ("Audit Notice")

under this Section 3.7, and shall identify the type of information needed for the audit. Such Audit Notice may not precede AT&T-13STATE's Notice of Misuse. Within a reasonable time following the Audit Notice, but no less than fourteen (14) days after the date of the notice (unless otherwise agreed by the Parties), WSP shall provide AT&T-13STATE with access to the requested information in any reasonably requested format, at an appropriate WSP location, unless otherwise agreed to by the Parties. The audit shall be at AT&T-13STATE's expense. All information obtained through such an audit shall be deemed proprietary and/or confidential and subject to confidential treatment without necessity for marking such information confidential. AT&T-13STATE agrees that it shall only use employees or outside parties to conduct the audit who do not have marketing, strategic analysis, competitive assessment or similar responsibilities within AT&T-13STATE.

3.8 AT&T-13STATE will and WSP may participate in the Order and Billing Forum (OBF) and the Telecommunications Industry Forum (TCIF) to establish and conform to uniform industry guidelines for electronic interfaces for pre-order, ordering, and provisioning. Neither Party waives its rights as participants in such forums or in the implementation of the guidelines. To achieve system functionality as quickly as possible, the Parties acknowledge that AT&T-13STATE may deploy interfaces with requirements developed in advance of industry guidelines. Thus, subsequent modifications may be necessary to comply with emerging guidelines. WSP and AT&T-13STATE are individually responsible for evaluating the risk of developing their respective systems in advance of guidelines and agree to support their own system modifications to comply with new requirements. In addition, AT&T-13STATE has the right to define Local Service Request (LSR) Usage requirements according to the General Section 1.0, paragraph 1.4 of the practices in the OBF Local Service Ordering Guidelines (LSOG), which states: "Options described in this practice may not be applicable to individual providers tariffs; therefore, use of either the field or valid entries within the field is based on the providers tariffs/practices."

3.8.1 Due to enhancements and on-going development of access to AT&T-13STATE's OSS functions, certain interfaces described in this Appendix may be modified, temporarily unavailable or may be phased out after execution of this Appendix.

3.8.2 WSP is responsible for obtaining operating system software and hardware to access AT&T-13STATE OSS functions as specified in: "CLEC Hardware/Software Requirements for Access of AT&T Uniform OSS Applications".

4. PRE-ORDERING

4.1 AT&T-13STATE will provide real time access to pre-order functions necessary to support WSP ordering of Wireless Number Portability (WNP). The following lists represent pre-order functions that are available to WSP so that WSP order requests may be created to comply with AT&T-13STATE region-specific ordering requirements.

4.2 Pre-ordering functions for Wireless Number Portability include:

4.2.1 Customer Service Information - CSI Inquiry:
Access to AT&T-13STATE retail or resold CPNI and account information for pre-ordering provides access to the Customer Service Record (CSR) containing the following information: billing name, billing address, service address, service and feature subscription, and long distance carrier identity. The CSR contains additional information, provided however, the WSP may access CSR information for the sole purpose of facilitating Wireless Number Portability. Additionally, WSP agrees that WSP will not access the information specified in this subsection until after it has the End User's request that their Local Service Provider be changed to WSP, and an End User authorization for release of CPNI complies with conditions as described in section 3.3 of this Appendix.

4.2.2 Address Validation Inquiry:
AT&T-13STATE provides address validation function.

4.3 Electronic Access to Pre-Order Functions:

4.3.1 AT&T-13STATE Pre-order Interface Availability: AT&T-13STATE will provide WSP access to the following interfaces:

4.3.1.1 An industry standard EDI/CORBA Pre-ordering Gateway is provided by AT&T-13STATE. This pre-ordering gateway supports two structural protocols, EDI and CORBA, as recommended by the technical industry committees. EDI/CORBA is application-to-application interface that can be integrated with the WSP's own negotiation system. EDI/CORBA is an industry-wide standard pre-ordering interface.

4.3.1.2 Enhanced Verigate is a Uniform GUI interface developed by AT&T-13STATE that provides access to pre-ordering functions. Enhanced Verigate is accessible via Web Toolbar.

5. ORDERING

5.1 AT&T-13STATE provides access to the same OSS interfaces, which support CLEC ordering of Local Number Portability, and thus these same AT&T-13STATE interfaces will be made available to Wireless Service Providers (WSPs) for the sole purpose of ordering a Wireless Number Portability (WNP). Any attempts to use other ordering functionality of the OSS interfaces for purposes other than WNP, may result in forfeiture of electronic access to OSS. Consistent with OBF, the industry mechanism for ordering WNP is via the Local Service Request (LSR). The AT&T-13STATE LSOR (Local Service Order Requirements) document will be updated with the conditions for ordering Wireline to Wireless Number Portability (WNP). When ordering WNP, the WSP will format the service request, in accordance with the AT&T-13STATE LSOR. AT&T-13STATE will provide WSP access to one or more of the following interfaces:

5.2 WNP Ordering Interface Availability:

5.2.1 AT&T-13STATE makes available to WSP an Electronic Data Interchange (EDI) interface for transmission of the Local Service Request (LSR) for the ordering of wireline to wireless number portability (WNP) as defined by the OBF and via EDI mapping as defined by TCIF. In ordering of WNP, the WSP and AT&T-13STATE will utilize industry guidelines developed by OBF and TCIF to transmit EDI data.

5.2.2 For AT&T-13STATE, WebLEX is the Uniform GUI interface that provides access to the ordering functions for WNP.

6. PROVISIONING

6.1 Provisioning for WNP in AT&T-13STATE: AT&T-13STATE will provision WNP as detailed in the WSP's LSR. Access to status on such WNP orders, consistent with the Uniform Plan of Record, will be provided via the following electronic interfaces:

6.1.1 For AT&T-13STATE, Order Status and Provisioning Order Status functionality is provided via the Uniform GUI interface, Enhanced Verigate, which will allow WSP to check WNP service order status.

6.1.2 Electronic Data Interchange (EDI) is the Uniform App to App interface that AT&T-13STATE uses to return Order Status and Provisioning Order Status for WNP.

7. REMOTE ACCESS FACILITY

7.1 WSP must access OSS interfaces via AT&T-13STATE's CLEC Remote Access Facility. For the AT&T SOUTHWEST REGION 5-STATE region, the LRAF located in Dallas, TX will be used. The PRAF in Fairfield, CA handles the AT&T-2STATE regions. The ARAF, located in Chicago, IL, serves AT&T MIDWEST REGION 5-STATE and the SRAF in New Haven, CT, handles the AT&T CONNECTICUT region. Connection to these Remote Access Facilities will be established via a "port" either through dial-up or direct connection as described in Section 7.2. WSP may utilize a port to access AT&T-13STATE OSS interfaces to perform the supported functions in any AT&T-13STATE where WSP has executed an Appendix OSS.

7.2 For AT&T-13STATE, WSP may use three types of access: Switched, Private Line, and Frame Relay. For Private Line and Frame Relay "Direct Connections," WSP shall provide its own router, circuit, and two Channel Service Units/Data Service Units (CSU/DSU). The demarcation point shall be the router interface at the LRAF, PRAF, ARAF, or SRAF. Switched Access "Dial-up Connections" require WSP to provide its own modems and connection to the AT&T SOUTHWEST REGION 5-STATE LRAF, AT&T CALIFORNIA PRAF, AT&T MIDWEST REGION 5-STATE ARAF, and AT&T CONNECTICUT SRAF. WSP shall pay the cost of the call if Switched Access is used.

7.3 For AT&T-13STATE, WSP shall use TCP/IP to access AT&T-13STATE OSS via the LRAF, ARAF, SRAF, and the PRAF. In addition, each WSP shall have one valid Internet Protocol (IP) network address per region. WSP shall maintain a user-id / password unique to each individual for accessing an AT&T-13STATE's OSS on WSP's behalf. WSP shall provide estimates regarding its volume of transactions, number of concurrent users, desired number of private line or dial-up (switched) connections, and length of a typical session.

7.4 For AT&T-13STATE, WSP shall attend and participate in implementation meetings to discuss WSP LRAF/PRAF/ARAF/SRAF access plans in detail and schedule testing of such connections.

8. DATA CONNECTION SECURITY REQUIREMENTS

8.1 WSP agrees that interconnection of WSP data facilities with AT&T-13STATE data facilities for access to the applicable OSS for the purposes described herein will be in compliance with AT&T-13STATE's Competitive Local Exchange Carrier (CLEC) Operations Support System Interconnection Procedures document current at the time of initial connection to a RAF. The following additional terms in this Section 8 govern direct and dial up connections between WSP and the PRAF, LRAF, ARAF and SRAF for access to OSS Interfaces.

8.2 Joint Security Requirements

8.2.1 Both Parties will maintain accurate and auditable records that monitor user authentication and machine integrity and confidentiality (e.g., password assignment and aging, chronological logs configured, system accounting data, etc.).

8.2.2 Both Parties shall maintain accurate and complete records detailing the individual data connections and systems to which they have granted the other Party access or interface privileges. These records will include, but are not limited to, user ID assignment, user request records, system configuration, time limits of user access or system interfaces. These records should be kept until the termination of this Agreement or the termination of the requested access by the identified individual. Either Party may initiate a compliance review of the connection records to verify that only the agreed to connections are in place and that the connection records are accurate.

8.2.3 Each Party shall notify the other party immediately, upon termination of employment of an individual user with approved access to the other Party's network.

8.2.4 Both Parties shall use an industry standard virus detection software program at all times. The Parties shall immediately advise each other by telephone upon actual knowledge that a virus or other malicious code has been transmitted to the other Party.

8.2.5 All physical access to equipment and services required to transmit data will be in secured locations. Verification of authorization will be required for access to all such secured locations. A secured location is where walls and doors are constructed and arranged to serve as barriers and to provide uniform protection for all equipment used in the data connections which are made as a result of the user's access to either the WSP or AT&T-13STATE network. At a minimum, this shall include: access doors equipped with card reader control or an equivalent authentication procedure and/or device, and egress doors which generate a real-time alarm when opened and which are equipped with tamper resistant and panic hardware as required to meet building and safety standards.

8.2.6 Both Parties shall maintain accurate and complete records on the card access system or lock and key administration to the rooms housing the equipment utilized to make the connection(s) to the

other Party's network. These records will include management of card or key issue, activation or distribution and deactivation.

8.3 Additional Responsibilities of Both Parties

8.3.1 Modem/DSU Maintenance And Use Policy: To the extent the access provided hereunder involves the support and maintenance of WSP equipment on AT&T-13STATE's premises, such maintenance will be provided under the terms of the Competitive Local Exchange Carrier (WSP) Operations Support System Interconnection Procedures document cited above.

8.3.2 Monitoring: Each Party will monitor its own network relating to any user's access to the Party's networks, processing systems, and applications. This information may be collected, retained, and analyzed to identify potential security risks without notice. This information may include, but is not limited to, trace files, statistics, network addresses, and the actual data or screens accessed or transferred.

8.3.3 Each Party shall notify the other Party's security organization immediately upon initial discovery of actual or suspected unauthorized access to, misuse of, or other "at risk" conditions regarding the identified data facilities or information. Each Party shall provide a specified point of contact. If either Party suspects unauthorized or inappropriate access, the Parties shall work together to isolate and resolve the problem.

8.3.4 In the event that one Party identifies inconsistencies or lapses in the other Party's adherence to the security provisions described herein, or a discrepancy is found, documented, and delivered to the non-complying Party, a corrective action plan to address the identified vulnerabilities must be provided by the non-complying Party within thirty (30) calendar days of the date of the identified inconsistency. The corrective action plan must identify what will be done, the Party accountable/responsible, and the proposed compliance date. The non-complying Party must provide periodic status reports (minimally monthly) to the other Party's security organization on the implementation of the corrective action plan in order to track the work to completion.

8.3.5 In the event there are technological constraints or situations where either Party's corporate security requirements cannot be met, the Parties will institute mutually agreed upon alternative security controls and safeguards to mitigate risks.

8.3.6 All network-related problems will be managed to resolution by the respective organizations, WSP or AT&T-13STATE, as appropriate to the ownership of a failed component. As necessary, WSP and AT&T-13STATE will work together to resolve problems where the responsibility of either Party is not easily identified.

8.4 Information Security Policies And Guidelines For Access To Computers, Networks and Information By Non-Employee Personnel:

8.4.1 Information security policies and guidelines are designed to protect the integrity, confidentiality and availability of computer, networks and information resources. Subsections 8.5 - 8.11 summarize the general policies and principles for individuals who are not employees of the Party that provides the computer, network or information, but have authorized access to that Party's systems, networks or information. Questions should be referred to WSP or AT&T-13STATE, respectively, as the providers of the computer, network or information in question.

8.4.2 It is each Party's responsibility to notify its employees, contractors and vendors who will have access to the other Party's network, on the proper security responsibilities identified within this Attachment. Adherence to these policies is a requirement for continued access to the other Party's systems, networks or information. Exceptions to the policies must be requested in writing and approved by the other Party's information security organization.

8.5 General Policies

8.5.1 Each Party's resources are for approved business purposes only.

8.5.2 Each Party may exercise at any time its right to inspect, record, and/or remove all information contained in its systems, and take appropriate action should unauthorized or improper usage be discovered.

8.5.3 Individuals will only be given access to resources that they are authorized to receive and which they need to perform their job duties. Users must not attempt to access resources for which they are not authorized.

8.5.4 Authorized users must not develop, copy or use any program or code which circumvents or bypasses system security or privilege mechanism or distorts accountability or audit mechanisms.

8.5.5 Actual or suspected unauthorized access events must be reported immediately to each Party's security organization or to an alternate contact identified by that Party. Each Party shall provide its respective security contact information to the other.

8.6 User Identification

8.6.1 Access to each Party's corporate resources will be based on identifying and authenticating individual users in order to maintain clear and personal accountability for each user's actions.

8.6.2 User identification shall be accomplished by the assignment of a unique, permanent user id, and each user id shall have an associated identification number for security purposes.

8.6.3 User ids will be revalidated on a monthly basis.

8.7 User Authentication

8.7.1 Users will usually be authenticated by use of a password. Strong authentication methods (e.g. one-time passwords, digital signatures, etc.) may be required in the future.

8.7.2 Passwords must not be stored in script files.

8.7.3 Passwords must be entered by the user in real time.

8.7.4 Passwords must be at least 6-8 characters in length, not blank or a repeat of the user id; contain at least one letter, and at least one number or special character must be in a position other than the first or last one. This format will ensure that the password is hard to guess. Most systems are capable of being configured to automatically enforce these requirements. Where a system does not mechanically require this format, the users must manually follow the format.

8.7.5 Systems will require users to change their passwords regularly (usually every 31 days).

8.7.6 Systems are to be configured to prevent users from reusing the same password for 6 changes/months.

8.7.7 Personal passwords must not be shared. A user who has shared his password is responsible for any use made of the password.

8.8 Access and Session Control

8.8.1 Destination restrictions will be enforced at remote access facilities used for access to OSS Interfaces. These connections must be approved by each Party's corporate security organization.

8.8.2 Terminals or other input devices must not be left unattended while they may be used for system access. Upon completion of each work session, terminals or workstations must be properly logged off.

8.9 User Authorization

8.9.1 On the destination system, users are granted access to specific resources (e.g. databases, files, transactions, etc.). These permissions will usually be defined for an individual user (or user group) when a user id is approved for access to the system.

8.10 Software And Data Integrity

8.10.1 Each Party shall use a comparable degree of care to protect the other Party's software and data from unauthorized access, additions, changes and deletions as it uses to protect its own similar software and data. This may be accomplished by physical security at the work location and by access control software on the workstation.

8.10.2 Untrusted software or data shall be scanned for viruses before use on a Party's corporate facilities that can be accessed through the direct connection or dial up access to OSS interfaces.

8.10.3 Unauthorized use of copyrighted software is prohibited on each Party's corporate systems that can be access through the direct connection or dial up access to OSS Interfaces.

8.10.4 Proprietary software or information (whether electronic or paper) of a Party shall not be given by the other Party to unauthorized individuals. When it is no longer needed, each Party's proprietary software or information shall be returned by the other Party or disposed of securely. Paper copies shall be shredded. Electronic copies shall be overwritten or degaussed.

8.11 Monitoring And Audit

8.11.1 To deter unauthorized access events, a warning or no trespassing message will be displayed at the point of initial entry (i.e., network entry or applications with direct entry points). Each Party should have several approved versions of this message. Users should expect to see a warning message similar to this one:

"This is a (AT&T-13STATE or WSP) system restricted to Company official business and subject to being monitored at any time. Anyone using this system expressly consents to such monitoring and to any evidence of unauthorized access, use, or modification being used for criminal prosecution."

8.11.2 After successful authentication, each session will display the last logon date/time and the number of unsuccessful logon attempts. The user is responsible for reporting discrepancies.

9. OPERATIONAL READINESS TEST (ORT) FOR ORDERING INTERFACES

9.1 Prior to live access to interface functionality, the Parties must conduct Operational Readiness Testing (ORT), which will allow for the testing of the systems, interfaces, and processes for the OSS functions. ORT will be completed in conformance with agreed upon processes and implementation dates.

10. OSS TRAINING COURSES

10.1 Prior to live system usage, WSP must complete user education classes for AT&T-13STATE-provided interfaces that affect the AT&T-13STATE network. Course descriptions and class schedules by region for WSPs will be available through their Wireless Account Manager. WSP Training schedules are subject to change, with class lengths varying. Classes are train-the-trainer format to enable WSP to devise its own course work for its own employees. Charges as specified below will apply for each class:

Training Rates	5 day class	4.5 day class	4 day class	3.5 day class	3 day class	2.5 day class	2 day class	1.5 day class	1 day class	1/2 day class
1 to 5 students	$4,050	$3,650	$3,240	$2,835	$2,430	$2,025	$1,620	$1,215	$810	$405
6 students	$4,860	$4,380	$3,890	$3,402	$2,915	$2,430	$1,945	$1,455	$970	$490
7 students	$5,670	$5,100	$4,535	$3,969	$3,400	$2,835	$2,270	$1,705	$1,135	$570
8 students	$6,480	$5,830	$5,185	$4,536	$3,890	$3,240	$2,590	$1,950	$1,300	$650
9 students	$7,290	$6,570	$5,830	$5,103	$4,375	$3,645	$2,915	$2,190	$1,460	$730
10 students	$8,100	$7,300	$6,480	$5,670	$4,860	$4,050	$3,240	$2,430	$1,620	$810
11 students	$8,910	$8,030	$7,130	$6,237	$5,345	$4,455	$3,565	$2,670	$1,780	$890
12 students	$9,720	$8,760	$7,780	$6,804	$5,830	$4,860	$3,890	$2,920	$1,945	$970

10.2 A separate agreement will be required as a commitment to pay for a specific number of WSP students in each class. WSP agrees that charges will be billed by AT&T-13STATE and WSP payment is due thirty

(30) days following the bill date. WSP agrees that personnel from other Wireless Service Providers may be scheduled into any class to fill any seats for which the WSP has not contracted. Class availability is first-come, first served with priority given to WSPs who have not yet attended the specific class.

10.3 Class dates will be based upon AT&T-13STATE availability and will be coordinated among WSP, the WSP's AT&T-13STATE Account Manager, and AT&T-13STATE Industry Markets CLEC Training Product Management.

10.4 WSP agrees to pay the cancellation fee of the full price noted in the separate agreement if WSP cancels scheduled classes less than two (2) weeks prior to the scheduled start date. WSP agrees to provide to AT&T-13STATE completed registration forms for each student no later than one week prior to the scheduled training class.

10.5 WSP agrees that WSP personnel attending classes are to utilize only training databases and training presented to them in class. Attempts to access any other AT&T-13STATE system are strictly prohibited.

10.6 WSP further agrees that training material, manuals and instructor guides can be duplicated only for internal use for the purpose of training employees to utilize the capabilities of AT&T-13STATE's OSS in accordance with this Appendix and shall be deemed "Proprietary Information" and subject to the terms, conditions and limitations of Section 20 of the General Terms and Conditions.

11. SERVICE BUREAU PROVIDER ARRANGEMENT FOR SHARED ACCESS TO OSS

11.1 AT&T-13STATE shall allow WSP to access the applicable AT&T-13 state OSS interfaces, as set forth in the WNP-OSS Appendix of the WSP's Wireless Interconnection Agreement, via a Service Bureau Provider under the following terms and conditions.

11.2 Notwithstanding any language in this Agreement regarding access to OSS to the contrary, WSP shall be permitted to access AT&T-13STATE OSS via a Service Bureau Provider as follows:

11.2.1 WSP shall be permitted to access AT&T-13STATE application-to-application OSS interfaces, via a Service Bureau Provider where WSP has entered into an agency relationship with such Service Bureau Provider, and the Service Bureau Provider has executed an Agreement with AT&T-13STATE to allow Service Bureau Provider to establish access to and use of AT&T-13STATE's OSS.

11.2.2 WSP's use of a Service Bureau Provider shall not relieve WSP of the obligation to abide by all terms and conditions of theirWNP-OSS Appendix of their Wireless Interconnection Agreement. WSP must ensure that its agent properly performs all OSS obligations of WSP under their Wireless Interconnection Agreement, which WSP delegates to Service Bureau Provider.

11.2.3 It shall be the obligation of WSP to provide notice in accordance with the notice provisions of the Terms and Conditions of their Wireless Interconnection Agreement whenever it established an agency relationship with a Service Bureau Provider or terminates such a relationship. AT&T-13STATE shall have a reasonable transition time to establish a connection to a Service Bureau Provider once WSP provides notice. Additionally, AT&T-13STATE shall have a reasonable transition period to terminate any such connection after notice from WSP that it has terminated its agency relationship with a Service Bureau Provider.