

***COMPETITIVE LOCAL EXCHANGE CARRIER***

***(CLEC)***

***OPERATIONS SUPPORT SYSTEM***

***INTERCONNECTION PROCEDURES***

**June 16, 2021**

**Version 7.1**

**AT&T SOUTHWEST**

**AT&T WEST**

**AT&T MIDWEST**

**AT&T SOUTHEAST**

Contents

[INTRODUCTION 4](#_Toc482878114)

[SUMMARY OF CHANGES 6](#_Toc482878115)

[IS CALL CENTER (ISCC) 10](#_Toc482878116)

[INTERCONNECTION REQUIREMENTS 11](#_Toc482878117)

[REMOTE ACCESS FACILITY (RAF) 12](#_Toc482878118)

[COORDINATION OF ACCESS REQUIREMENTS 13](#_Toc482878119)

[EXTERNAL BUSINESS PARTNER (EBIZ) PRIVATE LINE OR FRAME RELAY ACCESS 14](#_Toc482878120)

[Circuit Provisioning Activities 14](#_Toc482878121)

[VPN (IPSec VPN via Public Internet transport) 14](#_Toc482878122)

[MPLS, Point-to-Point Ethernet, Point-to-Point TDM or Frame Relay 14](#_Toc482878123)

[Network Provisioning Activities 15](#_Toc482878124)

[REMOTE ACCESS FACILITY (RAF) PRIVATE LINE OR FRAME RELAY ACCESS 16](#_Toc482878125)

[Circuit Provisioning Activities 16](#_Toc482878126)

[Network Provisioning Activities 16](#_Toc482878127)

[REMOTE ACCESS FACILITY (RAF) DIAL-UP ACCESS (ANALOG & DIGITAL) 17](#_Toc482878128)

[MISCELLANEOUS BULK DATA TRANSFER (SFG) ACCESS 18](#_Toc482878129)

[APPENDIX 1 19](#_Toc482878130)

[EXTERNAL BUSINESS PARTNER (EBIZ) Access Standards and Requirements 19](#_Toc482878131)

[VPN (IPSec VPN via Public Internet transport) Standards and Requirements 19](#_Toc482878132)

[MPLS, Point-to-Point Ethernet, Point-to-Point TDM or Frame Relay Standards and Requirements 20](#_Toc482878133)

[APPENDIX 2 23](#_Toc482878134)

[REMOTE ACCESS FACILITY (RAF) Access Standards and Requirements 23](#_Toc482878135)

[Private Line and Frame Relay Standards and Requirements 23](#_Toc482878136)

[APPENDIX 3 27](#_Toc482878137)

[REMOTE ACCESS FACILITY (RAF) Dial-up Access Standards and Requirements 27](#_Toc482878138)

[APPENDIX 4 28](#_Toc482878139)

[LSR XML Access Standards and Requirements 28](#_Toc482878140)

[GUI Access Standards 29](#_Toc482878141)

[LSR XML Provisioning Activities 30](#_Toc482878142)

[APPENDIX 5 31](#_Toc482878143)

[Miscellaneous Bulk Data Transfer (SFG) Access Standards and Requirements 31](#_Toc482878144)

[Miscellaneous Bulk Data Transfer (SFG) Provisioning Activities 31](#_Toc482878145)

[APPENDIX 6 32](#_Toc482878146)

[Establish a Dial-Up Connection for TCP/IP 32](#_Toc482878147)

[APPENDIX 7 35](#_Toc482878148)

[User ID Process 35](#_Toc482878149)

[Digital Certificates 35](#_Toc482878150)

APPENDIX 8 ………………………………………………………………………………………………………………. 36

Data Connection Security Requirements ………………………………………………………………............................. 36

[For CLEC Hardware/Software Requirements for Access to AT&T Uniform OSS Applications 40](#_Toc482878151)

# INTRODUCTION

This document provides information regarding options for electronic access to Operations Support Systems (OSSs) and procedures for connecting to an AT&T Incumbent Local Exchange Carrier (ILEC) company's External Business Partner (EBIZ) network. Access methods to electronic interfaces described herein are provided to comply with the Telecommunications Act of 1996, Competitive Checklist Item, Access to Support Systems, which stipulates that Competitive Local Exchange Carriers (CLECs) must be given equivalent access to ILEC data so they can service their customers in a timely manner.

The External Business Partner (EBIZ) network established across AT&T Wireline regions meets the Competitive Checklist requirement by providing CLECs with an entry point to access the functions of OSSs. This also meets the connectivity agreements as specified in the FCC Uniform and Enhanced Plan of Record.

Connectivity to AT&T’s Uniform Interfaces can only be accessed via one of AT&T’s regional EBIZ Points of Presence locations. Web Toolbar OSS applications offering Graphical User Interfaces (GUIs) may be accessed via the Internet using the CLEC's standard Internet Service Provider (ISP) [https://osstoolbar.att.com.](https://osstoolbar.att.com/) The LSR XML OSS application may be accessed via the Internet using the CLEC's standard Internet Service Provider (ISP). The connection will flow through a firewall to maintain data security.

More information may be obtained by contacting your CLEC Account Manager. Specific IP addresses are needed and will be provided by the IS Call Center.

The AT&T EBIZ Points of Presence locations are as follows:

* Alpharetta GA
* Dallas TX
* Fairfield CA
* Southfield MI

The EBIZ Points of Presence will connect to AT&T’s nationwide internal networks and will facilitate the uniform applications in the movement of traffic between regions. Regional xRAF connectivity will no longer be available for access to AT&T region-specific proprietary interfaces. Any EBIZ Point of Presence location can serve any AT&T Wireline region.

The “uniform” application software will be programmed to allow CLECs gaining access via any of the EBIZ Point of Presence locations to view customer data or place order requests for customers in any other AT&T region, subject to appropriate business rules and Interconnection Agreement requirements.

Non-discriminatory access to OSS functions is provided for unbundled network elements or resale services within the following functional areas:

* Pre-ordering
* Ordering/Provisioning
* Repair and Maintenance
* Billing

Further information concerning the above functions can be found on the CLEC Online web site <https://clec.att.com/clec/> or can be obtained from your CLEC Account Manager.

The access methods described in this document are available to CLECs who meet the following criteria:

1. The CLEC has contacted the appropriate CLEC Account Manager regarding doing business as a CLEC.
2. The CLEC has signed a Non-Disclosure Agreement with the appropriate AT&T ILEC Company.
3. The CLEC executes an Interconnection agreement including an OSS Appendix or appropriate OSS language.
4. The CLEC has completed applicable formal training sessions for those AT&T ILEC company OSSs that the CLEC will be utilizing.

In addition, there are certain activities that must take place to establish connectivity with the appropriate AT&T ILEC Company. These requirements are specified in other sections of this document.

**The CLEC should coordinate initial service connection procedures through their AT&T CLEC Account Manager. The CLEC Account Manager will set up the initial CLEC connectivity planning meetings as needed to include AT&T connectivity managers, members of the IS Call Center, and the AT&T OSS Customer Support Team.**

**During these meetings, questions concerning CLEC connectivity will be addressed. The IS Call Center will also provide forms that will assist the CLEC in documenting information needed to process their connectivity request.**

**A contract, that includes language governing OSS connectivity between the CLEC and the AT&T ILEC Company, must be executed and approved before any electronic information can pass between the two companies.**

# SUMMARY OF CHANGES

This section will identify the major changes that have been made throughout the text. The following table itemizes these changes.

***Change Description Table***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| DATE  | DESCRIPTION  | VERSION  | SECTION  | PAGE #  |
| 6/16/21 | Added Section in Appendix 8 for Conexus access security requirements | 7.1 | DATA SECURITY REQUIREMENTS  | 39 |
| 5/9/18 | Made major changes to accommodate retirement of RAF network (in favor of EBIZ network)Edited INTRODUCTION sectionAdded INTERCONNECTION REQUIREMENTS sectionAdded note of deprecation to REMOTE ACCESS FACILITY sectionSplit PRIVATE LINE OR FRAME RELAY ACCESS section into two sections: EXTERNAL BUSINESS PARTNER (EBIZ) PRIVATE LINE OR FRAME RELAY ACCESS and REMOTE ACCESS FACILITY (RAF) PRIVATE LINE OR FRAME RELAY ACCESSAdded note of deprecation to DIAL-UP ACCESS (ANALOG & DIGITAL) section and renamed section to REMOTE ACCESS FACILITY (RAF) DIAL-UP ACCESS (ANALOG & DIGITAL)Added placeholder section named MISCELLANEOUS BULK DATA TRANSFER (SFG) ACCESSAdded EXTERNAL BUSINESS PARTNER (EBIZ) Access Standards and Requirements appendix as new Appendix 1Added note of deprecation to former Appendix 1 (now Appendix 2) - Private Line and Frame Relay Standards and Requirements and renamed section to REMOTE ACCESS FACILITY (RAF) Access Standards and RequirementsMoved former Appendix 2 - Dial-up Access Standards and Requirements to Appendix 3, added note of deprecation to it and renamed it to REMOTE ACCESS FACILITY (RAF) Dial-up Access Standards and RequirementsMoved former Appendix 3 - LSR XML Access Standards and Requirements to Appendix 4Added Miscellaneous Bulk Data Transfer (SFG) Access Standards and Requirements appendix as new Appendix 5Moved former Appendix 4 - Establish a Dial-Up Connection for TCP/IP to Appendix 6 and added note of deprecation to itMoved former Appendix 5 - User ID Process to Appendix 7 | 7.0 | INTRODUCTIONREMOTE ACCESS FACILITYPRIVATE LINE OR FRAME RELAY ACCESSDIAL-UP ACCESS (ANALOG & DIGITAL)APPENDIX 1APPENDIX 2APPENDIX 3APPENDIX 4APPENDIX 5APPENDIX 6APPENDIX 7 |  |
| 3/6/13  | Removed reference to access to Web Toolbar over a dedicated circuit.  Removed reference to calling options and email addresses for ISCC contact.  | 6.0  | Introduction   IS Call Center  | 4   8  |
| 8/8/11  | Added information that AT&T only supports IPV4  | 5.9  | PRIVATE LINE OR FRAME RELAY ACCESS  APPENDIX 1   | 12    14  |
| 11/8/10  | Removal of EDI information.  | 5.8  | APPENDIX 3   | 17  |
| 7/10/09    | Addition of LSR XML Requirements  | 5.7  | LSR XML Requirements  | 3 4 10 12 19-21  |
| 4/21/08  | Removed Reference to Windows NT  Deleted page 24 – Creating a New Phone Book Entry - Windows NT  Added IE7 to the Toolbar requirements the & updated minimum hardware   | 5.6  |   | 13  24   27   |
| 5/18/07  | Removed References to Windows 95/98    Added Creating Dial-Up Network Connection in Windows XP   | 5.5  | DIAL-UP ACCESS (ANALOG & DIGITAL)  APPENDIX 4  | 13 & 21    21  |
| 4/30/07  | Changed hours of operation for the IS Call Center and updated the paragraph to show which regions are supported and the off hour coverage.  Removed reference to Windows NT, XP Service Pack 1 and 2 and IE6 Service Pack 1   | 5.4  | IS CALL CENTER (ISCC)   APPENDIX 5    | 8    26   |
| 3/6/07  | Changed the Sun Java Runtime Environment (JRE) to version v1.5.0\_10 as a requirement due to Daylight Savings Time (DST) scheduled for  | 5.3  | APPENDIX 5    | 26    |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | March 11.  Changed the reference and URL for the software to version v1.5.0\_10  |  |   APPENDIX 5  |   27  |
| 2/16/07  | Removed reference to Windows 95/98   Corrected a type in name of form, changed ID to IP   Removed example, Creating a new Phone Book entry – Windows 95/98  Removed Windows 98 from operating systems.  Changed the Sun Java Runtime Environment (JRE) to version v1.5.0\_06  Updated URL for new version of JRE   | 5.2  | REMOTE ACCESS FACILITY  PRIVATE LINE OR FRAME RELAY ACCESS  APPENDIX 4   APPENDIX 5  APPENDIX 5   APPENDIX 5  | 10   12    23   26  26   27  |
| 10/31/06  | Changed sbc.com to att.com (2 references)  Removed old URL  Removed old URL   Removed old URL   Remove outdated reference to footnote and add reference to OSS Hours of Operation  Removed old URL   Addition of XP Service Pack 2 as an option, and addition of minimum requirements for ExClaim application.  | 5.1  | INTRODUCTION  INTRODUCTION  IS CALL CENTER (ISCC)  REMOTE ACCESS REQUIREMENTS  APPENDIX 3, Number 7  APPENDIX 5, USER ID PROCESS  APPENDIX 5, CLEC Software Requirements for Toolbar Interconnection  | 4  5  7   8   17   24   26  |
| 5/31/06  | Rebranding.  Update xRAF locations.  Clarification of batch processing restrictions for EDI and CORBA Pre-Order Processing.  Clarification of batch processing restrictions for Verigate GUI Pre-Order Processing.  | 5.0  | All **\*\***  |   |

*\*\** ***NOTE:*** This revision is a complete replacement of any previous version of this document. As such, previous versions of this document are no longer accurate and must be destroyed.

# IS CALL CENTER (ISCC)

After a contract is signed between the CLEC and the AT&T ILEC Company, the Information Services Call Center (ISCC) is the single point of contact for all CLECs regarding OSS access problems. The ISCC is dedicated to providing quality professional customer service.

The ISCC is staffed by employees with varying technical expertise, including extensive knowledge of network operations, intelligent workstations and CLEC specific applications. The ISCC assumes ownership of all OSS problems reported by the CLEC and strives to provide prompt and knowledgeable resolutions. When necessary, the ISCC technicians coordinate with other help desks to provide prompt customer service.

***Objectives***

The ISCC will provide assistance to the CLECs by answering questions regarding access to AT&T ILEC company systems and applications. The ISCC will answer all calls using an Automatic Call Distribution (ACD) telephone system.

The intent of the ISCC is to solve as many problems as possible on the first call. If the ISCC agent cannot solve the problem, they will involve other support groups for resolution and report back to the caller.

The ISCC provides centralized OSS support for the AT&T Midwest, Southwest, Southeast and West regions and is available to CLEC’s 24 x 7. Contact and escalation information is also available on the ISCC web site accessed via the CLEC Online web site home page at <https://clec.att.com/clec/> .

IS Call Center Phone Number - 314-235-7225 option 3

|  |  |  |
| --- | --- | --- |
| UA Center E-mail -  | UACENTER@ATT.COM  | (Profile changes, security admin updates, administrative changes, User ID requests)  |
| IS Call Center Technology -  | ISCTECH@ATT.COM  | (File requests)  |

The ISCC may also be reached by calling the Mechanized Customer Support Center’s toll-free number, 1-877-681-2271, and then selecting Option 3.

# INTERCONNECTION REQUIREMENTS

AT&T is providing notice of a project to change the access methods in the Southeast for carriers that use point-to-point dedicated circuits and dial access to connect to the AT&T data centers.

The vendor equipment used to terminate dedicated point-to-point connections at the AT&T data centers and the vendor equipment used for dial access are at end-of-service-life (EOSL) and end-of-support (EOS) status. This makes maintaining and restoring service increasingly difficult. Carriers will now connect to AT&T over the internet to minimize the chances of extended degradation of service occurring in the event of an outage.

Carriers may connect via Virtual Private Network (VPN) using the IPSEC encryption protocol securely through the internet If a carrier only requires sending files to an electronic mailbox or retrieving files from an electronic mailbox using the secure file transfer protocol (sftp) with the secure shell (ssh) protocol, AT&T provides that connectivity over the internet.

Carriers impacted by the change will be required to make changes to their networks and security configurations to facilitate a seamless transition. Carriers that do not have the capability for VPN or don’t have internet access will be required to upgrade their networks. AT&T will work collaboratively with carriers in the planning and conversion to IPSEC tunnels or electronic mailboxes accessed via the internet to ensure minimal disruption during conversions.

The CLEC should notify their CLEC Account Manager when they wish to establish electronic connections to AT&T's remote access facility. The CLEC Account Manager will work with the CLEC to identify the functions that the CLEC wishes to perform, and to associate those functions with the corresponding application. The CLEC Account Manager or the CLEC should provide the circuit ID and the service due date as soon as it is known to the IS Call Center (ISCC).

Before a CLEC can access any AT&T ILEC company system, they must complete the CLEC User ID Request Form. The CLEC Account Manager will supply the CLEC with this form. After completing, the CLEC should return the form to the CLEC Account Manager, who then authorizes access by signing the form and forwarding it to the ISCC. The CLEC may also e-mail the form to the ISCC with a carbon copy (cc) to the CLEC Account Manager. By signing the form the CLEC agrees to AT&T ILEC company security requirements for access. A copy of those requirements will be supplied by the CLEC Account Manager along with the CLEC User ID Request Form. The CLEC must adhere to AT&T ILEC company security requirements when accessing AT&T systems.

AT&T has implemented a block User ID process. Access IDs for the uniform interfaces follow this new process. Refer to Appendix 7 for details regarding the block User ID process.

The CLEC Account Manager can provide a list of hardware/software requirements for access to each of the AT&T OSS functions and the hours of operation of each system. This information is also available on the CLEC Online web site, <https://clec.att.com/clec/> .

Up to this point the CLEC Account Manager has been the first point of contact for the CLEC. After receiving authorization to access the EBIZ network, future communication regarding connectivity and application functions should be referred to the ISCC. The ISCC becomes the primary contact for the CLEC to assist in answering OSS questions and resolving problems; e.g., installation and configuration of software, correcting CLEC hardware/software anomalies and problems connecting, expired password, application problems, network problems such as initial connect problems as in the connection dropping before getting to application and connection problems after getting to application.

**\*\*\* NOTE: Remote Access Facility (RAF) network infrastructure that terminates dedicated point-to-point connections and that are used for dial access at the AT&T data centers are at end-of-service-life (EOSL) and end-of-support (EOS) status. Thus, the material on this page will be deprecated. \*\*\***

# REMOTE ACCESS FACILITY (RAF)

This section may be used as a planning guide to identify most activities associated with providing for a network to network connection between an external entity and the OSS accessible via the AT&T Remote Access Facility (RAF) network. The AT&T Remote Access Facility (RAF) network is a data communications facility that provides a secure network interface from CLEC networks to AT&T ILEC Company Data Communications Network (DCN).

The “REQUIREMENTS” appendixes (2, 4, 5, 6 and 7) identify specific standards and requirements that are applied to remote access connections to the AT&T ILEC company Operation Support Systems. Please note that there are some applications for which connectivity can be established via the Internet or through direct connections using a browser configured to the Remote Access Facility (RAF) network. Please contact your OSS or CLEC Account Manager for more details.

The other sections identify the procedural steps required to provide an external entity remote access to AT&T ILEC company data communications resources. Because each CLEC's network facilities and environment may be different, there may be variances in the actual requirements. Appendix 2 contains guidelines for use in establishing an electronic connection to the AT&T Remote Access Facility (RAF). Appendix 4 contains guidelines associated with LSR XML. Appendix 5 contains miscellaneous Bulk Data Transfer information. Appendix 6 contains a sample procedure to configure a dial-up interface. Appendix 7 explains the User ID Process and addresses Digital Certificates

All CLECs will be asked to provide answers to the applicable questions which follow and forward them to the IS Call Center contact. This person can assist the project planner in completing this checklist.

The AT&T Remote Access Facility (RAF) network hours of availability are 24 x 7 x 365. However, the hours of availability for the various AT&T ILEC company Operation Support Systems correspond with the application’s hours of availability. Some restrictions are as follows:

|  |  |
| --- | --- |
| Batch File Transfers:  | Permitted from 9:00 p.m. through 12:59 a.m.  |
| Maintenance Window:  | Unavailable from 1:00 a.m. through 4:00 a.m.  |
| Batch File Transfers:  | Permitted from 4:01 a.m. through 7:00 a.m.  |

Eastern Time for AT&T EAST

Central Time for AT&T MIDWEST and AT&T SOUTHWEST

Pacific Time for AT&T WEST

**\*\*\* NOTE: Remote Access Facility (RAF) network infrastructure that terminates dedicated point-to-point connections and that are used for dial access at the AT&T data centers are at end-of-service-life (EOSL) and end-of-support (EOS) status. Thus, the material on this page will be deprecated. \*\*\***

# COORDINATION OF ACCESS REQUIREMENTS

Following are steps a CLEC will take in assessing their connectivity needs.

1. Requirements Gathering
	1. Identify Workstation Requirements;
	2. Identify Users And Associated Workstation Addresses Requiring Access;
	3. Identify Specific Host Systems (Operations Support Systems) to Access;
	4. Identify Networking Requirements.

1. Determine if a network to network connection with the AT&T ILEC Company currently exists and if so, coordinate with the AT&T ILEC Company to determine if multiple connections can exist based upon the IP addresses the CLEC is using over those connections.

1. Provide CLEC Network Contact Information to the AT&T ILEC Company.

# EXTERNAL BUSINESS PARTNER (EBIZ) ACCESS

## Connection Provisioning Activities

###  VPN (IPSec VPN via Public Internet transport)

1. CLEC Orders Public Internet Connectivity in desired location(s), if needed.

1. CLEC Orders IPSec VPN Termination Equipment for their location(s), if needed.
2. AT&T ILEC will provide IPSec VPN Termination Equipment to terminate the IPSec VPN tunnel(s) on the AT&T ILEC side.
3. CLEC and AT&T ILEC will negotiate the following terms:
	1. Identify Source and Destination Building Locations for IPSec VPN tunnel(s);
	2. Negotiate Tunnel Requirements Between Networks;
	3. Negotiate IPSec VPN Termination Equipment Configuration Requirements Between Networks.

1. CLEC Provides IPSec VPN Tunnel Configuration Information to the IS Call Center:
	1. Business Purpose for this connection
	2. Contract/tariff number
	3. CLEC Network & DNS Technical Contact information
	4. VPN tunnel termination endpoint(s) Street Address
	5. VPN tunnel peer IP address – **Must be valid, public, registered IP address (ownership or right-to-use will be validated)**
	6. VPN tunnel host IP address(es) – **Must be valid, public, registered IP address (ownership or right-to-use will be validated)**
	7. IKE Policies used for VPN tunnel(s) are as follows:
		1. Parameter: Value
		2. Message encryption algorithm: Triple-DES
		3. Message integrity (hash) algorithm: SHA
		4. Peer authentication method: Preshared key
		5. Key exchange parameters (Diffie-Hellman group identifier and Perfect Forward Secrecy Group): Group 2 (1024-bit)
		6. ISAKMP established security associations lifetime: 86400 seconds
	8. IPSec Parameters used for VPN tunnel(s) are as follows:
		1. Security-association (SA) establishment: ipsec-isakmp (IKE)
		2. IPSec Mode: Tunnel
		3. Mechanism for payload: ESP
		4. ESP transform: ESP-3DES
		5. Hashed Message Authentication Code: ESP-SHA-HMAC
		6. Security-association (SA) lifetime: 3600 seconds (1hr)

### MPLS, Point-to-Point Ethernet

1. CLEC or AT&T Internal Network Services Orders Connecting Circuit:
	1. Identify Source and Destination Building Locations for Circuits;
	2. Negotiate Circuit Requirements Between Networks;
	3. Negotiate Router Configuration Requirements Between Networks.

1. CLEC Orders Circuit Termination Equipment for Circuit Connection for their location, if needed.

1. AT&T ILEC will provide a Router to terminate on the AT&T ILEC side.

1. CLEC or AT&T Internal Network Services Provides Circuit Order Information to the IS Call Center:
	1. Provider of Circuit
	2. Circuit Number;
	3. Circuit Speed;
	4. Other Providers of Intermediate Circuit Spans;
	5. Circuit Type
	6. Termination address for the CLEC side of the connection
	7. Circuit serial link IP address(es) – **Must be valid, public, registered IP address (ownership or right-to-use will be validated)**
	8. CLEC network host IP address(es) – **Must be valid, public, registered IP address (ownership or right-to-use will be validated)**

## Network Provisioning Activities

1. CLEC provides the AT&T ILEC Company the following information: TCP/IP Address for VPN peer IP address, networks to be routed across VPN tunnel, etc. Connecting CLEC must have a valid, public, registered Internet Protocol (IP) network address for the network connection termination device peer IP address. The ownership or right-to-use for any IP address submitted will be validated before its use will be accepted. AT&T currently only supports IPv4. This information must be submitted via the Connection Specifications for New Connectivity form, available from your CLEC Account Manager.
2. CLEC provides the AT&T ILEC Company the following information: TCP/IP Address(es) for Remote Workstation(s). Connecting CLEC must have & use valid, public, registered Internet Protocol (IP) network addresses for referencing devices that need to interact with AT&T ILEC OSS applications. The ownership or right-to-use for any IP address submitted will be validated before its use will be accepted. AT&T currently only supports IPv4. This information must be submitted via the CLEC IP Request Form, available from your CLEC Account Manager.

1. Configure the Remote PC workstation and the TCP/IP communications software package using the information as supplied by the Application Sponsor. The current Web address is supplied on the CLEC IP Request form.

**Note 1:** The PC workstation must be configured to access the AT&T ILEC company LAN based resources using only the TCP/IP protocol.

**Note 2:** EBIZ Access forms (such as the Connection Specifications for New Connectivity form), LSR XML request forms are available from your CLEC Account Manager.

1. Test Network to Network Connectivity

1. Test the Remote PC Workstation’s Access to AT&T OSSs:

a) Access the AT&T ILEC Company OSS using an IP address. User should see successful connection to authorized resource.

1. Please note the AT&T currently only supports IPv4.

**\*\*\* NOTE: Remote Access Facility (RAF) network infrastructure that terminates dedicated point-to-point connections and that are used for dial access at the AT&T data centers are at end-of-service-life (EOSL) and end-of-support (EOS) status. Thus, the material on this page will be deprecated. \*\*\***

# REMOTE ACCESS FACILITY (RAF) PRIVATE LINE OR FRAME RELAY ACCESS

## Circuit Provisioning Activities

1. CLEC Orders Connecting Circuit:
	1. Identify Source and Destination Building Locations for Circuits;
	2. Negotiate Circuit Requirements Between Networks;
	3. Negotiate Router Configuration Requirements Between Networks.
2. CLEC Orders Circuit Termination Equipment for Circuit Connection for their location, if needed.
3. AT&T ILEC will provide a Router with and internal CSU to terminate on the AT&T ILEC side.
4. CLEC Provides Circuit Order Information to the IS Call Center:
	1. Provider of Circuit
	2. Circuit Number;
	3. Circuit Speed;
	4. Circuit Line Coding must be B8ZS;
	5. Circuit Framing must be ESF;
	6. Other Providers of Intermediate Circuit Spans;
	7. Circuit Type (Private line or Frame Relay).
	8. Termination address for the CLEC side of the connection

## Network Provisioning Activities

1. CLEC provides the AT&T ILEC Company the following information: TCP/IP Address For Remote Workstation(s). This information must be submitted via the CLEC IP Request Form, available from your CLEC Account Manager.
2. Configure the Remote PC workstation and the TCP/IP communications software package using the information as supplied by the Application Sponsor. The current Web address is supplied on the CLEC IP Request form.
	* **Note 1**: The PC workstation must be configured to access the AT&T ILEC company LAN based resources using only the TCP/IP protocol.
	* **Note 2**: RAF Access forms, LSR XML request forms are available from your CLEC Account Manager.
3. Test Network to Network Connectivity
4. Test the Remote PC Workstation’s Access to AT&T OSSs:
	1. Access the AT&T ILEC Company OSS using an IP address. User should see successful connection to authorized resource.
5. Please note the AT&T currently only supports IPV4.

**\*\*\* NOTE: Remote Access Facility (RAF) network infrastructure that terminates dedicated point-to-point connections and that are used for dial access at the AT&T data centers are at end-of-service-life (EOSL) and end-of-support (EOS) status. Thus, the material on this page will be deprecated. \*\*\***

**\*\*\* NOTE: Remote Access Facility (RAF) network infrastructure that terminates dedicated point-to-point connections and that are used for dial access at the AT&T data centers are at end-of-service-life (EOSL) and end-of-support (EOS) status. Thus, the material on this page will be deprecated. \*\*\***

# REMOTE ACCESS FACILITY (RAF) DIAL-UP ACCESS (ANALOG & DIGITAL)

For analog activities, skip steps 1 through 3.

For ISDN circuit provisioning activities, include all steps.

1. CLEC Orders Basic Rate ISDN (BRI) Circuit:
	1. This service should be configured as "2B+D" or “1B+D”. Each "B" channel is capable of voice and/or data at 64 or 56 Kbps. Each of these channels will be assigned a number known as a SPID (Service Profile Identifier).

1. CLEC Orders ISDN Terminal Adapter Equipment for their Circuit Equipment Termination.

1. CLEC Provides ISDN Circuit Order Information to the AT&T ILEC Company:
	1. ISDN BRI Circuit Number \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
	2. ISDN BRI Switch Type \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
	3. ISDN SPID For “B” Channel 1 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
	4. ISDN SPID For “B” Channel 2 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
	5. Phone Number For “B” Channel 1 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
	6. Phone Number For “B” Channel 2 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
	7. Remote Terminal Adapter Type \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
	8. Remote Premises Contact Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
	9. Remote Premises Contact Address \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
	10. Remote Premises Contact Telephone Number \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Configure the Remote PC workstation and the TCP/IP communications software package using the information as supplied by the Application Sponsor.

**Note:** The PC workstation must be configured to access the AT&T ILEC company LAN based resources using only the TCP/IP protocol.

1. Initiate Dial-up Connection and Test Network Connectivity.

1. Test the Remote PC Workstation’s Access to AT&T ILEC Company OSSs:
	1. Access the AT&T ILEC Company OSS using an IP address. User should see successful connection to authorized resource.

1. Appendix 6 contains sample procedures to configure a dial-up interface using Windows communications software.

**\*\*\* NOTE: Remote Access Facility (RAF) network infrastructure that terminates dedicated point-to-point connections and that are used for dial access at the AT&T data centers are at end-of-service-life (EOSL) and end-of-support (EOS) status. Thus, the material on this page will be deprecated. \*\*\***

# MISCELLANEOUS BULK DATA TRANSFER ACCESS

For miscellaneous bulk data transfers, AT&T has an Internet gateway or secure external drop box available through which the exchange of SFTP files can be accomplished. This AT&T secure external drop box or Internet gateway may have previously been known by your network, security, account management and applications support teams as “SEDB” or “AICXFER”.

Companies wishing to use this Internet gateway or secure external drop box infrastructure will need to convert with the support and assistance of AT&T in a coordinated effort. Each carrier will be required to test this access path and to report completion to AT&T when the migration is complete.

This file transfer gateway can replace or reduce the need for connections that companies currently have in place using dedicated network connectivity methods to AT&T (such as IPSec VPN or point-to-point circuits) or other special purpose internet gateways depending upon the OSS access needs for specific CLEC companies.

This file transfer gateway will only support Secure FTP transfers (SFTP) using Secure Shell (SSH) Public/Private keys. In general, companies have far fewer problems configuring SSH FTP through the firewalls, and use of SSH with Public/Private keys avoids the need to manage passwords and password changes.

# APPENDIX 1

## EXTERNAL BUSINESS PARTNER (EBIZ) Access Standards and Requirements

### VPN (IPSec VPN via Public Internet transport) Standards and Requirements

1. A Remote Access Facility for CLEC access is located in four locations. Each location has network access to any AT&T ILEC region.

1. Network to network connection between connecting entities will consist of either one IPSec VPN tunnel using static routing or two IPSec VPN tunnels using BGP routing with accompanying GRE tunnels across the public Internet.

1. All AT&T ILEC company routers used within the External Business Partner (EBIZ) network will be Cisco routers. Interconnection specific issues and requirements will be communicated with the connecting CLEC when remote access service activation is negotiated.

1. All network communications between AT&T ILEC company network address space and connecting CLEC network address space will use this network connection. All other logical/physical paths will be blocked. The current browser address is supplied on the CLEC IP Request form.

1. Static routes or Border Gateway Protocol Version 4 (BGP 4) will be the only routing methods used between entities. No other routing methods will be used. Only the BGP routing protocol traffic will traverse the accompanying GRE tunnels. The user data will traverse the IPSec VPN tunnel specifically.

1. Routed traffic over network link will use TCP/IP.

1. CLEC assumes all potential risks associated with network reliability and security of transmission over the public Internet & agrees to not hold AT&T liable for any Internet connectivity problems.

1. Point of demarcation for AT&T ILEC support will be the terminating device located in the AT&T ILEC network as well as the AT&T ILEC Internet connections (via the AT&T Internet Service Provider). Point of demarcation for CLEC support will be the terminating device on the CLEC end as well as their Internet connections (via their Internet Service Provider).

1. AT&T personnel will be responsible for the AT&T ILEC company router and/or network configuration.

1. CLEC provided router(s) are not allowed on AT&T ILEC company premises.

1. CLEC router(s) at the CLEC premises that must “communicate” with the AT&T ILEC company router(s) must conform to standards supportable by the AT&T ILEC Company provided router.

1. Connecting CLEC must have a valid, public, registered Internet Protocol (IP) network address for network connection (terminating device peer IP address). Connecting CLEC must also have & use valid, public, registered Internet Protocol (IP) network addresses for referencing devices that need to interact with AT&T ILEC OSS applications. The ownership or right-to-use for any IP address submitted will be validated before its use will be accepted. AT&T currently only supports IPv4.

1. Connecting CLEC is responsible for providing its own Internet connectivity per the following requirements:

**Supplier:** Internet connectivity may be ordered through CLEC’s supplier of choice.

**Type:** Not specified. Determined strictly by the needs of the CLEC.

The CLEC will be responsible for all replacement or repair of CLEC Internet connectivity.

**Bandwidth:** The CLEC is responsible for sizing Internet connectivity bandwidth to service its needs.

1. The connecting CLEC is responsible for providing the terminating router that would terminate the needed VPN tunnels for connectivity between the CLEC and the AT&T ILEC networks.

1. Connecting CLEC personnel will be responsible for CLEC router and/or network configuration, and all network equipment and circuit connection(s) up to the AT&T ILEC company point of demarcation.
2. All access to AT&T ILEC Company OSSs will be denied by default and permitted by authorized exception (as approved by application project manager).

1. All OSS access requires a valid AT&T ILEC company user identification and password. UserIDs can be associated with any CLEC IP address; i.e., workstation.

1. Multiple connecting partners will not enter an AT&T ILEC company's network over the same VPN tunnel termination(s). The only exception is when the connecting partner is a Service Bureau Provider (SBP). In this arrangement, the SBP can service multiple CLECs over the same physical termination. The Service Bureau Provider must have a written agreement with AT&T and appropriate wording may need to be amended to the CLEC(s) Interconnection Agreement before this connectivity arrangement may take place.

### MPLS, Point-to-Point Ethernet Standards and Requirements

1. A Remote Access Facility for CLEC access is located in four locations. Each location has network access to any AT&T ILEC region.

1. Network to network connection between connecting entities will be a single circuit connection or a pair of circuit connections where only one of them is primary at a particular point in time (in an active/standby state).

1. All AT&T ILEC company routers used within the External Business Partner (EBIZ) network will be Cisco routers. Interconnection specific issues and requirements will be communicated with the connecting CLEC when remote access service activation is negotiated.

1. All network communications between AT&T ILEC company network address space and connecting CLEC network address space will use this network connection. All other logical/physical paths will be blocked. The current browser address is supplied on the CLEC IP Request form.

1. Static routes or Border Gateway Protocol Version 4 (BGP 4) will be the only routing methods used between entities. No other routing methods will be used.

1. Routed traffic over network link will use TCP/IP.

1. Point of demarcation will be the serial port on the AT&T ILEC company provided router.

1. AT&T personnel will be responsible for the AT&T ILEC company router and/or network configuration.

1. CLEC provided router(s) or any other devices are not allowed on AT&T ILEC company premises.

1. CLEC router(s) at the CLEC premises that must “communicate” with the AT&T ILEC company router(s) must conform to standards supportable by the AT&T ILEC Company provided router.

1. Connecting CLEC must have a valid, public, registered Internet Protocol (IP) network address for network connection. AT&T currently only supports IPv4.

1. Connecting CLEC provides IP network addressing up to and including point of AT&T ILEC company demarcation (router serial port on AT&T ILEC Company provided router). Connecting CLEC provides IP addresses for both ends of the circuit from this IP network address. Connecting CLEC must also have & use valid, public, registered Internet Protocol (IP) network addresses for referencing devices that need to interact with AT&T ILEC OSS applications. The ownership or right-to-use for any IP address submitted will be validated before its use will be accepted.

1. Connecting CLEC is responsible for providing a circuit between the CLEC site and AT&T ILEC company per the following requirements:

**Supplier:** Circuit may be ordered through CLEC’s supplier of choice.

**Type:** MPLS Ethernet or Point-to-Point Ethernet.

**Bandwidth:** Minimum requirements: 56 Kbps, fractional T1 (1.544Mbps).

The CLEC is responsible for sizing the bandwidth to service their needs.

**Installation:** Must be coordinated through the IS Call Center.

**Termination Address:** Terminate Circuit at one of the following External Business Partner

(EBIZ) locations:

 **300 North Point Parkway**

**Alpharetta GA 30005**

**NPA-NNX: 770-750**

**211 South Akard Street**

**Dallas TX 75202**

**NPA-NNX: 214-464**

**2525 North Watney Way**

**Fairfield CA 94533**

**NPA-NNX: 707-435**

**23500 Northwestern Highway**

**Southfield MI 48075**

**NPA-NNX: 248-424**

1. The connecting CLEC is responsible for providing all of the required terminating equipment plus all network infrastructure on their premises, including connecting router:

1. Connecting CLEC personnel will be responsible for CLEC router and/or network configuration, and all network equipment and circuit connection(s) up to the AT&T ILEC company point of demarcation. The CLEC will be responsible for all replacement or repair of CLEC provided circuits(s).

1. All access to AT&T ILEC Company OSSs will be denied by default and permitted by authorized exception (as approved by application project manager).

1. All OSS access requires a valid AT&T ILEC company user identification and password. UserIDs can be associated with any CLEC IP address; i.e., workstation.

1. Multiple connecting partners will not enter an AT&T ILEC company's network over the same physical termination. The only exception is when the connecting partner is a Service Bureau Provider (SBP). In this arrangement, the SBP can service multiple CLECs over the same physical termination, as long as the connection type is Frame Relay. The Service Bureau Provider must have a written agreement with AT&T and appropriate wording may need to be amended to the CLEC(s) Interconnection Agreement before this connectivity arrangement may take place.

**\*\*\* NOTE: Remote Access Facility (RAF) network infrastructure that terminates dedicated point-to-point connections and that are used for dial access at the AT&T data centers are at end-of-service-life (EOSL) and end-of-support (EOS) status. Thus, the material on this page will be deprecated. \*\*\***

# APPENDIX 2

## REMOTE ACCESS FACILITY (RAF) Access Standards and Requirements

### Private Line and Frame Relay Standards and Requirements

1. A Remote Access Facility for CLEC access is located within each AT&T ILEC region.

1. Network to network connection between connecting entities will be a single circuit connection; i.e. private line or Frame Relay (T1 speeds or fractional T1).

1. All AT&T ILEC company routers used within the Remote Access Facility will be Cisco routers. Interconnection specific issues and requirements will be communicated with the connecting CLEC when remote access service activation is negotiated.

1. All network communications between AT&T ILEC company network address space and connecting CLEC network address space will use this network connection. All other logical/physical paths will be blocked. The current browser address is supplied on the CLEC IP Request form

1. Static routes or Border Gateway Protocol Version 4 (BGP 4) will be the only routing methods used between entities. No other routing methods will be used.

1. Routed traffic over network link will use TCP/IP.

1. Non-AT&T ILEC Company to non-AT&T ILEC company network system access is not permitted over the AT&T ILEC Company’s DCN.

1. Point of demarcation will be the serial port on the AT&T ILEC company provided router.

1. AT&T personnel will be responsible for the AT&T ILEC company router and/or network configuration.

 **\*\*\* NOTE: Remote Access Facility (RAF) network infrastructure that terminates dedicated point-to-point connections and that are used for dial access at the AT&T data centers are at end-of-service-life (EOSL) and end-of-support (EOS) status. Thus, the material on this page will be deprecated. \*\*\***

 **\*\*\* NOTE: Remote Access Facility (RAF) network infrastructure that terminates dedicated point-to-point connections and that are used for dial access at the AT&T data centers are at end-of-service-life (EOSL) and end-of-support (EOS) status. Thus, the material on this page will be deprecated. \*\*\***

1. CLEC provided router(s) are not allowed on AT&T ILEC company premises.

1. CLEC router(s) at the CLEC premises that must “communicate” with the AT&T ILEC company router(s) must conform to standards supportable by the AT&T ILEC Company provided router.

1. Connecting CLEC must have a valid, public, registered Internet Protocol (IP) network address for network connection. AT&T currently only supports IPV4.

1. Connecting CLEC provides IP network addressing up to and including point of AT&T ILEC company demarcation (router serial port on AT&T ILEC Company provided router). Connecting CLEC provides IP address for both ends of the circuit from this IP network address.

 **\*\*\* NOTE: Remote Access Facility (RAF) network infrastructure that terminates dedicated point-to-point connections and that are used for dial access at the AT&T data centers are at end-of-service-life (EOSL) and end-of-support (EOS) status. Thus, the material on this page will be deprecated. \*\*\***

**\*\*\* NOTE: Remote Access Facility (RAF) network infrastructure that terminates dedicated point-to-point connections and that are used for dial access at the AT&T data centers are at end-of-service-life (EOSL) and end-of-support (EOS) status. Thus, the material on this page will be deprecated. \*\*\***

1. Connecting CLEC is responsible for providing a circuit between the CLEC site and AT&T ILEC company per the following requirements:

**Supplier:** Circuit may be ordered through CLEC’s supplier of choice.

**Type:** Private Line or Frame Relay.

**Bandwidth:** Minimum requirements: 56 Kbps, fractional T1 (1.544Mbps). The CLEC is responsible for sizing the bandwidth to service their needs.

**Installation:** Must be coordinated through the IS Call Center.

**Termination Address:** Terminate Circuit at: one of the following regional xRAF locations:

**AT&T MIDWEST**

**2305 Sanders Road, Floor 2 Northbrook, IL 60062**

**NPA-NXX = 847-402**

**Before ordering a circuit to Northbrook contact your AT&T CLEC Account Manager for more detailed information on terminating at this location.**

**AT&T WEST**

**2525 North Watney Way, Room D216**

**Fairfield, CA 94533**

**NPA-NXX = 707-435**

**AT&T SOUTHEAST**

**9139 Research Dr.**

**Charlotte, NC. 28262**

**NPA-NXX = 704-510**

**AT&T SOUTHEAST**

**1876 Data Drive**

**Hoover, AL 35244**

**NPA-NXX = 205-988**

**AT&T SOUTHWEST**

**211 S. Akard, Room 367**

**Dallas, TX 75202**

**NPA-NXX = 214-464**

1. The connecting CLEC is responsible for providing the terminating CSU/DSU plus all network infrastructure on their premises, including connecting router:

 **\*\*\* NOTE: Remote Access Facility (RAF) network infrastructure that terminates dedicated point-to-point connections and that are used for dial access at the AT&T data centers are at end-of-service-life (EOSL) and end-of-support (EOS) status. Thus, the material on this page will be deprecated. \*\*\***

**\*\*\* NOTE: Remote Access Facility (RAF) network infrastructure that terminates dedicated point-to-point connections and that are used for dial access at the AT&T data centers are at end-of-service-life (EOSL) and end-of-support (EOS) status. Thus, the material on this page will be deprecated. \*\*\***

1. Connecting CLEC personnel will be responsible for CLEC router and/or network configuration, and all network equipment and circuit connection(s) up to the AT&T ILEC company point of demarcation. The CLEC will be responsible for all replacement or repair of CLEC provided circuits(s).

1. All access to AT&T ILEC Company OSSs will be denied by default and permitted by authorized exception (as approved by application project manager).

1. All OSS access requires a valid AT&T ILEC company user identification and password. UserIDs can be associated with any CLEC IP address; i.e., workstation.

1. Frame Relay encapsulation will be Internet Engineering Task Force (IETF) encapsulation.

1. Serial port interfaces in AT&T ILEC Company routers that terminate Frame Relay circuits will be “sub-divided” using sub-interfaces.

1. Multiple connecting partners will not enter an AT&T ILEC company's network over the same physical termination. The only exception is when the connecting partner is a Service Bureau Provider (SBP). In this arrangement, the SBP can service multiple CLECs over the same physical termination, as long as the connection type is Frame Relay. The Service Bureau Provider must have a written agreement with AT&T and appropriate wording may need to be amended to the CLEC(s) Interconnection Agreement before this connectivity arrangement may take place.

 **\*\*\* NOTE: Remote Access Facility (RAF) network infrastructure that terminates dedicated point-to-point connections and that are used for dial access at the AT&T data centers are at end-of-service-life (EOSL) and end-of-support (EOS) status. Thus, the material on this page will be deprecated. \*\*\***

# APPENDIX 3

 **\*\*\* NOTE: Remote Access Facility (RAF) network infrastructure that terminates dedicated point-to-point connections and that are used for dial access at the AT&T data centers are at end-of-service-life (EOSL) and end-of-support (EOS) status. Thus, the material on this page will be deprecated. \*\*\***

## REMOTE ACCESS FACILITY (RAF) Dial-up Access Standards and Requirements

1. Dial-up access (using analog modem or ISDN Terminal Adapter) will be provided using Point to Point Protocol (PPP). The connecting device (PC workstation) must be capable of initiating a PPP connection using a TCP/IP communications software package installed on the connecting device. TCP/IP application software such as Telnet, TN3270, FTP, etc., must reside and execute directly on the connecting device.

1. The point of demarcation for dial-up access (using analog modem or ISDN Terminal Adapter) will be the

“modem” port on the AT&T ILEC company provided access server. The dial-up phone number will be provided to the connecting CLEC with the AT&T ILEC company user identification and password information.

1. The Access Server modems are optioned to support analog dial-up speeds at a maximum connection rate of 56,000 bps. The modems will automatically detect the connection speed of the sending modem and adjust accordingly. The connection preference for the data connection is 8 data bits, 1 stop bit and no parity. TCP/IP header and data compression are supported.

1. The Access Server(s) are optioned to support ISDN dial-up speeds at a maximum connection rate of 128,000 bps. These servers support single or dual channel (Multi-link PPP) ISDN access. Password Authentication Protocol (PAP) support on the connecting Terminal Adapter is required. The connection preference for the data connection is 8 data bits, 1 stop bit and no parity. TCP/IP header and data compression are supported.

1. The Access Server will supply the end user’s connecting device with an IP address and a default gateway.

1. Access to AT&T ILEC company systems via analog or ISDN dial-up will require user authentication via a unique AT&T ILEC company user identification and password combination. The AT&T ILEC Company will provide the user identification and password to the connecting CLEC.

**\*\*\* NOTE: Remote Access Facility (RAF) network infrastructure that terminates dedicated point-to-point connections and that are used for dial access at the AT&T data centers are at end-of-service-life (EOSL) and end-of-support (EOS) status. Thus, the material on this page will be deprecated. \*\*\***

# APPENDIX 4

## LSR XML Access Standards and Requirements

1. In order to access the AT&T LSR XML Pre-Order, Order and Post-Order Interface, a CLEC may connect over a Private Line or Frame Relay connection into an xRAF or use Internet access to send LSR XML transactions to the AT&T ILEC company for processing. CLECs may use only one access method.

1. A CLEC may NOT use LSR XML Pre-Order, Order and Post-Order Interface over a dial-up connection into the xRAF, to send LSR XML transactions to an AT&T ILEC company for processing. For LSR XML Pre-Order and Post-Order Interface, an interactive two-way communication is required. This means that the CLEC’s system connects to AT&T’s LSR XML systems which then connect back to the CLEC system through the AT&T firewall. This communication scheme requires translation rules to exist in order to map the CLEC’s fixed IP address and port information. If a CLEC connects via Dial-Up, there is no fixed IP address and port information for the LSR XML systems to map back to. This information cannot be dynamically extracted.
2. The xRAF is not a store and forward service. It provides for a point of network interconnection.

1. All standards and requirements as identified in Appendix 1 (Private Line and Frame Relay Standards and Requirements) apply to LSR XML.

1. AT&T is committed to support LSR XML guidelines as developed by Industry Standard Forums. Industry websites for ATIS should be referenced for applicable documentation. The ATIS website may be found at:

[http://www.atis.org](http://www.atis.org/)

1. LSR XML Order Processing:

Requests and responses must be packaged individually (batching of requests is not supported).

While the number of files per minute or hour is dependent upon CLEC volumes, it is AT&T’s expectation that the CLEC workload will be reasonably distributed throughout the available hours. In general, a CLEC should send no more than 20% of their normal daily volume in any one hour, and no more than 30% of that hourly volume should be sent in any 10-minute period.

If a CLEC knows or has reason to believe its processing needs may exceed those which can be accommodated based on these guidelines, the CLEC must contact their AT&T Account Management Team to negotiate special arrangements. This process should be followed for special conversions or other special circumstances that involve large volumes of LSRs.

If a CLEC experiences problems on either their side or AT&T's side of the LSR XML interface and, after the problems are cleared, must send a backlog of LSRs to AT&T, the CLEC must contact the IS Call Center prior to resuming transmission of LSRs. The CLEC may then send LSRs at their typical hourly volume plus up to 200 additional LSRs in any 10-minute period. This should occur during **system processing hours only**. Ordering system processing hours can be found in the OSS Hours of Operation document. The OSS Hours of Operation document is available on the CLEC Online website <https://clec.att.com/clec/>by selecting CLEC Handbook from the left side menu, then selecting the handbook for your region. Once in the Handbook section, select OSS from the left side menu, then select Operations Support Systems. The OSS Hours of Operation document should then be one of the choices available to you. **Note – there is a difference between Ordering Availability hours and System Processing hours.**  If the CLEC requires a rate that exceeds this volume, they should coordinate through their AT&T Account Management Team and/or the IS Call Center.

A failure by a CLEC to comply with any of the above referenced guidelines that impacts performance measurement results will result in adjustments to performance measurements penalties payable via the invocation of the appropriate subsections of the Interconnection Agreement dealing with CLEC caused impacts.

1. LSR XML Pre-Order Processing.

The LSR XML pre-order processing supported by AT&T is based on interactive transactions between AT&T and the CLEC. This application is intended for use by CLECs on a real time basis only and any other use is neither contemplated nor supported by AT&T. Batch or mass query mode is not applicable for this application.

A failure by a CLEC to comply with any of the above referenced guidelines that impacts performance measurement results will result in adjustments to performance measurements penalties payable via the invocation of the appropriate subsections of the Interconnection Agreement dealing with CLEC caused impacts.

1. With the introduction of the uniform interfaces, AT&T will allow each CLEC to have up to three

CLEC\_APPL\_IDs within an AT&T region, per environment. When a CLEC contracts with a Service Bureau Provider, the CLEC\_APPL\_ID used to identify this arrangement will be considered to be one of the CLEC’s three CLEC\_APPL\_IDs. Each CLEC\_APPL\_ ID may have up to two unique IP address/port combinations (one for inbound transactions and one for outbound responses), or these IDs could use the same common IP address. These LSR XML CLEC\_APPL\_IDs are assigned by the AT&T LSR XML Group.

## GUI Access Standards

1. LEX GUI LSR Processing:

The LEX application supported by AT&T is designed and configured for interactive transaction processing in which the CLEC interfaces with the LEX GUI on a non-mechanized basis. This application is intended for use by CLECs on a real-time basis only and any other use is neither contemplated nor supported by AT&T. A CLEC planning to utilize another method other than this or their own mechanized system to interface with AT&T for LSR ordering is advised that LSR XML is the appropriate interconnection method. Batch or mass send mode is not applicable for this application, and any CLEC requiring batch processing of LSRs should consider LSR XML for that interconnection method.

Any LEX user encountering a high volume of repetitive LEX system errors (for example, averaging more than 10 system errors per minute during a 15 minute period) is expected to log out and contact the IS Call Center to report the problem. Should the user choose instead to continue initiating the transactions that are triggering this high volume of system errors and these transactions cause a degradation of service impacting other LEX users or impacting performance measurements, then AT&T reserves the right to temporarily deactivate this user’s ID until an AT&T representative contacts the CLEC to resolve the problem. (Note that system errors are processing exceptions encountered by the LEX user and do not include LSR Local Response Rejects**.** CLECs using LEX in a real-time non-mechanized manner, will not normally encounter system errors.)

A failure by a CLEC to comply with any of the above referenced guidelines that impacts performance measurement results may result in adjustments to performance measurements penalties payable via the invocation of the appropriate subsections of the Interconnection Agreement dealing with CLEC caused impacts.

1. Verigate GUI Pre-Order Processing:

Verigate GUI pre-order processing support by AT&T is based on interactive transactions between AT&T and the CLEC. This application is intended for use by CLECs on a real time basis only and any other use is neither contemplated nor supported by AT&T. Batch or mass query mode is not applicable for this application.

A failure by a CLEC to comply with any of the above referenced guidelines that impacts performance measurement results will result in adjustments to performance measurements penalties payable via the invocation of the appropriate subsections of the Interconnection Agreement dealing with CLEC caused impacts.

## LSR XML Provisioning Activities

1. The AT&T ILEC Company CLEC Account Manager will provide the CLEC with access to the necessary forms for requesting access to send/receive LSR XML transactions and/or bulk data. These request forms identify which batch files are available via NDM or FTP. Forms for LSR XML will provide AT&T with the information to identify the CLEC and allow for sending and receiving of transactions. Any changes or additions to the CLEC side of the interface should be communicated through these forms.

1. The forms will be completed by the CLEC and returned to the AT&T ILEC Company.

1. The AT&T ILEC Company CLEC Account Manager will email the completed forms to the ISCC at ISCTECH@ATT.COM . Incomplete forms will be returned to the CLEC Account Manager for completion.

1. The ISCC will forward the forms to AT&T Corporate Information Security (CIS) to establish network connectivity and appropriate permissions.

1. The ISCC will forward the forms to the RACF Help Desk to establish RACF authority, Logon IDs and passwords.

1. The ISCC will forward the data set name, together with the Logon ID and password information to the appropriate application groups. The ISCC will email the processed forms back to the CLEC Account Manager.

# APPENDIX 5

## Miscellaneous Bulk Data Transfer (SFG) Access Standards and Requirements

Bulk data transfers may include items such as billing records, address information tables, etc. LSRs are not considered bulk data. See item 7 (pages 16 – 17) for information on LSR XML processing.

1. A CLEC may use Connect:Direct (NDM) or FTP over a Private Line or Frame Relay connection into the xRAF, to send or pull **bulk** data transfers (i.e. non-LSR files) to an AT&T ILEC company for processing. A CLEC may use Connect:Direct (NDM) or FTP over a Private Line, Frame Relay, or dial-up (FTP only) connection into the xRAF, to send or pull **miscellaneous bulk** data transfers to or from an AT&T ILEC company for processing. While both NDM and FTP are supported, it is important to note that NDM provides other value added services above standard FTP, such as checkpoint restart, confirmation of file transmission and reception, automated job scheduling, etc. AT&T utilizes the standard NDM listening TCP port 1364 to send and receive NDM transmissions.

1. The xRAF is not a store and forward service. It provides for a point of network interconnection.

1. All standards and requirements as identified in Appendixes 1 and 2 (Private Line and Frame Relay Standards and Requirements, and Dial-up Standards and Requirements) apply to miscellaneous Bulk Data Transfer Access.

## Miscellaneous Bulk Data Transfer (SFG) Provisioning Activities

1. The AT&T ILEC Company CLEC Account Manager will provide the CLEC with the necessary forms for requesting access to send/receive LSR XML transactions and/or bulk data. These forms will be supplied to the AT&T ILEC company CLEC Account Manager by the IS Call Center (ISCC). These request forms identify which batch files are available via NDM or FTP. Forms for LSR XML will provide AT&T with the information to identify the CLEC and allow for sending and receiving of transactions. Any changes or additions to the CLEC side of the interface should be communicated through these forms.

1. The forms will be completed by the CLEC and returned to the AT&T ILEC Company.

1. The AT&T ILEC Company CLEC Account Manager will email the completed forms to the ISCC at ISCTECH@ATT.COM . Incomplete forms will be returned to the CLEC Account Manager for completion.

1. The ISCC will forward the forms to AT&T Corporate Information Security (CIS) to establish network connectivity and appropriate permissions.

1. The ISCC will forward the forms to the RACF Help Desk to establish RACF authority, Logon IDs and passwords.

1. The ISCC will forward the data set name, together with the Logon ID and password information to the appropriate application groups. The ISCC will email the processed forms back to the CLEC Account Manager.

**\*\*\* NOTE: Remote Access Facility (RAF) network infrastructure that terminates dedicated point-to-point connections and that are used for dial access at the AT&T data centers are at end-of-service-life (EOSL) and end-of-support (EOS) status. Thus, the material on this page will be deprecated. \*\*\***

# APPENDIX 6

## Establish a Dial-Up Connection for TCP/IP

When using the Windows 2000 or Windows XP TCP/IP Communication's Software package, the software may be configured to communicate with the Dial-up adapter as follows. It should be noted that the actual procedures a CLEC uses for dial-up networking configuration and subsequent connection may vary somewhat from the example provided in this document.

**Creating a New Dial-Up Network Connection - Windows XP:**

* START  SETTINGS  CONTROL PANEL
* Double-click "NETWORK CONNECTIONS”
* Click on “Create a new connection” to start the New Connection Wizard
* Click the “Next Button”
* Select a Network Connection Type of “Connect to the Internet”
* Click the “Next Button”
* Select “Set up my connection manually”
* Click the “Next Button”
* Select “Connect using a dial-up modem”
* Click the “Next Button”
* Enter the Name you wish to give to the connection you are creating

e.g. AT&T xRAF (OSS Dial-Up)

* Click the “Next Button”
* Enter the number to dial
* LRAF (AT&T SOUTHWEST) – 214-800-1000
* PRAF (AT&T WEST) – 707-434-0582
* ARAF (AT&T MIDWEST) – 847-326-3890
* SRAF (AT&T EAST) – 203-495-9658
* AT&T Southeast - 205-801-5221
* Click the "Next>" button  Select “Anyone’s use”
* Click the "Next>" button
* Leave the User Name & Password entries BLANK
* Uncheck the 2 check boxes

“Use this account name and password when anyone connects to the internet from this computer”

“Make this the default internet connection”

* Click the "Next>" button
* Optionally you may check “Add a shortcut to this connection to my desktop” (Recommended for ease of use)
* Click the "Finish" button

 **\*\*\* NOTE: Remote Access Facility (RAF) network infrastructure that terminates dedicated point-to-point connections and that are used for dial access at the AT&T data centers are at end-of-service-life (EOSL) and end-of-support (EOS) status. Thus, the material on this page will be deprecated. \*\*\***

 **\*\*\* NOTE: Remote Access Facility (RAF) network infrastructure that terminates dedicated point-to-point connections and that are used for dial access at the AT&T data centers are at end-of-service-life (EOSL) and end-of-support (EOS) status. Thus, the material on this page will be deprecated. \*\*\***

 **Connecting to the xRAF:**

* Double click on the Desktop icon (resulting from creating a connection – above)
* In the Connect to…… box leave the User ID and Password fields blank and make sure the phone number is correct, and contains all necessary prefixes
* Click the “Connect” button
* **When the “after dial window” opens hit ‘enter’**  When prompted enter your User ID and NAS PW
* At the Main Menu select “1 – Establish a PPP Session”
* When Garbage starts scrolling click the “Done” button

Please direct any questions to the IS Call Center at (314) 235-7225.

**Creating a New Phone Book Entry - Windows 2000:**

* From the Desktop double-click "My Computer"

***(There is no Dial-Up Networking folder for Windows 2000. The user can click the Link that says***

***“Network and Dial-up Connections”, or they can Double-click My Network Places, and then click “Network and Dial-up Connections.)***

* Double-click "Make New Connection" for the appropriate xRAF.
* Click the “Next” Button
* Select the “Dial-up to private network”
* Click the “Next Button”
* Enter the number to dial
* LRAF (AT&T SOUTHWEST) – 214-800-1000
* PRAF (AT&T WEST) – 707-434-0582
* ARAF (AT&T MIDWEST) – 847-326-3890
* SRAF (AT&T EAST) – 203-495-9658
* AT&T Southeast - 205-801-5221
* Click the "Next>" button
* Select “For all users”  Click on “Next Button”  Enter Connection Name.
* Click the "Finish" button to return to the Dial-Up Networking Folder
* If your modem is already configured, the Dial-Up Networking Dialog appears for the connection you just created, otherwise:
* Right-click on the icon you just created and select "Properties"
* Click on the "Configure" button
* Make sure that Maximum speed is 115200 and make sure the following are checked
* Enable Hardware flow control
* Enable modem error control
* Enable modem compression
* Click the “OK” button
* Select the “Options Tab” and Check the following
* “Display progress while connecting”

**\*\*\* NOTE: Remote Access Facility (RAF) network infrastructure that terminates dedicated point-to-point connections and that are used for dial access at the AT&T data centers are at end-of-service-life (EOSL) and end-of-support (EOS) status. Thus, the material on this page will be deprecated. \*\*\***

**\*\*\* NOTE: Remote Access Facility (RAF) network infrastructure that terminates dedicated point-to-point connections and that are used for dial access at the AT&T data centers are at end-of-service-life (EOSL) and end-of-support (EOS) status. Thus, the material on this page will be deprecated. \*\*\***

* “Prompt for name and password, certificate, etc.
* “Prompt for phone number”

***(Don’t click OK here, it will take you out of the Properties setting)***

* Select the "Security" tab
* Check Typical recommended settings
* Check terminal window

***(Don’t click OK here, it will take you out of the Properties setting)***

* Click on Networking” Tab  (Click on “Properties” button)
* Click on the “Network” Tab
* Check Obtain IP address automatically
* Obtain DNS server address automatically
* Click on the “Advanced” button

**Make sure the following is checked:**

* Check Use default gateway on remote network
* Check Use IP header compression

***(Don’t click OK here, it will take you out of the Properties setting)***

* + Select the “DNS” tab
	+ Make sure the following is checked:
	+ Append these DNS (“Append Primary and connection specific DNS Suffixes” is the default. If you select “Append these DNS suffixes (in order)”, then you must also type in the DNS Suffix Name, and click the Add button)
	+ Register this connection’s address in DNS

***(Don’t click OK here, it will take you out of the Properties setting)***

* Select the “WINS” tab
* Make sure that Enable LMHOSTS lookup is checked
* Click the "OK" button
* Click the "OK" button

**Connecting to the xRAF:**

* The user clicks on the “Network and Dial-up Connections link from either My Computer, or My Network Places.
* In the “Connect to…” box leave the User ID and Password fields blank and make sure the phone number is correct, and contains all necessary prefixes
* Click the “Connect” button
* **When the “after dial window” opens hit ‘enter’**  When prompted enter your User ID and NAS PW
* At the Main Menu select “1 – Establish a PPP Session”
* When Garbage starts scrolling click the “Done” button

Please direct any questions to the IS Call Center at (314) 235-7225.

**\*\*\* NOTE: Remote Access Facility (RAF) network infrastructure that terminates dedicated point-to-point connections and that are used for dial access at the AT&T data centers are at end-of-service-life (EOSL) and end-of-support (EOS) status. Thus, the material on this page will be deprecated. \*\*\***

# APPENDIX 7

## User ID Process

AT&T utilizes a process whereby blocks of User IDs are established by AT&T and then self-administered by each individual CLEC. The Block User ID Request Form and Block User ID Guidelines are available on the CLEC Online web site <https://clec.att.com/clec/> . CLECs are to contact their CLEC Account Manager for further information regarding the forms or the process.

The following is a brief description of the guidelines and responsibilities.

**CLEC “BLOCK USER ID” GUIDELINES & RESPONSIBILITIES**

It is the responsibility of each CLEC to ensure that the CLEC User Profile information on file is up-to date and accurate. Only the applications listed on the CLEC User Profile will be eligible for access by the block User ID’s.

An AT&T CLEC User ID Access form, in Microsoft Excel format, will be used for making the request for block User ID’s. This in an electronic form that will be e-mailed to the IS Call Center and will contain the following sections to be completed by the CLEC:

Company Data Section:

* Company Name
* Point of Contact
* Address, City, State, ZIP
* Phone Number

CLEC Security Administrators (CSA’s) Section:

* Name
* Address, City, State, ZIP
* Phone
* Pager
* E-Mail Address

The CLEC CSA’s responsibilities will include:

* Administering the User ID’s within their company and specific business units.

Responsible for keeping the block User ID’s active. This can be done by rotating the User ID’s and/or accessing any unassigned User ID’s in each application at least once every 30 days.

* Will be the single point of contact to the IS Call Center for Application password resets.
* Will be responsible for identifying themselves to the IS Call Center through the use of a nine-digit number assigned to their block ID’s. The nine-digit number is assigned by the IS Call Center upon creation of the block ID’s and is verified by AT&T Corporate Information Security for uniqueness.
* Responsible for notifying the IS Call Center regarding changes to CLEC Security Administrator contact information by updating their Request Form.

CLEC User ID Access Section:

* Choose Regional Access.
* Input OCN/UNE/ACNA/CCNA Information
* Request 1 to 4 Blocks of block User ID’s for application access.
* Specify number of User ID’s requested for each block associated with specific CLEC business units.

The AT&T ISCC will receive the CLEC User ID Request Form and begin processing the initial request. A new User ID prefix will be assigned to each CLEC for their new block User ID’s. AT&T Corporate Information Security will create the “Block of Generic User ID’s” for the CLEC’s new three-character code. The initial setup of the block User ID’s requires a 10 business day setup time. Additional blocks of ID’s can subsequently be requested and will be granted based on observed usage of the existing block(s) of ID’s.

## Digital Certificates

AT&T has determined that security requirements are met when AT&T performs certification and encryption at its server level. Therefore, individual CLECs will not be required to obtain Digital Certificates from AT&T in order to access AT&T’s Uniform GUI Interfaces via the Internet.

Should AT&T decide in the future that individual Digital Certificates would be needed to secure access via the Internet, CLECs will be notified of this change. Such notification, including an explanation of the process by which AT&T would administer those individual certificates, would be made in accordance with the Change Management Process and its associated notification timelines.

# APPENDIX 8

## Data Connection Security Requirements

**Joint Security Requirements:**

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.).

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.

CLEC shall immediately notify AT&T-21STATE when an employee user ID is no longer valid (e.g. employee termination or movement to another department).

The 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.

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 CLEC’s or AT&T-21STATE’s 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.

The 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.

**Additional Responsibilities of the Parties:**

Modem/DSU Maintenance and Use Policy:

To the extent the access provided hereunder involves the support and maintenance of CLEC equipment on AT&T-21STATE’s premises, such maintenance will be provided under the terms of this document, as applicable.

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.

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.

In the event that one (1) 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.

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.

All network-related problems will be managed to resolution by the respective organizations, CLEC or AT&T-21STATE, as appropriate to the ownership of a failed component. As necessary, CLEC and AT&T-21STATE will work together to resolve problems where the responsibility of either Party is not easily identified.

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

Information security policies and guidelines are designed to protect the integrity, confidentiality and availability of computer, networks and information resources. 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 are outlined below. Questions should be referred to CLEC or AT&T-21STATE, respectively, as the providers of the computer, network or information in question.

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.

**General Policies:**

Each Party’s resources are for approved for business purposes related to the wholesale agreements in effect between the Parties.

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.

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.

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

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.

**User Identification:**

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.

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.

User IDs will be revalidated on a monthly basis.

**User Authentication:**

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.

When passwords are used for the purpose of authentication of identity, either:

1. Whenever passwords are stored, including but not limited to in automatic login sequences, scripts, source code, batch files and function keys, they must be protected using:
	1. Strong Encryption and/or one-way hashing based upon Strong Cryptography;

where:

“Strong Cryptography” means the use of cryptography based on industry-tested, accepted, and uncompromised algorithms with minimum key lengths of 128-bits for symmetric algorithms and 2048-bits for asymmetric algorithms, and proper key management practices which incorporate a documented policy for the management of the encryption keys, such as sensitive stored data and digital certificates used for Transport Layer Security (TLS), including the expiration of encryption keys and digital certificates at least once every two years, and associated processes adequate to protect the confidentiality and privacy of the keys and credentials used as inputs to the cryptographic algorithm; and

“Strong Encryption” means the use of encryption technologies based upon Strong Cryptography.

— and/or —

* 1. Appropriate access controls intended to limit access to the passwords to only the designated owner or owners of the passwords, such as through the use of file and directory/folder permissions.

— or —

1. When the requirements of #1 above are not implemented and in use:
	1. Passwords must not be stored in script files.
	2. Passwords must be entered by the user.

Passwords must be at least six (6) to eight (8) characters in length, not blank or a repeat of the user ID; contain at least one (1) letter, and at least one (1) number or special character must be in a position other than the first or last position. 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.

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

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

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

**Access and Session Control:**

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.

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.

**User Authorization:**

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.

**Software and Data Integrity:**

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.

All 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.

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

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.

**Monitoring and Audit:**

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(n) (AT&T or CLEC) 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.”*

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.

**Access to Conexus**

In the event that CLEC has, or will be provided, connectivity to AT&T’s Nonpublic Information Resources, then CLEC shall not establish additional interconnections to AT&T’s Nonpublic Information Resources without the prior written consent of AT&T and shall:

a. Use only the mutually agreed upon facilities and connection methodologies to interconnect AT&T’s Nonpublic Information Resources with CLEC’s Information Resources; and

b. If the agreed upon connectivity methodology requires that CLEC implement a Security Gateway, maintain logs of all sessions using such Security Gateway. Such session logs must include origination IP address, destination IP address, ports/service protocols used, durations of access, and sufficiently detailed information to assist with a security incident or a forensic investigation (e.g., identification of the end user or application accessing AT&T). Session logs must be retained for a minimum of six (6) months.

**Where:**

“Cloud Service” is a service delivered via an “as a Service” cloud service model (e.g., Software as a Service (SaaS), Storage as a Service (STaaS), Database as a Service (DBaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS)).

“Conexus” is the strategic corporate data network for AT&T internal company use, supporting application access from all AT&T locations. The Conexus network policies and strategies integrate with AT&T’s comprehensive IT architecture. Non-AT&T entities, such as Business Partners, Customers, Suppliers and Vendors, may only be provided access to Conexus when they are contractually bound to help secure Conexus by complying with controls, policies and requirements identical to or substantially similar to those contained within the section Access to Conexus of this document.

“Information Resource(s)” means systems, applications, websites, networks, network elements, and other computing and information storage devices, along with the underlying technologies and delivery methods (e.g., social networks, mobile technologies, laptop computers, Portable Devices, Cloud Services, data analytics, call and voice/video recording, and Application Program Interfaces (APIs)).

“Portable Devices” means media and systems, with the exception of laptop computers, capable of being easily carried, moved, transported or conveyed. Examples of such devices include tablets, USB hard drives, USB memory sticks, Personal Digital Assistants (PDAs), and mobile phones (e.g., smartphones).

“Nonpublic Information Resources” means Information Resources that are not directly accessible from the Internet.

“Security Gateway” means a set of control mechanisms between two or more networks having different trust levels which filter and log traffic passing, or attempting to pass, between networks, and the associated administrative and management servers. Examples include firewalls, firewall management servers, hop boxes, session border controllers, proxy servers, and intrusion prevention devices.

# For CLEC Hardware/Software Requirements for Access to AT&T Uniform OSS Applications

Hardware requirements are detailed in the [Uniform OSS System Requirements Matrix](https://clec.att.com/clec_documents/unrestr/hb/13%20State/227/oss/OSSRequirementsMatrix.pdf) documentation found on <https://clec.att.com/clec/hb/shell.cfm?section=1121>