

## **Guidelines for Other Service Providers (OSPs)**

- Chapter - 1 - Definitions
- Chapter - 2 - General Guidelines for OSPs
- Chapter - 3 - Guidelines for sharing infrastructure between International OSP and Domestic OSP, Use of Distributed Architecture of EPABX and Use of CUG
- Chapter - 4 - Work-from-Home/ Work-From-Anywhere
- Chapter - 5 - Security Conditions

## Chapter – 1                      Definitions

The terms used in this document, unless the context otherwise requires, have the following meaning:

1. 'Authority' means Department of Telecommunications or its designated field units (Licensed Service Areas or LSAs).
2. 'Authorized Telecom Service Providers Provisioned Virtual Private Network (VPN)' means a network formed by interconnection between OSP Centres using leased circuits/ MPLS VPN etc. from authorised Licensees, for data transfer among the OSP Centres.
3. 'Company' means an Indian Company, registered under the Indian Companies Act, 2013 or a Partnership Firm or an organization registered under Shops and Establishments Act.
4. 'Domestic OSP' means the OSP providing Services to clients located within national boundaries of India.
5. 'International OSP' means an OSP providing Services to clients located beyond national boundaries or outside India.
6. 'LLP' means a Firm incorporated and registered under Limited Liability Partnership Act-2008 in India.
7. 'Other Service Provider' (OSP) is an Indian company, registered under the Indian Companies Act, 2013 or an LLP (Limited Liability Partnership) registered under LLP Act, 2008 or a partnership firm or an organization registered under Shops and Establishment Act or a Legal Person providing voice based Business Process Outsourcing (BPO) services.
8. 'OSP Centre' means the infrastructure of an OSP at a location in India.
9. 'Point of Presence' (POP) is a location where OSP places equipment like Private Automatic Branch Exchange (PABX), Interactive Voice Recording System (IVRS) etc., to act as an extension of its OSP Centre for collecting, converting, carrying and exchanging the telecom traffic related to its services.
10. 'Telecom Service Provider' (TSP)/ Telecom Licensee means an entity who has been granted a valid licence under Section-4 of the Indian Telegraph Act, 1885 to provide Telecom Service as per the License in a Licensed Service Area (LSA).
11. 'Telecom Resource' means Telecom facilities provided by Telecom Licensees having valid license under Indian Telegraph Act, 1885 and used by the OSPs including, but not limited to Public Switched Telecom Network (PSTN), Public Land Mobile Network (PLMN), Integrated Services Digital Network (ISDN), Leased Lines to carry traffic, the telecom bandwidth etc.

## Chapter - 2 General Guidelines for OSPs

1. No registration certificate will be required for OSP centres in India.
2. Special dispensations for OSPs:
  - 2.1 For the OSPs the collection, conversion, carriage and exchange of the PSTN/PLMN/ISDN traffic over the Virtual Private network (NPLC, MPLS VPN) interconnecting the different OSP Centres is permissible.
  - 2.2 The International OSPs are allowed to carry the aggregated switched voice traffic from their POP in a foreign country to their OSP centre in India over leased line/MPLS VPN.
  - 2.3 Interconnectivity of two or more Domestic OSP Centres of the same Company or group of companies is permitted. Similarly, interconnectivity among International OSP Centres is permitted.
  - 2.4 Interconnection of Remote Agent to the OSP centre/resources is permitted.
  - 2.5 An OSP having multiple centres may obtain internet connection at a centralised location and this internet can be accessed from other OSP centres using leased circuits/ MPLS VPN.
3. The OSPs may also operate as under:
  - Work From Home (WFH)
  - Work From Anywhere (WFA) in India
  - Infrastructure sharing
  - Centralized EPABX (i.e., Distributed Architecture of EPABX)
4. NO Bank Guarantee whatsoever will be required for any facility or dispensation under these Guidelines.
5. The concept of Work-From-Home/ Work-From-Anywhere shall be treated as Extended Agent Position/ Remote Agent of the OSP.
6. Interconnectivity between OSP centres belonging to different OSP companies shall be permitted.

7. Bypass of licensed International Long Distance Operator (ILDO) and National Long Distance Operator (NLDO) jurisdiction should not take place.
  
8. EPABX at foreign location in case of international OSP will be allowed. However, the OSP will take all the necessary measures to comply with the requirements of relevant provisions of Indian laws including applicable data privacy laws. In addition, the OSP shall maintain a copy of CDR and System logs in storage at any of its OSP centres in India.

**Chapter - 3                    Guidelines for sharing infrastructure between International OSP and Domestic OSP, Use of Distributed Architecture of EPABX and Use of CUG**

1.        Sharing of the infrastructure by the Domestic OSP and International OSP is allowed.
2.        Sharing the EPABX of International OSP Centre, Domestic OSP Centre and PSTN lines for office use is permitted subject to the condition that OSP shall ensure that no bypass of the network of the Authorized Telecom Service Providers shall be caused.
3.        Use of distributed architecture of EPABX for OSP centers across India:
  - 3.1      OSPs can have a distributed architecture of EPABX (main EPABX at a centralized location and media gateways at individual OSP centers) for their OSP centers across India, where the EPABX is owned by OSP. The provisions of sharing the infrastructure would apply.
  - 3.2      OSPs shall preserve the CDRs for all the voice traffic carried using the EPABX. The CDRs shall be segregated for each media gateway.
4.        Use of Closed User Group (CUG) for internal communication of the OSP company:
  - 4.1      The interconnectivity of the OSPs is permitted for the same company or same group of companies for internal communication and for its operations.
  - 4.2      Further, the OSPs are permitted to use CUG facility for their internal communication needs.

**Chapter - 4 Work From Home (WFH)/ Work From Anywhere (WFA)**

The concept of Work-From-Home will be encouraged under these guidelines. The WFH has been extended to provide Work-From-Anywhere in India. This facility of Extended Agent/ Remote Agent Position (i.e. Work-From- Home/ Anywhere) is permitted with the following conditions:

1. The agents at home shall be treated as Remote Agents of the OSP Centre and interconnection is permitted.
2. The Remote Agent is also allowed to work from any place within India.
3. OSP shall be responsible for any violation related to toll-bypass.

**Chapter - 5                      Security Conditions**

1. For EPABX installed at locations different than the OSP Centre, the remote access of all CDRs, access log, configurations of EPABX and routing tables shall be made available on demand from Authority/ Law Enforcing Agencies from at least one of the OSP centres.
2. The location of EPABX and client's Data Centre of Domestic OSPs shall be within India.
3. The OSP shall not engage in the provision of any Telecom Services.
4. On specific instances of infringements such as carriage of objectionable, obscene, unauthorized messages or communications infringing copyright, intellectual property etc. in any form on their networks, the OSP shall ensure that the carriage of such material on the networks is prevented immediately.
5. The OSP shall extend support to the Authority in tracing any nuisance, obnoxious or malicious calls, messages or communications transported through its equipment and network.
6. OSPs shall be required to preserve the CDRs for all the voice traffic carried using the EPABX. The CDRs shall be segregated for each media gateway. It shall be possible to view the CDR data along with details of the agent manning the position by remote login to CDR machine/ server. The time-stamp in the CDRs in the system(s) of the OSP shall be synchronized with the Indian Standard Time.
7. In all the above cases, CDRs / UDRs / System logs, etc. shall be maintained for a period of one year.
8. For Work-From-Home/ Work-From-Anywhere, the OSP shall ensure that the system logs are tamper-proof and the CDRs/ all logs of the activities carried out by the Extended Agent shall be maintained for one year.