Broadband Cell, 2nd Floor,
Bharat Sanchar Bhawan, Janpath,
New Delhi
Ph. 011-23316882
Fax. 011-23734052

भारत संचार निगम लिमिटेड
(भारत सरकार का उपक्रम)
BHARAT SANCHAR NIGAM LIMITED
(A Govt. of India Enterprise)

BSNLCO/GM(BB)/72-13/09- Broadband dated 11-09-09

To
All Heads of Circles/ Metro Districts

Sub: Implementation of Wi-Fi security Instructions

Ref: SP cell letter BSNLCO/SP/WiFi/2008-09/ dated 12/08/09 addressed to all CGMs

[1]. Kindly refer to the above subject. Also find enclosed the instructions issued by DOT on the Wi-Fi security.

[2]. **Intimation to Internet Leased line Customers:**

a. You may intimate all the Internet Leased line customers about the security to be followed in the Wi-Fi network. The customers may be intimated at regular intervals through mails or by printing in bills about the importance of securing the Wi-Fi internet facility.
b. Internet Leased Line (ILL) customers may also be intimated that they shall set up their own centralized authentication with necessary logs in case they use Wi-Fi Network for further distribution of internet bandwidth within their premises.
c. A sample letter/mail to be addressed to the Internet Leased Line customers is enclosed herewith.

[3]. Intimation to Broadband Customers:

a. You may intimate all the Broadband customers about the security to be followed in the Wi-Fi network. The customers may be intimated at regular intervals through mails or by printing in bills about the importance of securing the Wi-Fi internet facility.
b. All the Wi-Fi CPE's are to operate on secure mode only. The customers will be using Wi-Fi facility either using the Type-II/Type-IV ADSL CPE provided by BSNL or though installation of external Wi-Fi devices procured by them.
c. A sample letter/mail to be addressed to the Broadband customers is enclosed herewith.

[4]. Centralised Registration:

a. Customers who have Wi-Fi devices procured by them shall intimate BSNL through a centralized registration mechanism. The P3 Portal is being modified by the Broadband Network Circle for allowing the customers having Wi-Fi facility for registration. You will be intimated the moment the modification is completed in the P3 Portal. A letter written to this effect to CGM(BNW) Circle is enclosed

Endst No: - CGMT/HR/Broadband/508 Dated at AB 05-10-09

Copy forwarded to:-

1 ALL SSA Heads, Haryana Telecom Circle for information & necessary action please.

2. AD(IT) o/o CGMT, Circle office, Ambala for necessary action please

AD (BB-Plg)
O/o CGMT HR Ambala

b. Once the customer registration facility starts, customers are also to be intimated that, in case they are using Wi-Fi facility procured by them, their internet services will be disconnected, if they fail to register. The registered customers are to be checked whether they are using the Wi-Fi device in the secure mode. If not they have to be advised to do so. Else they shall be advised not to use the Wi-Fi device as the same is not meeting the national security requirements.

[5]. Centralised Authentication:

a. Centralised authentication with unique username/password is another requirement for the Security. For this BSNL shall have centralised authentication mechanism.
b. Centralised authentication mechanism through 802.1X standards is being tested in the NOC.
c. Once the centralised authentication is implemented, all the Wi-Fi enabled CPE's shall be configured to work through the centralised authentication mode only.
d. Detailed instructions will be issued once the testing is completed.

[6]. Customer Acquisition Forms:

a. Following clause may be added in all the Internet, Broadband and Internet Leased Line Customer Acquisition Forms: "In **case the customer wishes to deploy his own Wi-Fi based distribution of internet within the premises, the same shall be activated only after the same is registered with BSNL and secure centralized authentication enabled with BSNL. Please be informed that BSNL will not be in any way held responsible or answerable in case any such unauthorized usage of Wi-Fi technology is detected within your campus by the concerned authorities resulting in the non-compliance of the DoT order dated 23-02-09. The Authorities may include the Department of Telecommunications (DoT), TERM Cells of DoT, Local and all other Law Enforcement Agencies (LEAs) and any such other authority. Please note that any liability, including civil and criminal, for such unauthorized use and any resulting event connected thereto will be your sole responsibility. BSNL would also be constrained to suspend our services without any further notice in such an eventuality and without any liability on our part."**

(R. Saji Kumar)
DGM(NWP-I) CFA

Copy to :

(1) CGM, Broadband Network, New Delhi
(2) CGM, STR, Chennai
(3) GM, BNW, Bangalore
(4) DGM , STR, NOC, Bangalore

Broadband Cell, 2nd Floor,
Bharat Sanchar Bhawan, Janpath,
New Delhi
Ph. 011-23316882
Fax. 011-23734052

भारत संचार निगम लिमिटेड
(भारत सरकार का उपक्रम)
BHARAT SANCHAR NIGAM LIMITED
(A Govt. of India Enterprise)

BSNLCO/GM(BB)/72-13/09- Broadband dated 11-09-09

To

CGM (BNW New Delhi /Karnataka circles)

Sub: SP cell letter BSNLCO/SP/WiFi/2008-09/ dated 12/08/09 addressed to all CGMs

[1]. DoT vide letter no 820-1/2008-DS Pt.II dated 23/02/09 copy enclosed has issued guidelines for security under the Wi-Fi frequency Band. Customers will be having Wi-Fi facility either using the Type-II/Type-IV ADSL CPE provided by BSNL or though installation of external Wi-Fi devices procured by them.

a. BSNL has to implement centralized authentication of Wi-Fi customers using unique username/password without multiple logins for all such cases.
b. BSNL has to implement centralized registration facility for those customers (Broadband and Internet Leased Line) having their own Wi-Fi equipments.
c. Once the customer registers in the centralized registration facility, the field units shall visit his premises to check whether the device supports centralized authentication mechanism.
d. If the device is not supporting the centralized authentication mechanism, the field units have to advice the customers not to use the Wi-Fi device.
e. The centralized registration facility shall allow the customer to request for additional usernames also.

[2]. The following modifications are required in the P3 Portal

a. Facility for customers having their own Wi-Fi device to register
b. Facility for field units to view the registered customers
c. Facility for field units to submit their inspection/advice report
d. Facility for customers to request for additional usernames and creation of such usernames in the Servers.

[3]. The centralized authentication:

a. This is to be implemented through IEEE802.1x method.
b. The Multiplay network deployed has 802.1x based authentication supported in the BNG and the AAA servers.
c. The Type-II Wi-Fi CPE shall have only 802.1x based authentication.
d. This authentication acts as a second authentication other than the PPPoE authentication.
e. The Wi-Fi CPE will get the second authentication through the BNG from the AAA Server. The AAA will get the username/password information from the LDAP.

f. You may immediately enable the 802.1x based centralized authentication in the BNG & AAA Servers and the same may be tested for the Wi-Fi enabled CPEs.

g. Moreover for implementing this centralized authentication, in case any additional Server Hardware or Licenses are required for the AAA & LDAP, the same may be communicated at the earliest for inclusion in the Multiplay Phase-III procurement.

[4]. All the various Makes/Models of Type II CPEs may be tested for 802.1x based authentication & report on the same may be sent to this office.

[5]. In the 802.1x based authentication customer shall not be provided multiple simultaneous login on the same user ID & Password. The Ist user ID & Password can be the same as the PPP username/password. Necessary portal modification may be carried out for asking for customers additional User ID & Password (for those who are having more than one laptop)

[6]. All the CPEs suppliers have to modify the firmware for the CPE GUI such that GUI supports only 802.1x based wireless authentication. This is applicable to all the existing & new CPEs supplies.

Encl: a/a

(R Saji Kumar)
DGM(NWP-I) CFA

Copy to : (i) CGM, STR, Chennai
(ii) GM,BNW, Bangalore
(iii) GM(D), Karnataka Circle
(iv) DGM, STR, NOC, Bangalore

Government of India
Ministry of Communications & IT
Department of Telecommunications
Sanchar Bhawan. 20. Ashoka Road. New Delhi - 110 001
(AS-II Cell)

No 842-725/2005-VAS **Dated: 23.02. 2009**

To

All UASL/CMTS/BASIC Service Providers

Subject: Instructions under the UASL/CMTS/BASIC Service Licence regarding provision of Wi-Fi Internet service under delicensed frequency band

In the recent past concerns have been raised that Wi-Fi Networks were being misused by anti-social elements. Insecure Wi-Fi networks are capable of being misused without any trail of user at a later date. In order to address the issue related to insecure Wi-Fi network, all the UASL/CMTS/BASIC Services providers are hereby instructed to follow the following procedure for the secure use of Wi-Fi services under the delicensed frequency band in the interest of security of the nation with immediate effect:

(I) (a) Internet services (wired/wireless) provided by Licencee to new Subscriber

(i). Licencee will ensure a registered and secure Internet service including Wi-Fi connectivity through user Login ID and password to all the subscribers with central authentication mechanism.

(ii). Licencee shall deploy suitable Customer Premises Equipment (CPE) for wired / wireless internet connectivity at subscriber

end, keeping in view the further deployment of Wi-Fi connectivity for implementing the (i) above.

(iii). Licencee shall ensure that unique user ID and Password do not have provisions for simultaneous multiple logins. Licencee may give more than one user ID and Password to a single subscriber for multiple usage for his internet account.

(iv). Licencee shall put a clause in Subscriber Agreement of new subscribers that any Wi-Fi connectivity deployed by subscriber has to be activated only after it is registered for centralized authentication with the Licencee.

(b) Wi-Fi services provided at public places i.e Hotels, Restaurant, Airports Malls, Shops, Railway Stations through hotspot.

(i). Licencee shall create bulk Login IDs at each Wi-Fi hotspot location for controlled distribution. The authentication shall be done at a centralized server only which could be a POP location of the service provider.

(ii). Licencee or its Franchisee shall register the Subscribers for providing temporary Login ID and password for the use of public Wi-Fi spot through either of the following methods:

a. Retaining a copy of Photo Identity of the subscriber with Licencee which shall be preserved by the Licencee for a period of one year.

b. Provisioning of Login-ID and Password through SMS on subscriber's mobile phone through automated process and keeping mobile number of subscriber as the identity of the internet subscriber with reference to

Login-ID provided for a period of one year. In such cases, photo identity may not be necessary.

(c) Internet subscriber on Lease Lines

(i). Licencee will direct and take compliance from Leased line based internet subscribers to setup and maintain centralized authentication themselves for Internet Services including Wi-Fi usage. Leased line based internet subscribers shall also have the option to get the centralized authentication for their internet usage by the respective Licencee.

(d) Wi-Fi services deployed by existing subscriber

(i). Licencee shall ensure compliance to Para (I)(a)(i) to (I)(a)(iii) for all existing Wi-Fi customers who have taken Wi-Fi services from the Licencee.

(ii). Licencee will inform their Internet subscriber about registering Wi-Fi connectivity with Licencee through monthly bills, emails etc. at regular interval.

(iii). Efforts shall also be made to create awareness among public for using registered Wi-Fi connectivity.

(iv). Licencee shall direct its existing Internet subscribers, including those who have deployed Wi-Fi routers themselves, to get the Wi-Fi Internet connectivity registered with Licencee within four months.

(v). If it comes to the notice of Licensee that the internet subscriber has not registered with the licensee and is using Wi-Fi connectivity, Licensee is hereby directed to suspend the

internet services to such subscribers till they are registered with the Licencee.

(II) Para I(a)(i) to I(a)(iii) shall also be applicable for provisions in Para (I)(b)&(c) also. All the above actions shall be implemented within four months.

23.2.04.
(B L Pawar)
ADG(VAS-II)

Copy to:

1. Secretary, TRAI, New Delhi
2. Wireless Advisor, WPC Wing, New Delhi
3. DDG(Security), DoT, New Delhi
4. DDG(AS-I), DoT, New Delhi
5. DDG(DS), DoT, New Delhi
6. DDG(C&A), DoT for posting on the DoT website

<<Letter to Internet Leased Line Customers>>

Date 11-09-2009

Dear Customer,

Sub.: Important DoT Notification requiring your action

BSNL has been providing you Internet Leased Line (ILL) services, as per terms and conditions of the service, enabling you to access internet.

Due to recent cases of misuse of internet by anti-social and anti-national elements, especially through unlicensed band of Wi-Fi technology at customer premises, the Department Of Telecom (DoT) has issued a notification on 23-02-09(No 820-1/2008-DS Pt.II dtd 23-02-09) for ensuring secure use of Wi-Fi based internet access under the de-licensed frequency band. A copy of the said instructions is available on the DoT web site http://www.dot.gov.in/ We request you to peruse the entire document for necessary actions.

In accordance with the above instructions from DOT, **you are requested to kindly intimate us within one month from date of this mail**, whether the internet access provided to you through our ILL service is being used to run a Wi-Fi network for further distribution within your campus/location/organization.

In case you are using Wi-Fi technology at your premises, you are required to set up and maintain centralized authentication for your internet usage / Wi-Fi services and confirm compliance to the DoT instructions in writing within a month from the date of this email.

Please note that in case, we do not receive any reply from you within the stipulated time period., we will have to presume that you have ensured that the internet access service provided to you is **NOT being used in whatsoever manner for enabling** further Internet access within your campus/location/organization or to your customers, either on a paid or free basis, through application of Wi-Fi technology without secure mode and central authentication. Any resale of bandwidth through any technological means shall require compliance of DoT guidelines and instructions that are mentioned in the above link. .

Please be informed that BSNL will not be in any way held responsible or answerable in case any such unauthorized usage of Wi-Fi technology is detected within your campus by the concerned authorities resulting in the non-compliance of the DoT order dated 23-02-09. The Authorities may include the Department of Telecommunications (DoT), TERM Cells of DoT, Local and all other Law Enforcement Agencies (LEAs) and any such other authority. Please note that any liability, including civil and criminal, for such unauthorized use and any resulting event connected thereto will be your sole responsibility. We would also be constrained to suspend our services without any further notice in such an eventuality and without any liability on our part.

Thank you for your immediate response and co-operation on this issue in the interest of national security. We look forward to being your partner for all your telecom requirements.

Thanking you,

Yours faithfully,

Customer Service,
BSNL

<<Letter to Broadband Customers>>

Date 11-09-2009

Dear Customer,

Sub.: Important DoT Notification requiring your action

BSNL has been providing you Broadband services, as per terms and conditions of the service, enabling you to access internet.

Due to recent cases of misuse of internet by anti-social and anti-national elements, especially through unlicensed band of Wi-Fi technology at customer premises, the Department Of Telecom (DoT) has issued a notification on 23-02-09(No 820-1/2008-DS Pt.II dtd 23-02-09) for ensuring secure use of Wi-Fi based internet access under the de-licensed frequency band. A copy of the said instructions is available on the DoT web site http://www.dot.gov.in/ . We request you to peruse the entire document for necessary actions.

In accordance with the above instructions from DOT, **you are requested to kindly intimate us within one month from date of this mail**, whether the internet access provided to you through our Broadband service is being used to run a Wi-Fi network for further distribution within your location using any Wi-Fi devices other than the ones provided by us.

In case you are using Wi-Fi technology at your premises, (Either provided by us or acquired by you) you are requested to configure the modem in the secure mode only with username/password in order to prevent any unauthorized use. In case of any difficulty, we are pleased that you may contact our customer service center for assistance.

Please note that in case, we do not receive any response from you within the stipulated time period., we will have to presume that you have ensured that the internet access service provided to you is **NOT being used in whatsoever manner for enabling** further Internet access within your campus/location/organization or to your customers, either on a paid or free basis, through application of Wi-Fi technology without secure mode. Any resale of bandwidth through any technological means shall require compliance of DoT guidelines and instructions that are mentioned in the above link. .

Please be informed that BSNL will not be in any way held responsible or answerable in case any such unauthorized usage of Wi-Fi technology is detected within your premises by the concerned authorities resulting in the non-compliance of the DoT order dated 23-02-09. The Authorities may include the Department of Telecommunications (DoT), TERM Cells of DoT, Local and all other Law Enforcement Agencies (LEAs) and any such other authority. Please note that any liability, including civil and criminal, for such unauthorized use and any resulting event connected thereto will be your sole responsibility. We would also be constrained to suspend our services without any further notice in such an eventuality and without any liability on our part.

Thank you for your immediate response and co-operation on this issue in the interest of national security. We look forward to being your partner for all your telecom requirements.

Thanking you,

Yours faithfully,

Customer Service,
BSNL