National Institute for Research in Tuberculosis
Mayor V R Ramanthan Road
Chetput, Chennai 600031

Wireless Access Request Form

PLEASE NOTE: ALL PAGES OF THIS FORM ARE TO BE FILLED OUT BY A SUPERVISOR AND SIGNED. The form should be forwarded with Director/DIC Approval.

For assistance, please contact the EDP Help Desk at 9672. Once completed, please forward to EDP

Wireless Access:

Applicant Information:
(Print clearly or form can not be processed)

Today's Date: ____ / ____ / ____

Initial: ____________________ Name: _____________________ Phone: _______________
(if available)

Work Unit: ____________________ HOD Name: ________________________________

Status: *(Check one on each line)*

□ Staff □ Student □ Other: _______________________________________

□ Official Laptop □ Personal Laptop* Laptop MAC ID____________________

HOD Signature:

X____

Director/Director In-charge Signature:

X____

***The personal laptop should have Genuine/Licensed Operating System/Software's. The system should be mandatorily protected with Licensed Antivirus/Endpoint Security Solutions. If this requirement is not available in the laptop, the Wi-Fi connection will not be provided.**

Cont'd..2

IMPORTANT – Applicant must read, sign, and date this section. If this section is not signed and dated accounts cannot be provided access.

Accountability-General Requirements

Computer and Internet Users (Users):

- Users should behave in an ethical, proficient, informed, and trustworthy manner.
- Do not attempt to override technical or management controls (i.e., carrying sensitive data home on a usb/pendrive without prior approval, etc.).
- Use only systems, software, and data for which you have authorization and use them only for official business.
- Report security incidents, or any incidents of suspected fraud, waste or misuse of NIRT systems to appropriate officials.
- Protect passwords from access by other individuals. Never share or compromise your password. Make alternative provisions for access to information during your absence to avoid the sharing of passwords.
- Change passwords frequently. The frequency should be commensurate with the risk and criticality of the system, but should be no less often than every 90 days.
- Protect confidential and/or sensitive information from disclosure.
- Protect government property from theft, destruction, or misuse.
- Do not remove computers from NIRT premises unless authorized in accordance with NIRT property management requirements.
- Use the Internet for official business purposes only during normal work hours.
- Report any security incidents to the appropriate officials.
- Do NOT send highly sensitive information via e-mail or fax, unless encrypted.
- Protect copyrighted software and information in accordance with the conditions under which it is provided.
- Grant access to systems and data only to those who have an official need to know.
- Do not use your trusted position and access rights to exploit system controls or access data for any reason other than in the performance of official duties.
- The provision of internet access is the responsibility of designated personnel in the IT group. Users may not install connections to the internet or other networks or service providers.
- Users may not install network infrastructure equipment such as hubs, switches, routers, wireless access points, etc.

Applicant Name:

____

(Please Print)

Applicant Designation:

____

Applicant Signature:

_________ ________________________________

Date: ____ / ____ / _____