Draft Policy for
Usage of Wireless Network (Wi-Fi)
In the offices
Of Punjab Government

Government of Punjab

Department of Governance Reforms,
SCO 193-195, Sector-34A,
Chandigarh-160022

Date of Issue : …….

1.0 Purpose to the Policy

This policy establishes principles and requirements that govern the installation, configuration and acceptable use of user-installed wireless (Wi-Fi) access points (APs) across departments, corporations, boards and commissions of Government of Punjab.

2.0 Definitions

2.1. Access Point/Wireless (Wi-Fi) Access Point (AP): A device that allows Wi-Fi devices to connect to a wired network.

2.2. User-Installed Access Point: A non-ITS installed/managed access point.

3.0 Detailed Policy Statement

3.1. Background: Unsecured Wi-Fi network (commonly known as Wireless Local Area Network or WLAN) is an extremely serious security hazard for any network. Any unauthorized access, get access not only to internet bandwidth but can send e-mails, download classified and/or confidential data/information, upload obscene material, hack into networks, initiate attack on other computers in the network or connected to internet, send malicious code to others, install a Trojan or botnet on the victim's computer to get long-term control of it.

3.2. Objective of the policy: The policy has been framed with an objective to provide guidelines for the acceptable and authorized use of wireless network across the office(s) of Government of Punjab. The policy framework specifies minimum requirements however departments may elect to apply more stringent standards and/or guidelines.

3.3. Usage Policy: All devices, regardless of location or ownership, must satisfy the following minimum network connectivity requirements, as appropriate, before connecting to the Wi-Fi network. Additionally, devices known to be vulnerable, to present a security risk, or to be infected with malicious software must not be connected to the Wi-Fi network or to devices on the Wi-Fi network.

Devices not meeting these requirements are subject to being blocked or disconnected from the Wi-Fi network.

4.0 Scope of the Policy

4.1. The policy is applicable to all the authorised users Wi-Fi service installed in the office(s) of Government of Punjab

4.2. The Policy applies to the use, for the purpose of sending or receiving data through the wireless network.

4.3. The policy applies to all Wi-Fi setup configured in the office(s) of Government of Punjab.

4.4. The policy provides the standards of appropriate, acceptable and authorized use of the wireless network services provisioned by departments, corporations, boards and commissions of Government of Punjab.

4.5. The authorised user from various departments of Government of Punjab is bound by the relevant Policies and Regulations contained in the policy.

4.6. The existing policy supersedes any other policy previously approved and implemented.

5.0 Security Standards

5.1. User-installed Wi-Fi access points (APs) must be configured to use cryptographic keys or other standard access control methods to ensure that only authorized officials can connect to the Wi-Fi service. In case of requirement of extension of Wi-Fi service to the guest users, the Wi-Fi router should provision for separate security and access provisions thereby separating Wi-Fi service access to authorized officials and guest users.

5.2. User-installed Wi-Fi access points (APs) must be configured to provide a facility for MAC Authentication or MAC binding to allow the registration of the MAC address of the user device(s) in the wireless router, for which the access is to be allowed. This is an additional security measure for securing the access to the router.

5.3. The encryption of wireless devices should be WPA2 or higher.

6.0 Use of the Service

The use of the Service and any activities conducted online through the Service should adhere to IT Act 2000 and IT Act (Amendment) 2008, all laws, rules, regulations and statutory guidelines issued by Government of Punjab and Government of India time to time. The use of the Service for the following activities is prohibited:

6.1. **Spamming and Invasion of Privacy**: Sending of unsolicited bulk and/or commercial messages over the Internet using the Service or using the Service for activities that invade another's privacy.

6.2. **Obscene or Indecent Speech or Materials**: Using Services to advertise, solicit, transmit, store, post, display, or otherwise make available obscene or indecent images or other materials.

6.3. **Defamatory or Abusive Language**: Using the Service to transmit, post, upload, or otherwise making available defamatory, harassing, abusive, or threatening material or language that encourages bodily harm, destruction of property or harasses another.

6.4. **Forging of Headers**: Forging or misrepresenting message headers, whether in whole or in part, to mask the originator of the message.

6.5. **Hacking**: Accessing illegally or without authorization computers, accounts, equipment or networks belonging to another party, or attempting to penetrate security measures of another system. This includes any activity that may be used as a precursor to an attempted system penetration, including, but not limited to, port scans, stealth scans, or other information gathering activity.

6.6. **Distribution of Internet Viruses, Trojan Horses, or Other Destructive Activities**: Distributing information regarding the creation of and sending Internet viruses, worms, Trojan Horses, pinging, flooding, mail bombing, or denial of service attacks. Also, activities that disrupt the use of or interfere with

the ability of others to effectively use the Node or any connected network, system, service, or equipment.

6.7. **Facilitating a Violation of this Agreement of Use**: Advertising, transmitting, or otherwise making available any software product, product, or service that is designed to violate this Agreement, which includes the facilitation of the means to spam, initiation of pinging, flooding, mail bombing, denial of service attacks, and piracy of software.

6.8. **Other Illegal Activities**: Using the Service in violation of applicable law and regulation, including, but not limited to, advertising, transmitting, or otherwise making available ponzi schemes, pyramid schemes, fraudulently charging credit cards, pirating software, or making fraudulent offers to sell or buy products, items, or services.

6.9. **Resale**: The sale, transfer, or rental of the Service to customers, clients or other third parties, either directly or as part of a service or product created for resale.

7.0 Requirements for Network Connectivity of Wi-Fi Devices

7.1. **Access Control Measures**: Shared-access systems must enforce password or other authorization/authentication standards whenever possible and appropriate. In situations where systems ship with default passwords for network accessible devices, those passwords should be changed upon first use.

7.2. **Encrypted Authentication**: To protect against surreptitious monitoring of passwords. Suitably strong encryption shall be employed when passwords are transmitted over a network. Network traffic may be surreptitiously monitored, rendering these authentication mechanisms vulnerable to compromise. Encryption-capable services, such as SSH, SFTP, SCP, SSL, HTTPS, POPS, and IMAPS, may be used to meet this requirement.

7.3. **Patch Management Practices**: To ensure timely update of security patches, the networked devices shall run latest stable version of operating system and application software for which security patches are made available, and these

should be installed in a timely fashion. Exceptions may be made for patches that compromise the usability of critical applications following exception procedures. Implementation of additional measures may be required when exceptions are granted.

7.4. **Malicious Software Protection**: To protect networked devices from malicious software, such as viruses, spyware, and other types of malware. When readily available and as appropriate for specific operating systems, software to detect viruses and other malware shall be running, up-to-date, and have current virus definition files installed on all network devices as appropriate.

7.5. **Removal of Unnecessary Services**: To prevent surreptitious use of services not needed for the intended purpose or operation of the device. If a service is not necessary for the intended purpose or operation of a device, it shall not be running on that device; such services should be disabled, turned off, or removed.

7.6. **Session Timeout**: To prevent unauthorized access to restricted or essential services or devices left unattended for an extended period of time. Devices that access restricted and/or essential services that are left unattended for an extended period of time shall employ measures, such as session timeout or lockout mechanisms, that require re-authentication before users return to interactive use. Devices that host confidential or critical information may be subject to additional requirements.

8.0 Procedures for Blocking Network Access

Authorized network personnel's must take immediate action to address any threats that may pose a serious risk to network. For services hosted remotely, authorized network personnel's will work with the service provider to address the threat.

8.1. Authority

Authorized Network personnel have the authority to evaluate the seriousness and immediacy of any threat to network and to take action to mitigate that threat. Action that is taken will be responsible and prudent based on the risk

associated with that threat and the potential negative impact to the network caused by making the offending device(s) and/or account credentials (e.g. passwords) inaccessible. Examples of threats that will trigger blocking are:

8.1.1. The level of network activity is sufficiently large as to interfere with the normal business activity of the office.

8.1.2. Privileged access has been acquired by an unauthorized person.

8.1.3. An attack on another computer or network has been launched.

8.1.4. Confidential, private or proprietary electronic information or communications are being inappropriately collected.

8.1.5. Complaints have been received and verified regarding inappropriate activity or the system exhibits a high-risk vulnerability.

8.2. Notification procedure

8.2.1. The intent of Authorized network personnel who operate under these guidelines is to work cooperatively with departments in blocking network access. The practice shall be to notify Nodal officers of the departments prior to blocking in order that they may address the problem in a timely and appropriate manner. If the threat is immediate, or the impact is severe, as evaluated by network personnel, the offending device(s) will be blocked immediately and notification will be sent to the Nodal officers of the concerned departments', as appropriate regarding the threat.

8.2.2. If the threat is not immediate, or the impact is acceptable, notification of the threat shall be sent to the Nodal officers of the concerned departments', as appropriate. If a response is not received within 2 days indicating that the department is taking action to mitigate the threat, the offending device(s) will then be blocked.

8.2.3. In either case, if a block has been put in place it will be removed when the Nodal officers of the concerned departments and network personnel agree that the problem causing the incident has been addressed.

8.3. Recourse for blocked network access

If a department believes that a device has been inappropriately blocked it may request a review of the decision

9.0 Audit of Wireless Network

Department of Governance Reforms is the nodal agency to audit the Wi-Fi installations. Each department after configuration and implementation of wireless network shall inform Department of Governance reforms. Department of Governance Reforms shall Audit the wireless network and certify the installation.

10.0 Wi-Fi device security

10.1. Wi-Fi device administrator Usernames and Passwords:

Issue: The username and password are required to allow your computer / device to connect to wireless router and get access to the network. All hardware manufacturers usually provide default Usernames and Password combination as default factory setting.

Risk: The default usernames and password combination are usually common for different manufactures devices and are available on the internet and product manuals. Hackers can effortlessly break into your Wi-Fi network by just knowing the brand and model of your Wi-Fi router. Even beyond that hackers can change your Username and password and not only control your wireless connection but deny you the usage of the network itself.

Risk Mitigation: The default username and password of the Wi-Fi device shall be changed after the installation. The password must be a combination of alphabets, special characters and numbers and should be minimum 8 characters long. For example a real difficult-to-break passwords can be Ahr34$d92 or 7%rEc@bb.

10.2. Wi-Fi device Encryption

Issue: Information flow between wireless router and computer /device is encrypted. The old encryption standard 'Wired Equivalent Privacy' (WEP), is claimed to be broken within few seconds, even if using a complex passphrase. WEP encryption is now so simple to hack that it is considered as slightly better than no encryption at all. A weak encryption means it can be easily broken within manageable time, i.e. few seconds or minutes. 'Wi-Fi Protected Access-2' (WPA2) encryption is highly difficult to break, even with the help of highly powerful computers. The usage of WEP encryption may be due to (a) either the user is unaware / not bothered of the problem or (b) feel technology to upgrade to WPA / WPA2 is complex.

Risk: Statistically a very large percentage of Wi-Fi users are still using default configured WEP encryption technology to encrypt their information, even though highly superior WPA and WPA2 encryption standards are easily available. If the encryption is weak, a hacker can easily break the encryption, tap into the network and monitor all data flow and your activities.

Risk Mitigation: The encryption of wireless devices shall upgrade to WPA2.

10.3. Enable and use firewall

Issue: A typical IT security has different layers of security. No single layer of security is enough to survive various types of attack. Adding layers of security will ensure that attacks by hackers, Trojans, spyware and malware are resisted and mostly defeated.

Risk: Routers come with a built-in firewall but is either disabled or turned off.

Risk Mitigation: Enabling router's firewall can mitigate the risk. Enable all related built-in security features in the firewall. These features include to block anonymous internet requests or pings; browsing unwanted websites; defining MAC addresses; protect from malware and spyware; etc. This additional layer of security will protect Wi-Fi network not only from hackers and unwanted preying eyes but also from malicious software.

10.4. Use static IP addresses in the devices

Issue: Most of the devices on the network use dynamic IP addresses assigned to them using a DHCP server by Network Management Team.

Risk: It is very convenient to define dynamic IP address assignment in any network. At the same time, this will also work to the advantage of the hacker. The hacker's device will also be assigned a dynamic IP address and thus get connected to the network.

Risk Mitigation: Turning off Dynamic IP Address or "Obtain IP Address automatically" or DHCP (Dynamic Host Configuration Protocol) in the configuration can mitigate the risk.

10.5. Changing the Default System ID (SSID)

Issue: Wireless router come with a default system identifier (ID) called the SSID (Service Set Identifier) or ESSID (Extended Service Set Identifier). This ID is also commonly known as the name of your Wi-Fi network.

Risk: Though knowing the SSID does not allow a hacker to break into Wi-Fi network, it is usually considered that the person has not taken due precautions to protect their wireless network. Thus the wireless networks with default SSID are the most common targets of attacks.

Risk Mitigation: Changing the default SSID to a meaningful name can mitigate the risk.

10.6. Disable Public Broadcasting of your SSID

Issue: One of the features of the wireless router is to broadcast its SSID at a regular interval. This is to enable the connecting device to know the network to get connected. This is a vulnerability wherein information about wireless network set-up can be exposed.

Risk: The regular broadcast of SSID over air confirms existence of network and thus is vulnerable to hacking attacks.

Risk Mitigation: Disabling broadcasting network SSID by the router can mitigate the risk of exposing wireless network.

11.0 Interpretation & Modification of Policy

11.1. This Policy shall be valid for five years from the date of issuance of this policy.

11.2. Department of Governance Reforms reserves the right to bring any amendment, addendum, modification, revision etc. to this policy. Changes in the regulatory framework, technology, as well as market and technological advances may require revisions to this policy to keep the requirements and guidelines updated with the prevailing environment.

12.0 Effective Date:

12.1. This policy will be applicable with immediate effect.

13.0 Approval

13.1. This policy has been approved by the Council of Ministers as conveyed by the Department of General Administration Punjab vide their letter number < >, dated < >.

****

