STATE OF NEW HAMPSHIRE
DEPT OF INFORMATION TECHNOLOGY OPERATIONS

HOME WIRELESS CONFIGURATION GUIDELINES

Standard #:	NHS0026.02.2021.v2
Impact:	Statewide
Effective Date:	02/05/2021
Created Date:	06/04/2010
Last Reviewed Date:	02/05/2021
Last Revised Date:	02/05/2021
Status:	FINAL
Owner:	OPERATIONS

1. PURPOSE

This purpose of this policy is to establish configuration guidelines for home wireless networks used by authorized remote users accessing state resources managed by the Department of Information Technology (DoIT).

2. POLICY

When configuring your home wireless network, these standards must be followed within the limits of the network device being used.

- Change the default manufacturer admin password to a strong password at least 12 to 20 characters in length and containing special characters.
- Change the default Service Set Identifier (SSID) wireless name to something unique that does not contain revealing or identifying information.
- Designate a strong SSID passkey; provide only to those you authorize.
- Enable Wi-Fi Protected Access encryption (WPA2/WPA3). Use a strong password at least 12 to 20 characters in length and containing special characters. WEP Encryption is not allowed to access State resources. Change the password on a regular basis.
- Secure device from unauthorized users.
- Turn off the “plug ‘n play” feature on the router. The way the “plug ‘n play” service works creates an opportunity for unauthorized access and is best kept off if your network can function without it.
- Some home wireless routers have a firewall feature and if yours does it must be enabled and set to block inbound connections.
    - Turn off remote management of your router so that service is not listening for connections.
- We strongly suggest that you enable MAC-Address filtering to prevent unauthorized access. Most devices have that function, although your system may use a different terminology, for example the Netgear Orbi systems call it “Access Control”.
- Check for and update your firmware on a regular basis, we recommend monthly or sooner if your wireless router has a newly discovered vulnerability.
- Check on port 32764. This is a port used for firmware updates and has been known to be hacked. You can check to see if the port is open on your router here Check if port 32764 is open at this website. If it is open contact your ISP or vendor and if they cannot fix it then you may need to look for another device.
- You must use VPN when working on State resources, this ensures the traffic is encrypted from end-to-end.
- Securing IoT devices like doorbells, lighting systems and bridges, etc is highly recommended to keep your network secure. Keep these devices firmware updated on a regular basis. If your home

network is able to have multiple Wireless SSID's, we recommend that you put your IoT devices on a separate network from your mobile devices/PC's to improve the security posture.

- On your personal PC's/MacIntosh devices we recommend that you run Anti-Virus/Anti-Malware on all devices that are able to. Some devices have Anti-Malware scanning abilities that may require a purchase of a subscription service. Enabling these features improves your home network security posture.

3. ACCOUNTABILITY

Wireless access users must comply with all applicable policies and accepts that his or her access and/or connection to the State's networks may be monitored to record dates, times, duration of access, data types and volumes in order to identify unusual usage patterns or other suspicious activity. DoIT reserves the right to turn off, without notice, any access port to the network that puts the State's systems, data, users, and clients at risk.

4. DESCRIPTION

If you have questions or need assistance, please consult with your wireless vendor and/or your Internet service provider. Due to the number and types of wireless solutions, DoIT cannot provide assistance with these configuration guidelines. No support for the use of these devices will be provided

5. REFERENCE

Wireless Communications Policy
Mobile Device Security Policy
Personally Owned Device Policy
IT Standards Exception Policy
Remote Access Policy