1.0 PURPOSE

This document prescribes how wireless technologies will be deployed, administered, and supported to assure that State of West Virginia employees, guests, and contractors have access to a reliable, robust, and integrated wireless network, and to increase the security of the wireless network to the fullest extent possible.

2.0 SCOPE

This policy applies to all employees who install, authorize, or recommend wireless access point devices, unless employees are in an agency classified as "exempt" in West Virginia Code Section 5A-6-8, "Exemptions." The State's users are expected to be familiar with and to comply with this policy, and are also required to use their common sense and exercise their good judgment while using Internet services.

3.0 POLICY

3.1 Wireless access points are allowed on the State network if specifically **pre-approved in writing by the WVOT**.

3.2 Only designated IT Approval Authorities may request additional access points be added;

3.2.1 Requests must be submitted through the Service Desk.

3.2.2 No equipment may be purchased in advance of approval, and wireless equipment must comply with WVOT established standards.

3.3 Approved access points will be designated as "Open" or "Secured" ("Closed") based on the answers provided in the WAP Usage Requirement Form (Appendix A).

3.3.1 *Open Networks* are access points that are used by the public to gain access to the internet.

3.3.1.1 Each agency has different needs and requirements for public internet access. Agencies are encouraged to contact their WVOT Customer Relationship Manager to review available options.

3.3.1.2 Public access points should NOT connect to the WVOT internal use network.

3.3.1.3 Agencies should acquire 3rd party solutions, where feasible, to keep public and private networks physically separated and distinct.

3.3.1.4 At a minimum, all public traffic must be segmented from the State traffic on the internal network if a 3rd party alternative is not available.

3.3.1.5 Any State data that traverses an "Open" wireless network must use a VPN connection.

3.3.1.6 Federal Tax Information (FTI), Protected Health Information (PHI), and Personal Identifying Information (PII) must not be transmitted over Open Networks by any State employees.

3.3.2 *Secured Wireless Networks* are wireless access points that are accessible only to WVOT-approved and supported devices, and require a confidential access key for connectivity.

3.4 Networking Services, or its designee (e.g. contractor), will configure all wireless equipment and software, following the most current pre-established, approved, and documented configuration specifications.

3.4.1 After the wireless equipment is installed at the requested location, no configuration changes may be made without written approval of Networking Services management.

3.4.2 Networking Services will manage the access keys.

3.4.3 Network Services or its designee (e.g. contractor), will change the Wireless AP default SSID, and examine and change all other default parameters.

4.4.4 Conformance to standards referenced in this section may be audited for compliance.

3.4.4 All devices will use WPA (minimum) encryption or compliant with current WVOT 802.11 standards.

3.4.5 All devices will be compatible with, and include accommodation for, anti-theft mechanisms (i.e. security cable, locking bolts).

3.5 Any unapproved access point discovered in operation, and located on State property, whether connected to the WVOT network or not, is subject to being disabled and removed immediately and permanently, by the WVOT. This includes, but is not limited to, personal cell phones being used as a WAP.

3.6 Previously approved access points may be disapproved, disabled, reconfigured, or moved by Networking Services as needed to ensure future reliability, security, responsiveness, and coverage of the WVOT wireless network.

3.7 WVOT uses the 802.11 protocol as its wireless network standard, with the intention of delivering acceptable connection speeds for mobile and wireless devices.

3.8 WVOT will only support state owned wireless equipment for accessing corporate networks and systems wirelessly.

3.9 When necessary, WVOT will conduct a site survey to determine the appropriate placement of new or additional access points. All installations will be in compliance with all local safety, building, and fire codes.

3.10 All access point broadcast frequencies and channels shall be set and maintained by WVOT, or its designee (e.g. contractor). Any device or equipment found to be interfering with access point signals may be subject to relocation or removal, including, but not limited to, cordless phones, microwave ovens, cameras, light ballasts, etc.

3.11 Use of the wireless network is subject to the same usage parameters specified in WVOT's Information Security Policy and Internet acceptable use policies.

3.12 WVOT may conduct assessments of State properties to ensure there are no rogue access points present.

3.13 When possible, empty rooms and offices should have network jacks disconnected from the switch to prevent rogue access point installation.

3.14 WVOT reserves the right to turn off, without notice, any access point connected to the network.

3.15 All persons governed by this policy must immediately report to WVOT any incident or potential incident of unauthorized access point installation and/or disclosure of company resources, databases, networks, and any other related components of the organization's technology infrastructure, to incident@wv.gov.

4.0 RELEVANT MATERIALS/DOCUMENTS

This policy is consistent with the following federal and state authorities:

- 45 Code of Federal Regulations (CFR) §§ 164.308-316
- Freedom of Information Act
- Gramm-Leach Bliley Act (GLBA)
- Health Insurance Portability and Accountability Privacy Rule
- NIST SP 800-14 and NIST SP 800-53
- State Health Privacy Laws

- WV Code § 5A-6-4a
- WV Executive Order No. 7-03
- WVOT Policies Issued by the Chief Technology Officer (CTO), www.technology.wv.gov/security/Pages/policies-issued-by-the-cto.aspx

5.0 ENFORCEMENT & AUTHORITY

Any employee found to have violated this policy may be subject to disciplinary action up to and including dismissal. Disciplinary action will be administered by the employing agency and may be based upon recommendations of the WVOT and the **West Virginia Division of Personnel**. Please review the **WVOT Policy and Procedure Policy #1000** to review additional provisions concerning enforcement and policy authority.

6.0 DEFINITIONS

6.1 Access– The ability to locate, gain entry to, and use a directory, file, or device on a computer system or over a network.

6.2 Information Security – Those measures, procedures, and controls that provide an acceptable degree of safety for information resources, protecting them from accidental or intentional disclosure, modification, or destruction.

6.3 SSID – A Service Set Identifier is a name that identifies a wireless network. All devices on a specific wireless network must know its SSID.

6.4 Threat – Includes any person, condition, or circumstance that endangers the security of information or information systems in the context of information security.

6.5 User – A person authorized to access an information resource.

6.6 Open Network – An area that allows persons using laptop computers equipped with wireless network cards to connect to the WVOT network, via a VPN.

6.7 Secured ("Closed") – An area that allows State personnel using laptop computers equipped with wireless network cards to connect to the WVOT network directly. A network reserved for State of West Virginia employees and agencies. These wireless networks require password

6.8 Wireless Access Point - Any piece of equipment that allows wireless communication using transmitters and receivers to enable communications.

7.0 Change Log

- July 1, 2015 –

  - Added Section 3.1.1.1 – “Each agency has different needs and requirements for public internet access. Agencies are encouraged to contact their WVOT Customer Relationship Manager to review available options.”
  - Added Section 3.1.1.2 – “Public access points should NOT connect to the WVOT internal use network.”
  - Added Section 3.1.1.3 -- “Agencies should acquire 3rd party solutions, where feasible, to keep public and private networks physically separated and distinct. “
  - Added Section 3.1.1.4 -- “At a minimum, all public traffic must be segmented from the State traffic on the internal network if a 3rd party alternative is not available.”
  - Modified Section 4.4.4 – “WPA **(minimum)** encryption”
- 9/1/2016 – Policy Reviewed. No edits made.
- 10/20/2017 – Policy Reviewed. No edits made.
-