Information Technology Policy
Wireless LAN Technology

Number ITP-NET001	**Effective Date** November 12, 2012
Category Network	**Supersedes** All Prior Versions
Contact RA-ITCentral@pa.gov	**Scheduled Review** April 2023

1. Purpose

This Information Technology Policy (ITP) establishes enterprise-wide standards for Wireless Local Area Network (LAN) Technology and it's secure usage in a production environment.

2. Scope

This ITP applies to all offices, departments, boards, commissions, and councils under the Governor's jurisdiction (hereinafter referred to as "agencies").

Agencies and other organizations not under the Governor's jurisdiction, that connect to the Commonwealth network, shall follow this ITP to ensure they design and implement wireless LANs that facilitate enterprise-wide interoperability and standardization.

Third-party vendors, licensors, contractors, or suppliers shall meet the policy requirements of this ITP that are applicable to the products and services provided to the Commonwealth as outlined in the Responsibilities Section.

3. Definitions

3.1 Controller: Network device which controls the access points within a wireless network.

3.2 COPA-Campus wireless: Enterprise wireless network that bridges participating agencies' networks to allow wireless roaming capability.

3.3 Guest Wireless (COPA-Guest SSID): The Office of Administration's (OA) Controller for providing wireless access to the Internet that shall be used only by non-Commonwealth employees on a case-by-case basis.

3.4 Lobby Ambassador: Individual capable of creating Guest Wireless accounts.

3.5 Secure Wireless: A wireless implementation utilizing the centralized Controller for access to the internal Commonwealth network as well as the Internet.

3.6 Service Set Identifier (SSID): Identifies and specifies which 802.11 network is being joined.

3.7 WiFi Protected Access version 2 (WPA2): A security protocol, specified in the IEEE Wireless Fidelity (WiFi) standard, 802.11i, WPA2 uses AES (Advanced Encryption Standard), meaning it can now meet the government's Federal Information Processing Standard (FIPS) 140-2 security requirements.

4. Objective

- Uniform implementation of Wireless LANs.
- Assurance of information security to protect confidentiality of information.
- Safeguard the integrity of information.
- Establish common equipment platforms.
- Ensure appropriate access to information.
- Ensure centralized administration.

5. Policy

All new wireless LAN technology implementations are required to comply with the standards outlined in STD-NET001A *Wireless LAN Technology Standards, OPD-NET001B Wireless LAN Standardization* and the operational guidelines set forth in this ITP.

Operational Requirements

Agencies having a business need to implement a WLAN segment shall submit a request with the location via the IT Service Management Tool (refer to Section 7 Other ITPs/References for details). The Service Request design will be reviewed by the Office of Administration, Office for Information Technology, Network, Unified Telecommunication, and Security Operations (OA/OIT/NUTSO).

Equipment Requirements, encryption standards and specifications are outlined in the OPD-NET001B Wireless LAN Standardization.

Auditing

Agencies have the responsibility to ensure compliance with all ITPs, regulatory requirements and laws pertaining to whatever data flows over their managed wireless networks. Any agency implementing their own Secure Wireless network shall perform an assessment on the wireless network to show it has been set up correctly and in compliance with ITPs and NIST 800-97 Wireless security controls, pages 8-13 to 8-19). The results shall be sent to OA, OIT, Enterprise Information Security Office (OA/OIT/EISO).

OA/OIT/EISO may perform follow up spot checks on all wireless networks on an add-needed basis.

6. Responsibilities

6.1 Agencies shall

- Purchase the WLAN devices (APs and wireless user devices.)
- Perform security assessments on all agency managed wireless infrastructure in compliance with ITPs and NIST 800-97 and provide to OA/OIT/EISO for review.
- Submit the name of an individual who will be responsible for creating Guest Wireless accounts as the "Lobby Ambassador" for Guest Wireless.

6.2 Enterprise shall

6.2.1 OA/OIT/NUTSO shall

- Assign certificates through group policy.
- Facilitate authentication to the appropriate Enterprise Wireless Solution by required method(s).
- Conduct compliance audits of the COPA-Guest Wireless network to ensure the active accounts are in compliance with this ITP. Agencies found to have Commonwealth employees or other non-authorized personnel on the COPA-Guest network will be contacted by OA/OIT/NUTSO to remove those accounts and/or submit an IT Policy waiver request for this ITP.

6.2.2 OA/OIT/EISO shall

- Receive completed agency wireless security assessments and respond as needed.
- Perform spot checks on wireless networks as needed.

6.3 Third party vendors, licensors, contractors, or suppliers shall follow the standards listed in the STD-NET001A excluding utilizing the Enterprise Centralized wireless Controller solution(s)

7. Related ITPs/Other References

- Definitions of associated terms of this policy are published on the Office of Administration's public portal: http://www.oa.pa.gov/Policies/Pages/Glossary.aspx
- Commonwealth policies, including Executive Orders, Management Directives, and IT Policies are published on the Office of Administration's public portal: http://www.oa.pa.gov/Policies/Pages/default.aspx
- Management Directive 205.34 Amended Commonwealth of Pennsylvania Information Technology Acceptable Use Policy
- STD-NET001A *Wireless LAN Technology Standards*
- OPD-NET001B *Wireless LAN Standardization*
- NIST 800-97 – *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf*
- OA-OIT Service Request Process – (CWOPA limited access) https://itcentral.pa.gov/Pages/Enterprise-Services.aspx

8. Authority

Executive Order 2016-06 *Enterprise Information Technology Governance*

9. Publication Version Control

It is the Authorized User's responsibility to ensure they have the latest version of this publication, which appears on https://itcentral.pa.gov for Commonwealth personnel and on the Office of Administration public portal: http://www.oa.pa.gov/Policies/Pages/default.aspx. Questions regarding this publication are to be directed to RA-ITCentral@pa.gov.

10. Exemption from this Policy

In the event an agency chooses to seek an exemption from the guidance within this ITP, a request for a policy waiver is to be submitted via the enterprise IT policy waiver process. Refer to ITP-BUS004 *IT Policy Waiver Review Process* for guidance.

This chart contains a history of this publication's revisions. Redline documents detail the revisions and are available to CWOPA users only.

Version	Date	Purpose of Revision	Redline Link
Original	04/22/2005	Base Document	
Revision	11/24/2008	Update to leverage the Enterprise Certificate of Authority	
Revision	10/25/2010	Move 802.11n to Current	
Revision	12/20/2010	ITP refresh	
Revision	08/01/2012	ITP refresh	
Revision	12/30/2014	• Added policy to limit the number of simultaneous connections using the same user name to COPA_GUEST wireless network (Agency Responsibilities) • Removed "draft" from 802.11ac standard specification (Wireless LAN Technology Overview) and moved 802.11ac from research to current. • Updated the WiFi Alliance logo • Removed "Windows XP Wireless Auto Configuration" language, replaced with "WLAN AutoConfig service" in Section 7 (Recommended configuration - Do not suppress Service Set Identifier (SSID)) General formatting	
Revision	06/10/2016	• In Agency Responsibilities section, clarified Guest Wireless (COPA-Guest SSID) usage for only contractors and third-party non-Commonwealth employees; conference rooms Guest Wireless guidance for Lobby Ambassadors • Added audit language for Guest Wireless • Removed WPA from Definitions section • Added COPA-Campus wireless to Definitions section • Revised Guest Wireless definition Added Exemption section	
Revision	04/08/2022	• Updated Definitions • Added Objectives Section • Cleaned up Policy Section • Moved standards into new supplemental document STD-NET001A *Wireless LAN Technology Standards* • Pull information from policy and created new operational	Revised IT Policy Redline <04/08/2022>

		supplemental document OPD-NET001B *Wireless LAN Standardization* • Added Responsibilities Section • Updated Related ITPs/Other References Section • Updated Exemption Section • Added links	