MICHIGAN ECONOMIC DEVELOPMENT CORPORATION	**MICHIGAN ECONOMIC DEVELOPMENT CORPORATION** Information Technology	**Standard:** **INFRA.01.005**
Topic Area:	**MEDC Wireless LAN Standard**	
Distribution:	**All Michigan Economic Development Corporation Staff**	

Purpose: To establish a Michigan Economic Development Corporation (MEDC) standard for all MEDC Wireless Local Area Networks (WLANs) and for how WLAN technologies are deployed, administered, monitored and supported when attached directly to the MEDC networking infrastructure.

Contact/Owner: Michigan Economic Development Corporation
Information Technology

Scope: This defines the technologies used in the MEDC WLAN. MEDC Information Technology (IT) ensures WLAN technology is deployed in a fashion that preserves the security and integrity of the MEDC infrastructure and delivers an acceptable level of service for the users of wireless technology.

Standard:

Implementation

- All products utilized must be certified for compliance by the Wi-Fi Alliance. MEDC's current wireless system complies with the IEEE 802.11 standard to provide 802.11a/b/g/n/ac integrated end-to-end WLAN solutions. This product suite addresses Wireless Access Points (WAPs), network infrastructure, network management, wireless spectrum management, and the delivery of mobility services.
- MEDC IT centrally manages all of MEDC's wireless networks. This includes, but is not limited to, selection of network products, management of authentication solutions, installation of network devices, and monitoring of the wireless network. Only WAPs provided, installed and approved by MEDC IT are permitted on the MEDC network.
- MEDC IT reserves the right to remove or disconnect any WAP not installed and configured by MEDC IT personnel. A reasonable attempt will be made to contact the owner prior to disabling the network port to which an unauthorized device is attached. Wireless network devices causing denial of service (DoS) conditions will be shut down immediately.
- The MEDC IT will verify that network interface cards (NIC) / devices (including "built in" wireless NIC) are compatible with the MEDC wireless network infrastructure.

Issued Date:	Last Revision:	Last Reviewed:	Next Review Date:
November 17, 2016	November 17, 2016	April 30, 2018	April 30, 2019

- Implementations should minimize radio frequency "leakage" to unauthorized locations.
- WAP management must be compatible with existing MEDC management systems.
- Post-implementation vulnerability assessments should be performed once a year.
- Due to the inherent nature of the wireless technology, MEDC does not guarantee the availability of wireless access at all times. The implementation of the wireless system is intended to help augment (not replace) the current wired LAN.

Security

- MEDC IT will be responsible for overseeing the security of the MEDC WLAN in accordance with the following:
    1. The wireless network shall be on a separate internet protocol (IP) segment from the wired network at a given location where both a wired and wireless network exist.
    2. All WAPs will be installed and configured in such a way as to comply with MEDC required security features for wireless networking, including unique identification of users and restrictions to provide connectivity only to those users who are entitled to access.
    3. MEDC IT will identify and mitigate DoS attacks as necessary.
    4. MEDC IT will monitor and approve where MEDC managed WLAN devices can connect to the MEDC network, by using the following controls: Firewalls, Access Control Lists (ACLs), protocols, services, and ports.
    5. No peer-to-peer WLAN connections will be allowed.
    6. No wireless roaming from one WAP to another will be allowed if the WAPs are on different IP segments.
    7. Non-authenticated or "guest" users will only be allowed limited access to the Internet and secured DMZ applications for conducting MEDC related business.

Auditing & Monitoring

- Wireless management devices must be able to log all WLAN connections, system configuration changes or updates, failed attempts to connect to the MEDC WLAN, rogue WAPs and all system alarms and events. MEDC IT will maintain an audit trail of all changes made to the wireless management devices.
- WLAN audits should be conducted on a regular and as needed basis.

- MEDC IT network monitoring will include active detection, identification, and the appropriate response to rogue WAPs, as well as unauthorized access attacks identified by the WLAN system.

Interference Management

- IEEE standard 802.11-based networks operate using unlicensed wireless spectrum. Given this, only a very small number of wireless WAPs can be in active operation within a given geographic area without creating performance-degrading interference for each other. Even given limited deployment, it is important to have the WAP frequency settings configured in a non-interfering way. For this reason, coordination among those operating WAPs is essential.
- All equipment that operates intentionally or inadvertently in the wireless frequency spectrum will be carefully installed and configured to avoid interference between components of different network segments and wireless equipment. Consistent with ensuring the management of interference:
    1. The installation, management, and use of all wireless communication devices shall be consistent with federal and state laws and regulations and with MEDC policy.
    2. The order of priority for resolving unregulated frequency spectrum use conflicts shall be according to the following priority list:
        a. Life and safety
        b. MEDC business operations
        c. Training or demonstration
        d. Public access
        e. Personal
- MEDC IT will respond to reports of suspected devices causing interference and disruption of the WLAN network. Where interference cannot be resolved, the use of wireless devices may be restricted.

Configuration

- Service set identifiers (SSIDs) must not remain at their default settings.
- SSIDs must not identify the state or any of its agencies or organizations.
- Secure SSIDs will be broadcast.
- SSIDs must be unique and centrally managed by MEDC IT.
- MEDC IT is responsible for all configuration management.
- WLAN system devices must have their system time synchronized with a MEDC IT approved network time protocol (NTP) time source.

- The WAP radio signal must be tuned to minimize signal leakage beyond intended coverage areas.

Secure MEDC-NET Authentication

- The authentication protocols will follow IEEE 802.1X standards.
- Protected Extensible Authentication Protocol (PEAP) will be used to authenticate clients by creating an Advanced Encryption Standard (AES) encrypted secure socket layer/transport layer security (SSL/TLS) tunnel between the client and the authentication server, which protects the ensuing exchange of authentication information from casual inspection.
- MEDC-approved wireless client devices (workstation, laptop, etc.) will be authenticated against a trusted MEDC domain machine account, using a Kerberos network authentication protocol key, before access to MEDC-NET internal resources will be granted.
- Following successful device authentication, approved internal MEDC wireless users will be authenticated against a trusted MEDC domain account by supplying a valid User ID/Password.
- The MEDC approved user must have a MEDC managed device with a MEDC approved WLAN network adapter and device drivers that support 802.1X and WPA2 (Wi-Fi Protected Access 2) encryption. All other network connections must be disabled when connected to a MEDC WLAN.
- Devices must also be preconfigured with the correct WLAN settings, which include the WLAN name and the authentication method(s) required for use.

MEDC-GUEST Wi-Fi Authentication

- The MEDC IT Helpdesk personnel will assist to establish a single user account that will be used by all MEDC-GUEST Wi-Fi customers to authenticate until such time as a unique user authentication system can be implemented. A logon page will be displayed when attempting to access the Internet via a web browser. This password will change every 90 days.
- Informational table tents will be provided to WLAN customers for display in conference rooms or common areas. The table tent will provide the MEDC-GUEST SSID information.

MEDC-GUEST Wi-Fi Acceptable Use

- MEDC provides “MEDC-GUEST” Wi-Fi Internet access to MEDC business associates within MEDC managed LAN buildings where the MEDC WLAN service is installed. This is a restricted access Internet-only service, subject to the MEDC Acceptable Use Policy.

Encryption

- IEEE 802.11i, also known as WPA2 (Wi-Fi Protected Access 2) will be used for authentication handshaking and encryption. The 802.11i architecture contains the following components: 802.1X for authentication (entailing the use of PEAP with an approved authentication server), robust security network (RSN) for keeping track of associations, and Advanced Encryption Standard (AES) for encryption and data integrity.

Compliance

- Operating Unit: Any and all projects, consulting requests, equipment and software acquisition requests, or invitations to bid (ITB) relating to WLAN connectivity are subject to the functional requirements contained in this standard and will be subject to review for compliance with this standard.
- MEDC IT will review and revise these standards as wireless technologies evolve. MEDC IT will develop awareness materials to allow MEDC employees to understand the risks and responsibilities associated with wireless technologies. Exceptions from this standard for reasons other than those outlined above will be made through the standard MEDC exception handling process.

Definitions:

802.1X: An IEEE networking protocol which provides authentication mechanisms to devices trying to connect to a LAN or WLAN

802.11: An IEEE set of standards for frequency and bandwidth for wireless communications.

ACL: Access Control List - Access lists filter network traffic by controlling whether routed packets are forwarded or blocked at the router's interfaces, based on the criteria specified within the access lists.

AES: Advanced Encryption Standard – A specification for encrypting electronic data that was established by the National Institute of Standards and Technology.

Authorized Providers: Includes MEDC NTSD and other technical groups who have been granted the authority to provide WLAN technology.

IEEE: Institute of Electrical and Electronics Engineers – A nonprofit organization. Among its many functions is the setting of wireless standards

Kerberos: A computer networking authentication protocol that allows nodes (e.g. modems, hubs, bridges, switches) to identify themselves to each other

LMAN: The state of Michigan Lansing Metropolitan Area Network.

Lobby Ambassador: A feature of Cisco software to create guest user accounts

NTP: Network Time Protocol – An internet protocol for synchronizing computer clock among networked computers

PEAP: Protected Extensible Authentication Protocol – A protocol developed by Cisco, Microsoft, and RSA Security for transmitting authentication data over wireless 802.11 networks

MEDC-NET: MEDC TCP/IP networks, including LMAN and MEDC Wide Area Networks (MEDC-WAN).

MEDC-WAN: MEDC TCP/IP networks in remote office locations.

SSID: Service Set Identifiers – Essentially a network name. It is a unique identifier attached to the header of packets sent over a WLAN

TLS/SSL: Transport Layer Security/Secure Socket Layer - Cryptographic protocols, based on public key cryptography, which provide security over the Internet

Wi-Fi Alliance: A non-profit trade organization that promotes Wi-Fi technology and certifies whether Wi-Fi products meet certain levels of interoperability. From its web site (www.wi-fi.org): "Wi-Fi CERTIFIED is a program for testing products to the 802.11 industry standards for interoperability, security, easy installation, and reliability"

WPA2: Wi-Fi Protected Access 2. This is based on the IEEE 802.11i standard and provides government grade security by using National Institute of Standards and Technology algorithms and authentication.

Zone 0: Untrusted networks, including the Internet, and unrestricted access private networks.

Zone 1: The State of Michigan and business partner semi-trusted networks including demilitarized zone (DMZ) applications (like web applications), web pages, and client based applications.

Zone 2: State of Michigan internal trusted networks including the Lansing Metropolitan Area Network (LMAN) backbone. This includes network connectivity to more than 1,100 SOM government Wide Area Network sites around the state.

Zone 3: State of Michigan restricted networks including resources located within the DTMB Hosting Centers: Lake Superior and Traverse Bay. Zone 3 is used for highly secure private information

Authoritative Policies:	INFRA.01
Associated Procedures:	INFRA.01.005.01

Signature and Title of Approver:	**Date:**
Tilak Mohan, Chief Information Officer Digitally signed by Tilak Mohan DN: cn=Tilak Mohan, o=Michigan Economic Development Corporation, ou=Information Services, email=mohant1@michigan.org, c=US Date: 2018.05.04 19:02:37 -04'00'	April 30, 2018

Author:	Approver:	Approval Date:	Description of Change(s):
Kim Fedewa	Tilak Mohan	November 16, 2016	Original copy approval.
Kim Fedewa	Tilak Mohan	June 9, 2017	Annual Review – No change.
Kim Fedewa	Tilak Mohan	April 30, 2018	Annual Review – No change.