METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY INFORMATION SECURITY POLICY	POLICY NUMBER: ISM 6
SUBJECT: TELEWORKING AND MOBILE COMPUTING POLICY	DISTRIBUTION DATE: 9/4/2015
	EFFECTIVE DATE: 9/4/2015
ISSUING AUTHORITY: Director of Information Technology Services of the Metropolitan Government of Nashville and Davidson County	EXPIRATION: UNTIL RESCINDED

PURPOSE

The purpose of this policy is to ensure the users of the Metropolitan Government of Nashville and Davidson County (Metropolitan Government) achieves and maintains information security when using mobile computing and teleworking devices or facilities.

POLICY

1. Access and Use
   All acceptable access and use of Metropolitan Government information technology is defined in *ISM 1 Acceptable Use of Information Technology Assets Policy.* Users will comply with all aspects of that policy in addition to the requirements of this policy.

2. Permitted Forms of Remote Access
   All permitted forms of remote access are defined in *ISM 1 Acceptable Use of Information Technology Assets Policy.*

3. Types of Access Granted for Telework Devices

   3.1 Telework PC Access
   Users working on devices either owned by Metropolitan Government or a user of Metropolitan Government for the purpose of working off-site shall access resources only as approved by the Director, department head, supervisor or his or her designee.

   3.2 Third Party Owned Computers and Devices
   Computers not owned by Metropolitan Government or by the teleworker (e.g., hotel computers, public kiosks, conference computers, friend's PCs) and other devices (e.g., cell phones, tablets, wearables) may only access information assets configured for external access, such as hosted web-based applications, such as web-based email. Access to the internal Metropolitan Government network and information assets hosted on that network, which requires Metropolitan Government approved remote access solutions, shall not be allowed. The installation of any Metropolitan Government approved remote access solutions on these devices is prohibited.

4. Sensitive Information and Teleworking

Sensitive information that is stored on or sent to or from telework devices shall be protected with Metropolitan Government Information Technology Services (ITS) Department supplied security controls. Sensitive information handling is addressed the *ISM 1 Acceptable Use of Information Technology Assets Policy*. Users shall be fully aware of data contents and classification of data that is taken off-site.

5. Teleworking User Requirements

5.1 Securing Information

5.1.1 Using Physical Security Controls

All devices and papers that contain Sensitive information that are taken outside Metropolitan Government's facilities shall be handled to meet Metropolitan Government minimum physical security requirements. These are defined in the *Mobile Device and Removable Media Physical Security Requirements* standard.

5.1.2 Removable Media Use

Removable media use is addressed in *ISM 1 Acceptable Use of Information Technology Assets Policy*.

5.2 Backing Up Information

Proper storage of Metropolitan Government information, including critical business information, is addressed in *ISM 1 Acceptable Use of Information Technology Assets Policy*.

5.3 Destroying Information When No Longer Needed

Proper disposal of Metropolitan Government information is addressed in *ISM 1 Acceptable Use of Information Technology Assets Policy*.

6. Approved Smart Phones, Blackberries, etc.

The use of any mobile device, such as a mobile phone, Blackberry, etc., that will be used to store Metropolitan Government data is addressed in *ISM 1 Acceptable Use of Information Technology Assets Policy.*

7. Securing Home Networks and Using External Networks

7.1 Reference Data for Wireless Home Network Security

In order to ensure that all connectivity to Metropolitan Government information technology is secure, users shall maintain appropriate security on any network that will be used to access Metropolitan Government information technology, including home networks.

7.2 Wired Home Networks

Teleworkers shall secure their wired home networks to help protect their telework devices. The home network shall have a security device between the ISP and the

telework device. Metropolitan Government information technology departments do not provide support to user's home networks

7.3 Wireless Home Networks
Teleworkers shall secure their wireless home networks so that their remote access communications are protected. They shall secure these networks following the recommendations from the documentation for the home network's wireless access point (AP). Wherever possible, encryption should be configured and activated on the wireless access point (AP). Metropolitan Government information technology departments do not provide support to user's home networks.

7.4 External Networks
Teleworkers shall be aware that networks other than their home networks are unlikely to provide much protection for their network devices and communications, such as a laptop using any third-party provided wireless hotspot. They shall use a remote access solution provided by Metropolitan Government and they shall activate the secure remote access solution (e.g., establishing a VPN session) immediately after connecting to the third-party network.

8. Securing non-Metropolitan Government Issued Teleworker-Owned PCs
Users shall take necessary precautions against compromising the confidentially, integrity and availability of all Metropolitan Government information technology by meeting Metropolitan Government minimum security requirements to secure any non-Metropolitan Government issued device that is used to access Metropolitan Government information technology.

9. Miscellaneous
This policy supersedes all previous Metropolitan Government teleworking and mobile computing policies written or communicated. Users are responsible for periodically reviewing this policy for any revisions and for adhering to those revisions. This policy may be amended or revised at any time by Metropolitan Government. This policy does not supersede any departmental, agency or board policies that address areas defined in this policy as long as the requirements of such departmental, agency or board policies equal or exceed the minimum requirements set forth in this policy. This policy does not waive the responsibility of the user from following all applicable legal and/or regulatory requirements.

SCOPE, BACKGROUND and GOVERNANCE

This information is set forth in the *Metropolitan Government Scope, Background and Governance Statement for Information Security Policies*.

DEFINITIONS

Terms used in this policy are defined in the *Metropolitan Government Information Security Glossary*.

CONTACT

Questions should be directed to (615) 862-6222 or by email at ciso@nashville.gov, or by mailing them to CISO, Information Technology Services Department, 700 2nd Avenue South, Suite 301, P. O. Box 196300, Nashville, TN 37219-6300.

SIGNATURE

Keith Durbin,
Chief Information Officer/Director of ITS
Metropolitan Government of Nashville and Davidson County

REFERENCES

ISO 27002: sections 11.7
NIST Special Publications 800-88, *Media Sanitation Guide*
NIST Special Publications 800-46, *Guide to Enterprise Telework and Remote Access Security*
NIST Special Publications 800-124*, Guidelines on Cell Phone and PDA Security*
NIST Special Publications 800-53 Rev5, Recommended Security Controls for Federal Information Systems and Organizations: AC-7, AC-14, AC-20, MA-4NIST Cybersecurity Framework PR.AC-3, PR.MA-2
Center for Internet Security Critical Security Controls 1, 7, 8, 13
Criminal Justice Information Services Security Policy v 5.6

REVISION HISTORY

REVISION	DATE	CHANGES
1.0	5/3/2011	First released version
2.0	5/1/2014	Updated with minor edits.
2.1	9/4/15	Updated with minor edits.
2.2	6/28/16	Addition of applicable NIST CSF divisions and NIST SP 800-53 areas as references.
2.3	10/26/18	• Modified SP800-53 version from 3 to 5 to reflect what version policy was reviewed against. • Changed “PDA” to “tablets, wearables” in 3.2 • Added review of applicable CSCs. Added review of applicable Criminal Justice Information Services Security Policy