METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY **INFORMATION SECURITY POLICY**	POLICY NUMBER: ISM 16
SUBJECT: SEPARATION OF DEVELOPMENT, TEST, AND PRODUCTION ENVIRONMENTS POLICY	DISTRIBUTION DATE: 8/1/2011 EFFECTIVE DATE: 2/1/2012
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of Information Technology Services of the Metropolitan Government of Nashville and Davidson County	EXPIRATION: UNTIL RESCINDED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 that the Metropolitan Government of Nashville and Davidson County (Metropolitan Government) correctly and securely operates its information processing facilities

POLICY

1. Generally
   Metropolitan Government shall separate development, test and operational facilities to reduce the risks of unauthorized access or changes to the operational system and business data.

2. Baseline Configuration
   In order to support the separation of development, test and operational facilities, Metropolitan Government shall develop, document and maintain under configuration control a current baseline configuration of its information system, including its operational software. Such components include the standard operational software load for a workstation, server, network component, or mobile device including operating system/installed applications with current version numbers and patch information.

   Metropolitan Government also shall:

   2.1. Review and update the baseline configuration of its information system, including its operational software:
   - At a frequency that shall be determined by the department head;
   - When required due to new threats in the environment [disgruntled employee, vendor issues, hacking, new worms/viruses]; and
   - As an integral part of information system component installations and upgrades;

   2.2. Maintain an up-to-date, complete, accurate and readily available baseline configuration documentation of the information system; and
   2.3. Employ a deny-all, permit-by-exception authorization policy to identify operational software allowed to execute on the information system.

3. Separation of Duties
   3.1. To reduce risk of accidental change or unauthorized access to operational software and business data, there should be a separation of duties based on development, test and operational facilities;
   3.2. System security hardening should be accomplished by removing access to compilers, editors and system tools from operational systems when not required determined by least/minimal privilege and/or user role; and
   3.3. Users should use appropriate login to accomplish tasks with least amount of privilege needed.

4. Separation of Environments
   4.1. Test and development systems should be clearly marked or identified as non production systems;
   4.2. Sensitive data should not be copied into test and development systems; and
   4.3. Data and operational software of test systems should emulate production systems as closely as feasible.

5. Access Restrictions for Changes
   Metropolitan Government shall implement acess controls in accordance with applicable Metropolitan Government security policies that allow only qualified and authorized individuals access to information system components for purposes of initiating changes, including upgrades, and modifications.

6. Least Functionality
   Metropolitan Government shall configure the application, service, or information system to provide only essential capabilities and shall specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.

7. Network Diagram
   Metropolitan Government shall recommend that a complete network topological drawing on the information system solution is maintained in a current status.

8. Security of Configuration Documentation
   Metropolitan Government shall protect the system documentation from unauthorized access and documentation shall be classified “Confidential” at a minimum.

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: section 10.1.4
- NIST Special Publications 800-53 Rev3, *Recommended Security Controls for Federal Information Systems and Organizations;* CM-2
- Criminal Justice Information Services (CJIS) Security Policy

REVISION HISTORY

REVISION	APPROVAL DATE	CHANGES
1.0	8/1/11	First released version
1.1	8/15/2018	5 – 8 added to be in line with CJIS.