METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY **INFORMATION SECURITY POLICY**	POLICY NUMBER: ISM 16
SUBJECT: SOFTWARE AND INFORMATION SYSTEM DEVELOPMENT POLICY	DISTRIBUTION DATE: EFFECTIVE DATE: 9/1/2020
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of Information Technology Services of the Metropolitan Government of Nashville and Davidson County	EXPIRATION: UNTIL RESCINDED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 describe the software and information system development requirements for the Metropolitan Government of Nashville and Davidson County (Metropolitan Government) Development practices should ensure that software will be adequately documented, tested and deployed before it is used for critical business processes and storing of information and reduce the risk of the software being exploited.

POLICY

1. Software and System Development Life Cycle
   Metropolitan Government departments and agencies shall be responsible for developing, maintaining, and managing a System Development Life Cycle (SDLC), which provides code control, works to prevent unauthorized access to the applications, data and systems. All software developed in-house which runs on production systems shall be developed according to the established processes and procedures of the appropriate department's SDLC. Each department, agency and board of the Metropolitan Government must provide for the integrity and security of its information assets throughout the SDLC beginning at acquisition through development and maintenance, so that security becomes an integral component of the agency's information technology activities.

2. Role Based Access Controls
   Metropolitan Government shall utilize role-based access control systems to restrict system access privileges to users when dealing with non-public information or with critical business services. Systems shall have designated access control administrators who manage system wide privileges for user roles. Should the access control administrator also be a regular user of the system, they shall have two role-based accounts – one for administrative access and one for user-based access.

3. Three Tier Development Environment
   Metropolitan Government shall separate development, test and production environments to reduce the risks of unauthorized access or changes to the operational system and business data. This separation between non-production and production application environments to reduce the risks of unauthorized access or changes and aid in supporting methodology execution. The three operational environments are test, development and production.
   3.1. Test and development systems should be clearly marked or identified as non production systems;

3.2. Sensitive data should not be copied into test and development systems; and
3.3. Data and operational software of test systems should emulate production systems as closely as feasible.

4. Quality Assurance and Production Delivery
Metropolitan Government shall implement quality assurance and production delivery procedures related to software and information system delivery.

5. Audit Controls and Management
Metropolitan Government shall evaluate and implement appropriate audit controls and change management processes for ongoing support and maintenance of developed software and implemented information systems.

6. Vulnerability Testing
Metropolitan Government shall define software testing tools and techniques to be used as part of security review for the developed software and implemented systems.

7. Software Licensing
All software developed for Metropolitan Government is intellectual property of Metropolitan Government. Metropolitan Government shall determine the license type as part of project's functional user requirements.

8. Separation of Duties
8.1. 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;
8.2. 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
8.3. Users should use appropriate login to accomplish tasks with least amount of privilege needed.

9. Access Restrictions for Changes
Metropolitan Government shall implement access 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.
9.1. Access Restrictions
Only qualified and authorized individuals shall be allowed to obtain access to its software and source code, for purposes of initiating changes, including upgrades and modifications. Access restrictions for change shall also include software libraries.
9.2. Record of Accesses
Records of access shall be maintained for ensuring that configuration change control is being implemented as intended and for supporting after-the-fact actions should its unauthorized changes to its operational software and source code be detected.

10. 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.

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

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

13. Developer Configuration Management
    Metropolitan Government shall require the developer of the system, system component, or system service to:
    - 13.1. Perform configuration management during system, component, or service design; development; implementation; operation; disposal;
    - 13.2. Document, manage, and control the integrity of changes;
    - 13.3. Implement only Metropolitan Government approved changes to the system, component, or service;
    - 13.4. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; and
    - 13.5. Track security flaws and flaw resolution within the system, component, or service and report findings to the applicable Metropolitan Government Director, Agency Head or Elected Official.

14. Developer Testing and Evaluation
    Metropolitan Government shall require the developer of the system, system component, or system service, at all post-design phases of the system development life cycle, to:
    - 14.1. Create and implement a security and privacy assessment plan;
    - 14.2. Perform unit, integration, system and/or regression testing/evaluation as needed and appropriate;
    - 14.3. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation;
    - 14.4. Implement a verifiable flaw remediation process; and
    - 14.5. Correct flaws identified during testing and evaluation.

    The testing and evaluation may include:
    - Static Code Analysis
    - Threat Modeling and Vulnerability Analyses
    - Independent Verification of Assessment Plans and Evidence
    - Manual Code Reviews
    - Penetration Testing
    - Attack Surface Reviews
    - Verify Scope of Testing and Evaluation
    - Dynamic Code Analysis

15. Development Process, Standards and Tools
    Metropolitan Government shall require the developer of the system, system component, or system service to follow a documented development process that:
    - 15.1. Explicitly addresses security requirements;
    - 15.2. Identifies the standards and tools used in the development process;
    - 15.3. Documents the specific tool options and tool configurations used in the development process; and
    - 15.4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and

    Metropolitan Government shall review the development process, standards, tools, tool options, and tool configurations periodically to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy applicable security requirements.

16. Developer Provided Training
    Metropolitan Government shall require the developer of the system, system component, or system service to provide training on the correct use and operation of the implemented security and privacy functions, controls, and/or mechanisms.

17. Developer Security Testing
    Software developers/integrators (vendors/contractors or in-house) with oversight from qualified security engineer(s) identified by Metropolitan Government shall:
    - 17.1. Create and implement a security test and evaluation plan
    - 17.2. Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process
    - 17.3 Document the results of the security testing/evaluation and flaw remediation processes

18. Developer Security Architecture and Design
    Metropolitan Government shall require the developer of the system, system component, or system service to produce a design specification and security architecture that:
    - 18.1. Is consistent with and supportive of the Metropolitan Government's security architecture which is established within and is an integrated part of the organization's enterprise architecture;
    - 18.2. Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and
    - 18.3. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.

19. Supply Chain Protection
    Metropolitan Government shall protect against supply chain threats/attacks as part of a comprehensive, defense-in-depth information security strategy.

20. Trustworthiness
    All software and information systems, developed by vendors/contractors (or in-house), shall meet necessary levels of trustworthiness as determined by Metropolitan Government.

21. Developer Screening
    Metropolitan Government shall require that the developer of Metropolitan Government system, system component, or system service:
    - 21.1. Have appropriate access authorizations;
    - 21.2. Satisfy appropriate personnel screening criteria and
    - 21.3. Provide information that the access authorizations and screening criteria are satisfied.

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

- NIST Special Publications 800-53 Rev5, *Recommended Security Controls for Federal Information Systems and Organizations;* SA-8, SA-10, SA-11, SA-15, SA-16, SA-17, SA-20, SA-21
- NIST SP 800-23, Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
- Criminal Justice Information Services (CJIS) Security Policy ver 6.0
- NIST Cybersecurity Framework ver. 2.0
- NIST Special Publication 800-171 rev. 3, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*
- Payment Card Industry Data Security Standard version 4.0.1

REVISION HISTORY

REVISION	APPROVAL DATE	CHANGES
1.0	8/31/2020	First released version
1.1	8/29/2025	Change to reflect use of rev 5 of NIST 800-53 as a reference Change to reflect use of rev 2 of NIST Cybersecurity Framework Change to reflect use of version 6 of CJIS as a reference Change to reflect use of version 4.01. of PCI-DSS as a reference

		Change to reflect use of NIST 800-171 r3 as a reference