METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY # INFORMATION SECURITY POLICY	POLICY NUMBER: ISM 22
SUBJECT: SYSTEM SECURITY PLANS (SSP) POLICY	DISTRIBUTION DATE: 10/10/2025 EFFECTIVE DATE: 10/30/2025
ISSUING AUTHORITY: Director of Information Technology Services of the Metropolitan Government of Nashville and Davidson County	EXPIRATION: UNTIL RESCINDED

PURPOSE

This policy establishes the requirement for developing, maintaining, and reviewing System Security Plans (SSPs) for all information systems that support critical functions or store, process, or transmit sensitive information. The SSPs serve as foundational documentation for managing cybersecurity risk and ensuring compliance with applicable federal and local standards.

A document that describes how an organization meets the security requirements for a system or how an organization plans to meet the requirements, and it documents the specific security controls (policies, procedures, and technical measures) that are implemented or planned to be implemented to protect the system.

DEFINITIONS

Terms used in this policy are defined in the *Metropolitan Government Information Security Glossary*. The following terms used in the policy are defined as:

- System Security Plan - A document that describes how an organization meets the security requirements for a system or how an organization plans to meet the requirements. (SOURCE: NIST)
- System Owner - Person or organization having responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system. (SOURCE: NIST)

POLICY

1. Roles and Responsibilities

1.1. The Chief Information Security Officer (CISO) shall
- 1.1.1. oversee the implementation and governance of a Master Security Plan, outlining enterprise-wide security controls,
- 1.1.2. consult on development of appropriate sub-System Security Plans (SSPs) and
- 1.1.3. ensures alignment with NIST guidance and Metro's cybersecurity strategy.

1.2. The ISSC shall review and recommend updates to this policy and associated procedures.

1.3. Directors, Agency Heads and Elected Officials shall
- 1.3.1. ensure SSPs are developed and maintained for all applicable systems within their purview,
- 1.3.2. ensure SSPs are reviewed and updated at least annually or upon significant system changes and
- 1.3.3. designate appropriate resources for SSP development.

1.4. System Owners shall
- 1.4.1. develop and maintain SSPs in accordance with Metro and NIST requirements,

1.4.2. ensure SSPs accurately reflect the system's security controls, architecture, and risk posture,
1.4.3. protect the security plan from unauthorized disclosure and modification, and
1.4.4. coordinate with the CISO for SSP development, reviews and audits.

2. System Security Plan (SSPs) Requirements

2.1. SSPs should be developed for all systems that:
2.1.1. Support critical government functions.
2.1.2. Store, process, or transmit sensitive or regulated data (e.g., PII, PHI, CJIS).
2.1.3. Are externally hosted or integrated with third-party services.

2.2. Each SSP must include:
- System description.
- Description of information stored, collected, processes, etc., including classification of information.
- Security control implementation details.
- Roles and responsibilities.
- Risk assessments and mitigation strategies.
- Continuous monitoring and incident response procedures.

2.3. SSPs must be reviewed:
- Annually.
- After major system changes (e.g., architecture, hosting, data classification).
- Following security incidents or audit findings.

3. Integration with Risk Management

3.1. SSPs should be integrated into Metro's broader risk management and compliance processes.
3.2. SSPs should inform the development of Plans of Action and Milestones (POA&Ms) for identified control gaps.

4. Training and Awareness

Internal role-based training should be provided for appropriate Metro staff on SSP development and maintenance.

SCOPE, BACKGROUND and GOVERNANCE

This policy applies to all departments, agencies, and boards of the Metropolitan Government of Nashville and Davidson County, excluding those explicitly exempted under the Metro Scope and Governance Statement.

CONTACT

Questions should be directed to (615) 862-6222 or by email at ciso@nashville.gov.

SIGNATURE

John Griffey

John Griffey,

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

REFERENCES

- NIST SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*
- NIST SP 800-171 Rev. 3, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*
- NIST Cybersecurity Framework (CSF) 2.0

REVISION HISTORY

REVISION	APPROVAL DATE	CHANGES
1.0	10/10/2025	First released version