METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY **INFORMATION SECURITY POLICY**	POLICY NUMBER: ISM 21
SUBJECT: CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT POLICY	DISTRIBUTION DATE: 10/10/2025 EFFECTIVE DATE: 10/31/2025
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of Information Technology Services of the Metropolitan Government of Nashville and Davidson County	EXPIRATION: UNTIL RESCINDED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 establish a consistent and risk-based approach to managing cybersecurity risks associated with third-party vendors and supply chain partners who provide products and or services to the Metropolitan Government (Metro). This policy establishes the requirements for identifying, assessing, managing, and monitoring cybersecurity risks associated with third-party vendors and supply chain partners.

DEFINITIONS

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

POLICY

1. **Roles and Responsibilities**
   - 1.1. The Chief Information Security Officer (CISO) shall oversee the implementation of a cybersecurity supply chain risk management (C-SCRM) program, ensures alignment with NIST guidance, and report to the Information Security Steering Committee (ISSC).
   - 1.2. The ISSC shall review and recommend updates to this policy and associated procedures.
   - 1.3. Directors, Agency Heads and Elected Officials shall ensure vendor compliance within their operational areas and ensuring all applicable procurement and assessment procedures are conducted.
   - 1.4. Directors, Agency Heads and Elected Officials shall ensure that a departmental point of contact is established for all vendors.
   - 1.5. Directors, Agency Heads and Elected Officials shall ensure that appropriate service level agreements (SLAs) or other contractual obligations are established in accordance with the criticality of the service provided by the vendor.
   - 1.6. Procurement and CISO shall develop a process for adding required security clauses to contracts.
   - 1.7. Vendors shall comply with all applicable Metro policies and contractual obligations.

2. **Training and Awareness**

   Internal role-based training shall be provided to appropriate Metro staff around C-SCRM related procedures.

3. **Risk-Based Tiering**

3.1. Metro shall develop a process for categorizing vendors and suppliers based on the criticality of the services or products they provide to the department and agency and the sensitivity of the data they are entrusted, have access to or process on behalf of Metro.

3.2. Risk tiering shall inform the level of due diligence, monitoring, and contractual requirements.

4. Pre-Engagement Due Diligence and Risk Assessment

Prior to engagement, all vendors shall undergo a cybersecurity risk assessment. Risk assessments shall consider:

- Supplier ownership and control (e.g., foreign influence)
- Software and hardware source(s)
- History of security incidents or regulatory violations
- Sub-tier supplier dependencies
- Presence of appropriate contract language
- Review of third party attestations or certifications of the vendor’s security management program

5. Contractual Requirements

Metro shall develop a process for adding appropriate contractual requirements to contracts. These clauses shall include, but not be limited to:

- Security and privacy clauses aligned with Metro policies;
- Incident notification requirements (within 24 hours of discovery of a security breach that might have compromised Metro information or services);
- Right to audit and assess security controls;
- Data handling, retention, and destruction requirements;
- Vendor responsibility for ensuring flow-down of security requirements to subcontractors
- Data privacy clauses stating that any data provided to the vendor, including information provided by Metro residents , is only to be used to fulfill the contracted services and that any additional data that is inferred or determined based on primary information that is provided to the provider, i.e. “second-order data”, is only to be used to fulfill the contracted services. Metro provided data or data collected on behalf of Metro shall not to be used for marketing or commercial purposes and the vendor asserts no rights to this information outside of fulfilling the contracted services;
- Data storage clauses that no Metro data, including backups, are to be stored outside of United States jurisdiction;
- Appropriate levels of cyber risk and technical errors and omissions insurance is provided; and
- Appropriate service level agreements.

6. Onboarding and Access Control

6.1. Vendors shall complete Metro security awareness training if required.

6.2. Vendor access shall be provisioned on a least-privilege basis and reviewed quarterly by the appropriate department or agency.

6.3. Departments shall immediately report to the appropriate IT department when a vendor account is no longer is use and is to be terminated.

7. Continuous Monitoring

7.1. Departments shall monitor high- and moderate-risk vendors on an ongoing basis for:

- Security posture (e.g., vulnerability disclosures, breach reports)
- Compliance with contractual obligations
- Changes in ownership, location, or service scope

7.2. Departments shall immediately report any changes to service scope to CISO to trigger a reassessment of risk.

8. Supply Chain Mapping and Transparency

Departments shall maintain an inventory of vendors providing critical services or hosting sensitive information and those vendors sub-tier dependencies.

9. Incident Response and Reporting

9.1. Departments shall take steps to ensure vendors cooperate with Metro's incident response processes and provide timely access to logs, systems, and personnel as needed.

9.2. Security events and incidents, including compromise and data breaches, involving vendor systems that impact Metro data or operations must be reported immediately to the appropriate departmental point of contact.

9.3. Departmental point of contact shall report any known or suspected information technology security incidents immediately in accordance with their Department's procedures. In the absence of any defined procedures, departmental point of contact shall report incidents to the appropriate management staff, such as their supervisor, who shall report it to the Metropolitan Government Help Desk.

10. Termination and Offboarding

10.1. Upon contract termination, vendors shall return or securely destroy all Metro data and certify destruction.

10.2. Departments shall inform the appropriate IT department of contract termination so that any user accounts can be deproivisioned and any changes to technical controls, such as firewall rules, software installations, etc. can be rolled back.

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. It covers all third-party entities, including contractors, suppliers, service providers, and system integrators. This policy applies to all Metro Nashville departments and agencies that engage with external vendors, contractors, suppliers, or service providers who:

- Access, process, or store Metro data
- Provide software, hardware, or cloud-based services
- Integrate with Metro's IT infrastructure
- Support critical operations or public services on behalf of Metro

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 800-161r1: Cybersecurity Supply Chain Risk Management Practices
- NIST SP 800-53 Rev. 5: Security and Privacy Controls
- NIST Cybersecurity Framework (CSF) 2.0

REVISION HISTORY

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