METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY # INFORMATION SECURITY POLICY	POLICY NUMBER: ISM 4
SUBJECT: EXTERNAL PARTY SECURITY	DISTRIBUTION DATE: 1/1/2014
	EFFECTIVE DATE: 7/1/2014
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of Information Technology Services of the Metropolitan Government of Nashville and Davidson County	EXPIRATION: UNTIL RESCINDED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 define the rules for maintaining the security of the Metropolitan Government of Nashville and Davidson County's (Metropolitan Government) information, information technology assets and information processing facilities that are accessed, processed, communicated to, or managed by external parties or where external parties add products or services to information processing facilities.

POLICY

Generally, Metropolitan Government shall:

- Identify the security risks to Metropolitan Government's information, information technology assets and information processing facilities from business processes involving external parties and implement appropriate controls before granting access;
- Address all identified security risks before giving customers access to Metropolitan Government's information or assets; and
- Have agreements in place with external parties addressing relevant security requirements, as applicable, for access, process, communication with, or management of Metropolitan Government's information, assets, or information processing facilities.

1. Identification of Risks Related to External Parties

1.1 Metropolitan Government shall identify and manage the security risks, including regulatory compliance considerations, related to information, information technology assets and information processing facilities for any external party who:

- Has access to an information processing facility;
- Has unescorted physical access to Metropolitan Government's assets such as offices, computers, file cabinets;
- Has logical access to Metropolitan Government's databases or information systems;
- Has connectivity between an external party network and Metropolitan Government's network; and/or
- Has access to any Metropolitan Government's information.

1.2 Metropolitan Government shall also implement the controls necessary to prevent access to and protect information and information technology assets that is not intended to be accessible by external parties.

2. Addressing Security When Dealing with Citizens and Customers

Metropolitan Government shall identify all security requirements prior to granting access to or releasing any Metropolitan Government information or information technology assets to citizens or other customers. These security requirements will be addressed, when necessary, using customer agreements and other applicable security requirements.

3. External Party Agreements

Metropolitan Government shall implement agreements with external parties who provide products or services involving access to, processing of, communication with, or managing Metropolitan Government's information, information technology assets and information processing facilities.

External party providers shall include, for example, service bureaus, contractors, hosted services providers and other organizations providing information system development, information technology services, outsourced applications, and network and security management. Metropolitan Government shall assign a designated individual to manage external party relationships and this person will ensure that information security requirements are included where applicable.

Metropolitan Government, in external party agreements, shall:

- **Require external parties to report perceived security incidents that may impact the confidentiality, integrity or availability of Metropolitan Government data immediately or no more than 24 hours after incident discovery;**
- Explicitly include personnel security requirements in acquisition-related documents;
- Require compliance with applicable Metropolitan Government's information security policies and processes and require appropriate parties to sign agreements stating they will comply with applicable Metropolitan Government information security policies, associated processes, and supporting standards;
- Require primary external parties to require their sub-contractors to abide by Metro policies and security requirements, as applicable;
- Require external parties to employ confidentiality agreements, as applicable;
- Address appropriate security controls in accordance with applicable federal laws, state laws, Executive Orders, directives, policies, regulations, standards, and guidance;
- Define and document information security oversight and user roles and responsibilities with regard to external party information system services; and
- Ensure monitoring and review of external parties that includes adherence to Metropolitan Government information security policies, monitoring service level agreements, and review all security incidents reported by external parties.

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 4, 6.2
NIST Special Publication 800-53 Rev5, Recommended Security Controls for Federal Information Systems and Organizations: AC-8, AT-2, CA-3, PL-4, PM-9, PS-7, RA-3, SA-1, SA-9, SC-7

REVISION HISTORY

REVISION	DATE	CHANGES
1.0	1/1/2014	First released version
1.1	3/31/2014	Revised with minor edits for clarification purposes
1.2	8/15/2018	Add hosting services to clarify they are external parties. Modified SP800-53 version from 3 to 5 to reflect what version policy was reviewed against.