METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY **INFORMATION SECURITY POLICY**	POLICY NUMBER: 18
SUBJECT: IT CONTINGENCY/DISASTER RECOVERY PLANNING	DISTRIBUTION DATE: 9/1/2011 EFFECTIVE DATE: 3/1/2012
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OF INFORMATION TECHNOLOGY SERVICES OF THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY	EXPIRATION: UNTIL RESCINDED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) establishes, maintains and implements plans for emergency response, backup operations and post-disaster recovery for Information Systems, including any Information Technology Assets that support those systems.

POLICY

1. Generally

   Metropolitan Government's IT contingency/disaster recovery planning capability must meet applicable (and agreed to with customers) service levels supporting critical operations in the event of a disruption. The procedures for execution of such a capability shall be documented in a formal IT contingency/disaster recovery plan ("Plan"), scoped to the information system(s) that support department, agency and board services. Metropolitan Government personnel shall be trained to execute IT contingency/disaster recovery planning procedures. The Plan shall meet the requirements of applicable federal, state and local laws and regulations.

2. Integration with Business Continuity Plans

   The Plan shall represent a broad scope of activities designed to sustain and recover critical IT services following an emergency. Metropolitan Government shall properly prepare response, recovery and continuity activities for disruptions affecting its information systems, business processes and facilities. Due to the inherent relationship between an information system and the business processes it supports, there should be coordination between all applicable stakeholders during Plan development and updates to ensure that recovery strategies and supporting resources neither negate each other nor duplicate efforts.

3. The Plan

   Every Metropolitan Government department, agency and board with services that are dependent on information systems shall, as applicable:

   3.1. Develop a Plan for the information system that:
   - Identifies essential missions and business functions and associated requirements;
   - Provides recovery objectives, restoration priorities and metrics;

- Addresses roles, responsibilities, and assigned individuals with contact information;
- Addresses maintaining essential missions and business functions despite an information system disruption, compromise or failure;
- Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented;
- Is reviewed and approved by appropriate officials within Metropolitan Government;
- Includes assessing Plan effectiveness and incorporating lessons learned;
- Includes a test Plan; and
- Requires the use of an alternate storage site.

3.2. Distribute copies of the Plan to a defined list of key contingency personnel, identified by name and/or by role, and organizational elements, as determined by the department, agency or board;
3.3. Coordinate Plan activities with incident handling activities;
3.4. Review the Plan for the information system;
3.5. Revise the Plan to address changes to Metropolitan Government, its information system or environment of operation and problems encountered during Plan implementation, execution or testing; and
3.6. Communicate Plan changes to a defined list of key contingency personnel, identified by name and/or by role, and organizational elements, as determined by the department, agency or board.

4. Plan Training

Each Metropolitan Government department, agency and board, shall train its personnel in their Plan roles and responsibilities with respect to the information system and provide refresher training annually or as triggered by a major infrastructure change.

5. Plan Testing and Exercises

Each Metropolitan Government department, agency and board shall:

5.1. Test and/or exercise the Plan for the information system at least annually, using the applicable department's, agency's or board's discretion as to the type of test and/or exercise, to determine the Plan's effectiveness and Metropolitan Government's readiness to execute the Plan. In no case shall such test and/or exercise be less comprehensive than a tabletop exercise; and
5.2. Review the Plan test/exercise results and initiate corrective actions.

6. Alternate Storage Site

Each Metropolitan Government department, agency or board shall establish an offsite secure storage site including necessary agreements to permit the storage and retrieval of information system backup information.

7. Alternate Processing Site

Each Metropolitan Government department, agency and board shall:

7.1. Establish an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within the agreed upon time period as described in the service level agreement with the applicable department, agency or board when the primary processing capabilities are unavailable; and

7.2. Ensure that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the Metropolitan Government-defined time period for resumption.

8. Telecommunications Services

Each Metropolitan Government department, agency and board shall establish alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions when the primary telecommunications capabilities are unavailable.

9. Information System Backup

Each Metropolitan Government department, agency and board shall securely backup resources as needed to facilitate meeting their defined recovery time and point objectives.

10. Information System Recovery and Reconstitution

Each Metropolitan Government department, agency and board shall provide for the recovery and reconstitution of the information system to a known state after a disruption, compromise or failure. It shall also protect backup and restoration hardware, firmware and software.

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.

____

Keith Durbin
Director of Information Technology Services

REFERENCES

- ISO 27002: section 10.1.4
- NIST Special Publications 800-53 Rev5, *Recommended Security Controls for Federal Information Systems and Organizations;* CM-2
- NIST Cybersecurity Framework: PR.IP-9, PR.IP-10, RC.RP-1, RC.IM-1,RC.IM-2, RC.CO-3

REVISION HISTORY

REVISION	DATE	CHANGES
1.0	9/1/11	First released Version
1.1	10/26/2018	• Modified SP800-53 version from 3 to 5 to reflect what version policy was reviewed against. •Added review of applicable CSCs. Change in policy number to address new numbering scheme.