CITY OF LONG BEACH

INFORMATION TECHNOLOGY DISASTER RECOVERY POLICY

I. SCOPE

Information technology ("IT") is an integral part of the City of Long Beach's (the "City") operations. The impact of an unplanned IT disruption could significantly impact City's operations.

II. PURPOSE

To ensure the City's IT system and/or electronic data is able to be recovered as quickly and effectively as possible following an unplanned disruption.

III. BACKUP PROCEDURES

All data, operating systems and utility files must be adequately and systematically backed up. The Network Specialist shall keep on file with the City Clerk a written description of the City's current technology related backup procedures. At a minimum, the backup procedures must include:

1. The frequency and scope of backups;

2. The location of all stored backup data;

3. The specific method for backing up and any other important details relating to the process (e.g., file-naming conventions, method of transporting data offsite, etc.);

4. The process and frequency to verify that City data has been effectively backed up;

5. The process and frequency to test the City's ability to restore backup information; and

6. Records of software licensing.

IV. OFFSITE BACKUPS

In the event City data or backups are stored offsite, the Network Specialist will ensure any and all offsite locations meet acceptable security requirements and other conditions of storage (temperature control, fire prevention, etc.). The Network Specialist will request a written statement or agreement from the applicable vendor(s) which clearly describes the expectation for safeguarding the data, especially if it contains personal, private or sensitive information. In addition, the Network Specialist will periodically check with New York State Archives to review the laws and regulations pertaining to offsite data storage (http://www.archives.nysed.gov/records/mr_data_storage.shtml).

V. IT CONTINUITY PLANNING

With the input of applicable Departments, the Network Specialist will develop and maintain a written IT Continuity Plan. The Continuity Plan will focus on sustaining critical IT functions during and after an unscheduled interruption and will be annually reviewed and updated as deemed appropriate by the Network Specialist. At a minimum, the Continuity Plan will include, but not be limited to:

1. Roles and responsibilities of key City personnel;

2. Communication protocols with outside parties (e.g., law enforcement, IT vendors);

3. Prioritized mission-critical processes and services;

4. Technical details concerning how systems and data will be restored; and

5. If applicable, resource requirements necessary to implement the plan.

VI. IT POLICY AMENDMENTS

As deemed necessary by the Network Specialist, the City shall review its Information Technology Disaster Recovery Policy and shall approve policy revisions, if any, by formal resolution.

ADOPTED: OCTOBER 29, 2020