CITY OF LONG BEACH
INFORMATION TECHNOLOGY POLICY

I. SCOPE

Theft, fraud and inappropriate access to information are among the hazards associated with the City of Long Beach's (the "City") Information Technology ("IT") systems. A municipality may face significant financial loss or a system failure as a result of cyber threats, attacks or breaches.

II. PURPOSE

To ensure the City protects sensitive data and IT systems by taking efforts that will reduce the risk of a technology breach.

III. IT POLICY STATEMENTS

To protect its data and information, the City will:

1. On an annual basis, the IT Department will perform a cybersecurity self-assessment, which will:

    a. Determine what personal, private and sensitive information the City collects, and where it resides on its IT systems.

    b. Determine what type of computer hardware and software is currently being utilized and verify that anti-virus and firewall protection as well as software and operating system updates are current.

    c. Identify employees who have access to sensitive financial or other private information.

    d. Confirm the security of all applicable onsite and cloud backups.

2. Notify affected parties if an unauthorized individual(s) obtains sensitive and private data.

3. Allow only authorized individuals to access the IT systems of the City remotely. Individuals must be authorized through Council resolution with the concurrence of the City Manager.

4. Grant system access to employees only for those IT resources that are necessary to fulfill their respective job responsibilities.

5. "Lock" computers when they are unattended by enabling a system to automatically do so after a specific time of inactivity and establish procedures for employees to manually lock their IT system(s) when they leave their workstation.

6. Maintain proper inventory and physical controls over tangible and intangible IT property.

7. Separated employees will be immediately blocked from access to IT systems and digital information.

8. Provide regular cybersecurity training, as applicable determined by the Network Specialist, to City employees or officials.

9. The Director of IT will notify the City Manager when an employee(s) attempts to access a website that has been blocked.

10. The Director of IT will notify the City Manager immediately of any attempts to breach the City's IT systems.

11. The IT Department must be aware of the changing world of cybersecurity and make certain the City is prepared to deal with the latest trends that could put the security of its data at risk. As such, the IT Department will develop and maintain a disaster recovery plan to safeguard the City.

12. All City employees must be made aware, by the Network Specialist, of the City's disaster recovery plan.

XV. IT POLICY AMENDMENTS

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

ADOPTED: OCTOBER 29, 2020