EXECUTIVE ORDER NO. 2-97

INFORMATION TECHNOLOGY SECURITY POLICY

WHEREAS, information and information systems are critical and important City of Philadelphia assets, and without reliable and accurate information and information systems the City cannot meet its responsibilities to the citizens of Philadelphia;

NOW, THEREFORE, by the powers vested in me by the Philadelphia Home Rule Charter, it is hereby ordered:

SECTION 1
INFORMATION TECHNOLOGY SECURITY PROGRAM

A. The Mayor's Office of Information Services (MOIS) is hereby assigned the responsibility for citywide information technology security.

B. MOIS, in coordination with the Office of the Inspector General and, with respect to Internet use and access, the Department of Public Property, Communications Division, will establish an Information Technology (IT) Security Program to ensure that information and information systems are properly protected from a variety of threats.

C. The IT Security Program will address all aspects of the information technology environment including, but not limited to, network, desktop computer, mainframe computer, electronic mail, and Internet functions and services.

D. The IT Security Program shall include a compliance assurance program that will educate City employees in applicable laws, regulations, and City policies, establish procedures for enforcing compliance, and periodically evaluate the extent to which City information systems are and are not adequately protected.

SECTION 2
RESPONSIBILITIES

A. MOIS will appoint an Information Technology Security Officer who, under the supervision of the Chief Information Officer (CIO), will define, prescribe, and institute a citywide Information Technology Security Program.

B. MOIS will establish an Information Technology Security Steering Committee to support the prioritization and implementation of security policies and procedures. The members of the Steering Committee will include, but are not limited to, the Managing Director, the Chief Information Officer, the Commissioner of Records, the Commissioner of Public Property, the Inspector General, the City Solicitor, and the Risk Manager, or their designees.

C. MOIS will coordinate with City agency heads to ensure the designation of an IT Security Officer for each agency and the establishment of appropriate functions within each agency to institute IT Security policies and procedures.

D. With the advice of, and in coordination with, the Information Technology Security Steering Committee, MOIS will develop specific policies, procedures and mechanisms to audit, measure, and assure compliance with IT security procedures, including, where appropriate, penalties for violation. On the basis of periodic audits, MOIS will determine the degree to which the City's information and information systems are properly protected and comply with applicable law and regulations.

E. MOIS will develop such policies, procedures, and mechanisms for the following areas of IT activity, and for such other areas as the Information Technology Security Steering Committee and the CIO determine to be appropriate:

- fraud, embezzlement, electronic and physical sabotage, terrorism, extortion, and industrial espionage
- erroneous, inaccurate, and inappropriate data
- privacy
- infringement of copyright and other propriety rights by City personnel and others, including, but not limited to, use and duplication of software in violation of license terms
- electronic mail
- availability of City information and databases to commercial and non-commercial entities and to members of the public
- service interruption and data loss due to technical failures or natural and other disasters
- integrity and security of City information and databases, including protection against unauthorized access and unauthorized disclosure
- security of micro-computers and computer networks
- the City's Internet site
- education of City employees with respect to copyright and other applicable law and IT security policies
- compliance assurance

F. MOIS and the Department of Public Property, Communications Division, will jointly establish a policy and specific procedures governing access to and use of the Internet by City employees. The Department of Public Property, Communications Division, will manage and administer Internet use and access in accordance with such policy and procedures, including, but not limited to, establishing user profiles and access levels, and monitoring and auditing user access through telephone lines, wireless transmission, the Internet firewall, and otherwise.

SECTION 3
RESPONSIBILITIES OF CITY AGENCIES

A. City agencies will, in coordination with the MOIS IT Security Officer, *designate* Agency IT Security Officers and establish appropriate functions to implement IT security policies and procedures.

B. City agencies will institute policies and procedures sufficient to ensure compliance with all laws, regulations, and City policies governing City information systems and the use of computer hardware and software.

SECTION 4
INVESTIGATIONS AND CONTROL

A. Agency IT Security Officers will report serious instances of security violations to the MOIS Information Technology Security Officer and the Inspector General's Office. Security violations may involve any part or aspect of the City's information systems including, but not limited to, local area and citywide networks, software applications, hardware/software systems, data, physical environment, unauthorized access to City premises where IT functions are performed, theft of or damage to computer hardware and other IT equipment, software, or data, unauthorized disclosure of City data, violation of copyright and other applicable law, fraud, and misuse of City information systems.

B. The Inspector General will be primarily responsible for conducting investigations of serious security violations. The Inspector General will inform MOIS, and where appropriate, the Department of Public Property, Communications Division, of the result of its investigations so that security vulnerabilities may be identified and addressed. MOIS and the Department of Public Property, Communications Division, will ensure that the Inspector General is informed of any citywide information security issues, trends and developments.

C. MOIS and the Department of Public Property, Communications Division, will provide technical support to the Inspector General during investigations, collect data to identify IT vulnerabilities, and develop and disseminate policies and procedures to correct security deficiencies.

SECTION 5
EFFECTIVE DATE

This Order shall become effective immediately.

October 6, 1997
Date

Edward G Rendell
Edward G. Rendell, Mayor