Office of the Mayor
Tulsa, Oklahoma

Executive Order No. 2002-01
February 14, 2002

ESTABLISHMENT OF RESPONSIBILITIES AND REQUIREMENTS FOR NETWORKS AND COMPUTER SYSTEMS SECURITY

By virtue of the power vested in me, as Mayor of the City of Tulsa, it is hereby ordered:

Section 1. **PURPOSE**

To establish responsibilities, requirements, standards, and procedures for insuring a high level of security for the City's Metropolitan Area Network, Local Area Networks, Information Systems, and Internet/Intranet Systems.

Section 2. **RESPONSIBILITIES**

A. The Information Technology Steering Committee (ITSC) shall have the following responsibilities:

i. the creation of security policies and procedures for the City's Metropolitan Area Network, Local Area Networks, Information Systems, and Internet/Intranet Systems;
ii. the development and/or recommendation of security training and education programs;
iii. updating of the of personal computer usage policy (HR 819) and Information Systems Security policy (HR 821).

B. The Telecommunications and Information Services Department (ITIS) shall have the following responsibilities:

i. monitor operational security practices;
ii. perform regular systems security tests;
iii. inform Department Heads of the need to correct security deficiencies within the Department Head's department;
iv. if a Department Head does not take the appropriate action to correct a security deficiency, take the necessary actions to resolve the situation;
v. respond, as necessary, to electronic attacks and other problems;
vi. developing and implementing standards for network design, optimization, monitoring, and management;

vii. insure that all devices attached to the City Network are identified by MAC or Internal Protocol Address and assess the security of each device;

viii. maintain an on-going security program to provide control measures and address risks;

ix. present to the ITSC a report on risks, control measures, recent problems and successes in maintaining security on a biannual basis;

x. manage all phases of remote access to the City's Network and insure the Help Desk is aware of the requirements for remote access;

xi. to utilize Network scanning devices to determine if data can be accessed;

xii. Manage City Internet and Intranet connectivity, links, firewalls and any access to the City Network or systems via the Internet.

C. Department Heads shall have the following responsibilities:

i. implement Department security training ;

ii. when informed by IT IS of security deficiencies within the Department, take the appropriate actions to correct the problems;

iii. insure that employees utilizing computers and accessing information sign an "Affidavit for Security Access" and acknowledging the employee has read the Oklahoma Computer Crimes Act, the City's Personal Computer Use Policy, the City's Information Systems Security Policy, the email use policy, and the internet use policy;

iv. retain each employee's "Affidavit for Security Access" in the employee's departmental personnel file.

D. Department Computer System Administrators shall secure all systems permitting null sessions. Each Department should insure that new computer installation include setting personal computers for no null sessions. Where feasible, null session access to all personal computers and servers should be turned off.

Section 3. **NETWORK CONNECTIONS**

A. No connections may be made to the City Network without TISD coordination and approval. To request a connection, a Department Head or designee should contact the Help Desk.

B. TISD will take the take necessary measures to eliminate network exposures to outside agencies, both connected to the network and via the Internet. In the event equipment cannot be secured such connections will be eliminated or access will be routed through discreet firewalls.

C. A Department Head must be approve the use of a modem by anyone in the Department. The Department Head or designee must submit a request to the Help Desk for all existing and new modems. Modems are not to be utilized with Network connected devices, except for vendor diagnostics and support, and special requirements where Internet connection is not viable. Such modems will remain in the "off" state until "on" times are coordinated/scheduled.

D. Anyone wanting to utilize software or techniques that facilitate remote utilization or control of personal computers must obtain the approval of his/her Department Head and TISD.

Section 4. **COMPUTER PASSWORD PROTECTION**

Each Department shall be responsible for password utilization and protection. Employees are required to secure passwords from unauthorized viewing or access. Each Department should test passwords upon creation for toughness. Each Department shall test passwords biannually. TISD shall assist the Departments in testing passwords.

Section 5. **WIRELESS DEVICES**

Purchase and use of wireless devices are restricted. The approval of a Department Head and TISD is required before an employee obtains a commercial/subscription for wireless services and/or network access.

M. Susan Savage, Mayor

FEB 14 2002
Date

CITY OF TULSA OKLAHOMA

ATTEST:

City Clerk

APPROVED:

City Attorney