MUNICIPALITY OF MONROEVILLE

ALLEGHENY COUNTY, PENNSYLVANIA

ORDINANCE NO. 2124

AN ORDINANCE OF THE MUNICIPALITY OF MONROEVILLE AMENDING THE CODE OF THE MUNICIPALITY OF MONROEVILLE, CHAPTER A366, ADDING AN AMENDMENT TO THE EMPLOYEE HANDBOOK

BE IT ORDAINED AND ENACTED, by the Municipality of Monroeville in Council assembled as follows:

SECTION 1. The Municipality of Monroeville hereby adopts an amendment attached Exhibit "A" to the Municipality of Monroeville Employee Handbook for the purpose of adding the following Sections:

SECTION 7.27.3 Computer System Data Security Policy

SECTION 2. Any Ordinance in conflict with said ordinance shall be repealed to the extent of such conflict.

ORDAINED AND ENACTED this 12th day of October, 1999

ATTEST:

Marshall W. Bond
Municipal Manager

MUNICIPALITY OF MONROEVILLI

Sean F. Logan
Mayor

ENTERED INTO LEGAL BOOK: October 22, 1999

SUBJECT: Computer System Data Security Policy
DATE: October 5, 1999

I. POLICY

It is the policy of the Municipality of Monroeville to preserve the confidentiality of department, personnel, business, academic, and research data, to protect this data from unauthorized access or disclosure, and to grant access to this data only on a "need to know" basis. This policy defines appropriate administrative, technical, and physical safeguards to protect the confidentiality, controlled availability, accuracy, and integrity of data managed or maintained by municipal computer systems.

II. PROCEDURE

A. Municipal Manager' designees

The Municipal Manager assigns or authorizes appropriate municipal staff as his designees for normal computer system user account management functions and expedient response to data security issues. These designees may work either within the municipality's Information Systems department or within departments which provide decentralized computer systems services and support.

B. Data Stewardship

1. The Municipal Manager, or designee identifies supervisory positions in user departments or functional areas to serve as stewards for computer system data or functions. For example:

    - Engineering department representatives should be responsible for evaluating and approving requests for access to GIS and Engineering functions.
    - Finance Department representatives should be responsible for evaluating and approving requests for access to finance system functions.
    - Public Safety representatives should be responsible for evaluating and approving requests for access to police, fire, and EMS system functions.

2. The data steward approves access to a function based upon a user's need to know.

3. The data steward is responsible for periodic reviews of data accessibility and recommendations for appropriate access modifications.

Computer System and Data Access

1. Access to all municipal multi-user computer systems should be activated and controlled by computer system user account identification codes and passwords. All requests for computer system user accounts should be made in writing by a data steward or, for functions without stewards, the user's supervisor, thereby certifying the user's need to know. Once a user account has been assigned, the user's supervisor is responsible for monitoring appropriate activity and for communicating information regarding improper activity or a change in a user's job function or status which may require access modification or account termination.

2. All municipal computer system accounts should be secured by a minimum of two account-specific variables: (1) User Identification Code (commonly known as a userid or username); and (2) User Password. The Municipality of Monroeville does not consider the Identification Code to be confidential. However, *the password should at all times be treated by the assigned user as secret*, and all reasonable measures should be taken by the user to protect and maintain this secret status. Passwords should not be disclosed by the user at anytime to anyone for any purpose.

3. A user should be assigned only one computer system account for each computer system, application, or function, unless otherwise authorized by the Municipal Manager, or designee.

4. Upon assignment of an account or passage of this policy, users should be required to sign a "Receipt," certifying that they will comply with all municipal policy and procedure regarding the proper use and handling of confidential municipal data. This receipt should include the user's social security, employee identification number, or other personal identifier, to facilitate secondary authentication within the systems. Computer accounts for which no receipt is signed should be terminated.

5. By accepting and using an account, the assigned user agrees to comply with all departmental and municipal policies regarding proper use and authorized activities. The user agrees to be held accountable to the municipal and its related entities for any liability, demands, claims, damages, suits, or judgments for injury or damage to any person or property, or loss caused by negligence or intentional acts or omissions, in connection with access to and use of municipal computer systems and data, including but not limited to unauthorized access or disclosure of confidential business, research, academic, or other municipal data.

6. Each time a user account is employed to gain access to a municipal system, the assigned user is solely responsible for properly and completely exiting the computer system at the completion of activities.

7. All municipal computer system accounts should be issued for the performance of authorized municipal activities. Unauthorized use of municipal computer accounts is prohibited. "Authorized municipal

activities" are defined as those approved by the user's supervisor, department head, designated data stewards, Municipal Manager, or designee. In the course of normal, authorized activities, users are prohibited from browsing, copying, printing, or otherwise making use of any data other than that for which their computer access has been specifically approved.

8. All data entered into, stored within, reported from, or transported via municipal computer systems is the property of the Municipality of Monroeville. Management reserves the right to observe and review activities by users of these systems. Examples of "management" include police and fire chiefs, administrative department heads, department and program directors, staff members' direct supervisors, and the Municipal Manager. *Users of municipal computer systems should have no expectation of privacy regarding their activities on these systems.*

9. To protect the Municipality's data security interests, information regarding the technical specifications of data security protocols should not be disclosed to any persons or entities outside of the municipality without the permission of the Municipal Manager, or designee.

D. Suspension, Resumption, and Termination of Access

Computer system user accounts shall be suspended for the following reasons, unless otherwise excepted by the Municipal Manager, or designee:

- After five successive failed attempts to gain access via a user account. Such invalid attempts may be the result of unauthorized parties attempting to guess or "crack" the user account. The account should remain suspended pending review by the Municipal Manager, or designee.
- If the account remains inactive for a period of 90 days or more.
- If activity within the account, upon the judgment of the Municipal Manager, or designee, is detrimental to the Municipality or in conflict with municipal policy, procedure, objectives, or intent.

Suspended accounts may be reactivated and access resumed only upon the approval of the Municipal Manager, or designee.

Computer system user accounts shall be terminated for the following reasons, unless otherwise excepted by the Municipal Manager, or designee:

- If the account remains inactive for a period of 180 days or more.
- If the assigned user for the account has a change in job function or position which alters or eliminates the user's need-to-know.
- If the assigned user for the account is terminated from employment or service to the municipality.
- If activity within the account, upon the judgment of the Municipal Manager, or designee, is detrimental to the municipality or in conflict with municipal policy, procedure, objectives, or intent.

E. Use of Computer Workstations

1. Municipal computer workstations, including standalone personal computers and all network-attached devices, should only be used for authorized municipal activities. Unauthorized use of municipal computer workstations is prohibited. "Authorized municipal activities" are defined as those activities approved by the user's supervisor, department head, and/or Municipal Manager, or designee.

2. Municipal computer workstations, including standalone personal computers and all network-attached devices, which may contain confidential municipal data or have the potential to facilitate access to such data, should be protected by reasonable measures from unauthorized use. "Reasonable measures" include device-based power-on or logon password protection, password-secured screen savers, and/or placement of devices in locations which are normally inaccessible to unauthorized parties.

3. Users of computer workstations are responsible for taking reasonable precautions to protect the integrity of applications and data on those systems. The municipality recommends that users of computer workstations perform regular backups of key files or even entire hard drives in an effort to protect the integrity and functionality of these systems.

F. Penalties for Misuse of Access

Misuse of computer user accounts, including but not limited to the unauthorized access or disclosure of confidential municipal data, whether deliberate or accidental, may result in municipal-imposed disciplinary measures up to and including termination of employment, as well as civil and criminal penalties.