Passed: June 15, 2009

RESOLUTION NO. 2009-06-022R

A RESOLUTION ADOPTING IDENTITY THEFT PREVENTION PROGRAM

WHEREAS, the United States Congress has enacted the Fair and Accurate Credit Transactions Act of 2003 which requires that creditors are required to develop written policies and procedures regarding the detection, prevention and mitigation of identity theft.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF URBANA, ILLINOIS, as follows:

That the Identity Theft Prevention Program and the Personal Information Protection Policy attached hereto is hereby adopted.

PASSED by the City Council this 15th day of June, 2009.

Phyllis D. Clark, City Clerk

APPROVED by the Mayor this 24th day of June, 2009.

Laurel Lunt Prussing, Mayor
By: Charles A. Smyth, Mayor Pro-tem

PERSONAL INFORMATION PROTECTION POLICY

WHEREAS, the State of Illinois has enacted a Personal Information Protection Act (815 ILCS 530/1 et seq.); and

WHEREAS, the disclosure of personal information may result in identity theft which is prohibited by Illinois law (720 ILCS 5/16 G-1 seq.); and

WHEREAS, it is appropriate to develop a written policy to protect against the unintentional or inadvertent disclosure of protected personal information.

NOW, THEREFORE, the following Personal Information Protection Policy is hereby promulgated:

1. Purpose. The purpose of this policy is to identify protected personal information and establish operating policies and procedures to protect against the inadvertent disclosure of protected personal information.

2. Protected Personal Information. As used herein shall include the following information whether stored in electronic or printed format and whether belonging to any customer, employee or contractor:

A. Credit card information including the following:

1. Credit card number
2. Credit card expiration date
3. Three (3) digit security code
4. Cardholder name
5. Cardholder address

B. Tax identification numbers:

1. Social Security number
2. Business identification number
3 Employer identification number

C. Payroll information including:

1. Paychecks

2. Pay stubs
3. Tax form
4. Bank account and routing information

D. Cafeteria plan associated paperwork

E. Medical information including but not limited to:
1. Doctor names
2. Insurance claims
3. Prescriptions
4. Any related personal medical information

F. Other personal identifiers including:

1. Date of birth
2. Address
3. Phone number
4. Maiden name
5. Name
6. Customer number
7. Driver's license number or state ID card identification card number
8. Employment identification number

G. Codes and passwords including:

1. Security codes
2. Access codes or passwords to access to financial accounts or City property or information systems
3. Personal identification numbers (PINs)
4. Electronic identification numbers

3. City employees are encouraged to use commonsense judgment in securing protected personal information. If an employee is uncertain of the sensitivity of a particular piece of information, the employee should contact a supervisor for direction. The following policies are designed to guide employees in handling and securing protected personal information.

A. File cabinets, desk drawers, overhead cabinets and any other storage space containing documents with protected personal information will be locked when not in use.

B. Storage rooms containing documents with personal protected information and record retention areas will be locked at the end of each work day or when unsupervised.

C. Desks, work stations, work areas, printers and fax machines and common-shared work areas will be cleared of all documents containing protected personal information when not in use.

D. Whiteboards, dry erase boards, writing tablets, et cetera in common-shared work areas will be erased, removed or shredded when not in use.

E. When documents containing protected personal information are discarded they will be placed inside a locked shred bin or immediately shredded using a mechanic cross-cut or Department of Defense approved shredding device. Locked shred bins are labeled "confidential paper shredding and recycling". Municipal records, however, may only be destroyed in accordance with the State of Illinois Records Retention Policy.

F. Protected personal information may be transmitted using approved municipal email. All protected information must be encrypted when stored in electronic format.

G. Any protected personal information sent externally must be encrypted and password protected and only to approved recipients. Additionally, a statement such as the following shall be included in the email: This message may contain confidential and/or priority information and is intended for the person/entity to which it was originally addressed. Any use by others is strictly prohibited.

H. When discarding devices that contain protected personal information stores in an electronic format, the protected personal information shall be destroyed or wiped clean so that the protected personal information is either unintelligible or destroyed.

4. Exceptions. This policy shall not prohibit the following:

A. The capture or transmission of protected personal information in the ordinary and lawful course of business of the City of Urbana.

B. The use of protected personal information by a peace officer, court office or other law enforcement personnel whether federal, state, or local while in the lawful performance of official duties.

C. The disclosure of protected personal information as allowed pursuant to the Illinois Freedom of Information Act, the Illinois Open Meeting Act or any other applicable law or court order.