City of Phoenix

ADMINISTRATIVE REGULATION	A.R. NUMBER 1.90 revised
	FUNCTION General
SUBJECT INFORMATION PRIVACY AND PROTECTION	Page 1 of 5
	EFFECTIVE DATE March 19, 2009
	REVIEWED DATE

I – Purpose

Maintaining information privacy and protection is essential to preserving the City's high level of public trust. This Administrative Regulation (AR) establishes Citywide policies to protect personal identifying information (PII) and restricted City information regardless of its format (i.e. electronic, computerized or hard copy formats). Information is defined as any data or record collected, obtained and/or maintained by the City of Phoenix. This AR applies to all employees, contractors and third parties with access to City information. For more information specific to contractors and third parties, see Administrative Regulation 1.91. Any questions should be directed to the City Privacy Officer/Information Technology Services.

II – Definitions

1. Personal Identifying Information: refers to any information that identifies and describes an individual, including but not limited to, the individual's first name and last name, or first initial and last name **combined** with:

   - *private information* – examples include residence or mailing address, telephone number, protected health information, date of birth, mother's maiden name, etc.; or

   - *government-issued identifiers or information* – examples include Social Security Number, driver's license or non-operating identification number, citizenship status or alien identification number, tax identification number, etc.; or

   - *financial account information* – examples include credit card or debit card numbers, savings or checking account numbers, any other security entitlement account number, retirement account number, account passwords or access codes, etc.

2. Restricted City Information: information for which unauthorized access, modification, or loss could have a negative affect on the City or the public. Examples include sensitive public infrastructure and/or utility information, all information exempt from public disclosure under state or federal public records laws, customer databases, employee personnel records and information, selected procurement information, licensed proprietary or copyrighted information, and security information.

3. Breach of Information Security (Breach): unauthorized acquisition of and access to personal identifying and restricted City information. Good-faith acquisition of personal identifying and restricted City information by a City employee or agent is not a breach of information security, provided the information is not used for a purpose unrelated to City business or subject to further willful unauthorized disclosure.

4. Critical Breach of Information Security (Critical Breach): unauthorized acquisition of and access to unencrypted or unredacted computerized information that contains an individual's first name or first initial and last name in combination with one or more of the following: (1) the individual's Social Security Number, (2) driver's license or non-operating identification number, (3) financial account number or credit/debit card number in combination with any required security code, access code or password that would permit access to the individual's financial account. In addition, access to this information must materially compromise the security or confidentiality of the information maintained and cause or be reasonably likely to cause substantial economic loss to an individual. Good-faith acquisition of this information by a City employee or agent is not a critical breach of information security, provided the information is not used for a purpose unrelated to City business or subject to further willful unauthorized disclosure.

III – Securing Personal Identifying Information and Restricted City information

Personal identifying information and restricted City information should only be accessed in order to perform specific job-related responsibilities or assignments. All employees should comply with their department's Information Management Plan, which establishes departmental policies for collecting, managing and securing personal identifying information and restricted City information collected or obtained in the course of conducting City business.

Personal identifying information and restricted City information, whether in electronic format or hard copy, should be secured and protected at all times to avoid unauthorized access. When not in use, users should ensure this type of information is physically secured or protected through approved electronic methods. When this type of information is saved to laptop computers, computerized devices, or removable storage devices, the data should be protected through a City-approved method, such as encryption or password protection, and the equipment or device itself should be secured by storing it in a locked desk, cabinet, or by another appropriate method when not in use.

When personal identifying information and restricted City information, regardless of its format, is no longer necessary or exceeds record retention requirements, the information should be redacted or destroyed through appropriate and secure methods. For appropriate authorization and disposal of public records, follow established procedures outlined in AR 1.61 Records Retention Policy. For information on disposal of electronic media, contact Information Technology Services.

Separate and apart from the requirements for protecting personal identifying information as defined previously in this AR, employees are reminded that Social Security Numbers or financial account information should never be disclosed.

Any concerns regarding the unauthorized access to or inappropriate use of personal identifying information and restricted City information should be reported to an employee's immediate supervisor as soon as possible. In the event of a potential critical breach of information security, the Department Head and City Privacy Officer shall also be notified.

IV – Information Management Plan

Each City department will develop an Information Management Plan establishing policies for collecting, managing and securing personal identifying information and restricted City information generated, collected, or obtained in the course of conducting City business. Departments should develop an inventory of the information they currently collect, use and/or store, including information shared with another department or business entity. The Plan should:

- identify all departmental personal identifying information and restricted City information regardless of format
- limit or eliminate collection and/or storage of redundant or unnecessary personal identifying information and restricted City information
- define appropriate measures to be taken to ensure privacy and security of personal identifying information and restricted City information
    - computerized information – procedures ensuring information is protected through a City-approved method and appropriate connectivity in accordance with relevant City AR's and IT standards as well as applicable regulatory, legal, and contractual requirements
    - hard copy – procedures for assuring that files or documents containing personal identifying information and restricted City information are secure when not in use or when removed from the office for business purposes
- outline departmental policies for the creation, access, use and destruction of personal identifying information and restricted City information
- identify appropriate levels of access for personal identifying information and restricted City information, and all positions with potential access

- identify procedures for sharing information with private and third-party requests that meet public records laws without violating privacy laws or interests

- Every Department which accepts credit/debit cards is responsible for ensuring reasonable steps are taken to identify how the department intends to comply with payment card industry (PCI) standards (refer to A.R. 3.96 for specific requirements)

- outline strategies that will be used to inform and educate employees regarding information privacy and protection

Department Heads are responsible for assuring the department's Information Management Plan complies with all applicable laws, regulatory requirements, City policies and contractual requirements. To assist departments with ensuring they meet this requirement, questions regarding the nature, scope or extent of personal identifying information and restricted City information should be reviewed with the Law Department. Public records management or record retention requirements should be reviewed with the City Clerk Department. Infrastructure requirements and methods for appropriately protecting computerized data should be reviewed with Information Technology Services.

Departments are responsible for maintaining current Information Management Plans. Plans should be revised as appropriate when business processes change that affect personal identifying information or restricted City information. At a minimum, departments shall review their Plans annually. Copies of the initial plan and any updates should be submitted to the City Privacy Officer, who may circulate it for review by a team of representatives including the Law, City Clerk, Personnel and Information Technology Services Departments. The City Privacy Officer shall also maintain a central repository of all current department Plans.

V – Handling Unauthorized Access, Disclosure or Loss of Personal Identifying Information and Restricted City information

Each department is responsible for ensuring reasonable steps are taken to ensure the privacy, integrity and security of personal identifying information and restricted City information is maintained. These steps include:

- All potential breaches of information security shall be reported up the supervisory chain of command to the Department Head. In the event of a potential critical breach of information security, the City Privacy Officer shall also be notified.

- An investigation shall be conducted, subject to the needs of law enforcement, taking necessary measures to determine the nature and scope of the incident. An investigative summary shall be forwarded to the City Privacy Officer for his/her review and recommendations.

- If the investigation reveals a critical breach of information security, the City Privacy Officer shall notify the City Manager's Office. The City Manager, or his/her designee, in consultation with the Law Department and Public Information Office, shall determine how the affected individuals or organizations will be notified.

- The City is only obligated to notify individuals affected by ***critical*** breaches of information security. Although not legally required to do so, the City may choose to issue notifications regarding other breaches. All notifications must be approved by the Public Information Office and the City Manager, or his/her designee.

- The City shall take all appropriate actions to address unauthorized use and/or recover lost or stolen personal identifying information and restricted City information.

VI – Acknowledgement

Departments are responsible for ensuring all affected employees, business partners and third parties are aware of and trained on the department's Information Management Plan and this AR. At a minimum, follow-up training shall occur annually and any time the department's Plan is revised.

VII – City Auditor Department

The City Auditor Department will conduct periodic audits to evaluate compliance with the responsibilities set forth in this AR. Those audits will include departmental assessments of Information Management Plans and the department-specific policies, procedures, and mechanisms in place to ensure sustained compliance with those Plans.

VIII – Violation of this Policy

Violation of this AR may be subject to disciplinary action up to and including termination.

FRANK FAIRBANKS, City Manager

By: _____
Lisa Takata
Executive Assistant to the City Manager