**City of Phoenix**

| ADMINISTRATIVE REGULATION | A.R. NUMBER<br>1.91 revised |
|---|---|
| | FUNCTION<br>General<br>Page 1 of 3 |
| SUBJECT<br>**INFORMATION PRIVACY AND PROTECTION SUPPLEMENT – DATA SHARED WITH THIRD PARTIES** | EFFECTIVE DATE<br>March 19, 2009 |
| | REVIEW DATE |

## I – Purpose

This Administrative Regulation (AR) is intended to supplement AR 1.90, Information Privacy and Protection, by providing guidance for City Departments when sharing data, including personal identifying information and restricted City information, with a third party. Maintaining information privacy and protection is essential to preserving the City's high level of public trust. All City employees and Departments share responsibility for ensuring information collected and maintained by the City is adequately protected. This AR does not address public records requests, but rather, instances when the City is sharing data with external business partners. Any questions should be directed to the City Privacy Officer/Information Technology Services.

## II – Definitions

1. The definitions set forth in AR 1.90 are incorporated by reference to this AR.

2. Third Party: refers to any non-City employee, entity or organization to whom the City may provide information in the course of performing City business. Examples include vendors, consultants, contractors, insurance companies, credit bureaus, residents, and other government entities.

## III – Department Responsibilities

Individual departments are responsible for the oversight of third parties who have access to the department's data, including personal identifying information and restricted City information.

Prior to sharing personal identifying information and/or restricted City information with a third party, the department must complete each of the following steps:

- Document in its Information Management Plan why sharing personal identifying information or restricted information with third parties is necessary.

- Clarify in its Information Management Plan the data being shared that is to be considered personal identifying information and/or restricted information.

- Require the third party to comply with state, federal, and local privacy laws, and City policies.

- Verify whether the third party conducts background checks of its employees and any other individuals who will have access to the personal identifying information and restricted City information it receives from the department. Require third-party employee credentialing and bonding for these employees.

- Verify whether the third party has appropriate data security systems and procedures, including transfer safeguards, disposal procedures, breach response and notification procedures.

- Require third parties to acknowledge that they are prohibited from releasing information to other independent parties and from using the information for any purpose other than that which it received the information.

- Require the third party to notify the contracting City department immediately if a breach is suspected.

- Require the third party to acknowledge that it is prohibited from notifying individuals affected by a breach or critical breach of the City's information without the prior written consent of the City. The third party must also acknowledge that it will be responsible for costs incurred by the City to investigate potential breaches and/or to notify those affected. The third party must also acknowledge that it will be responsible for any costs the City incurs to defend itself, including attorneys' fees, and for any monetary damages or penalties the City is assessed as a result of breaches of information resulting from the third party's negligence.

- Include provisions in written contracts with third parties that require data security safeguards. Where the business relationship with the third party is not conducive to the execution of a written contract, the department must enter into a Data Security Agreement with the third party.

**IV – Contracts and/or Data Security Agreements**

In light of the above responsibilities, departments shall enter into written agreements that detail the City's expectations regarding information privacy and protection. The Law Department shall be consulted and must approve all contract language.

Where a City Department is required by state, federal, or local law to disclose information to a third party and that information includes personal identifying information and restricted City information, a written agreement will not be required.

The Municipal Court is subject to the administrative supervision of the Arizona Supreme Court pursuant to Article VI, § 3, of the Arizona Constitution and is exempt from the requirements of this AR to the extent such requirements may be inconsistent with Rules and Administrative regulations of the Arizona Supreme Court.

**V – 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 not only assessments of department-specific policies, procedures, and mechanisms in place to ensure sustained compliance with this AR, but also assessments of the information security measures implemented by the third party.

**VI – 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