

AUDIT REPORT TRACKING SYSTEM (ARTS)

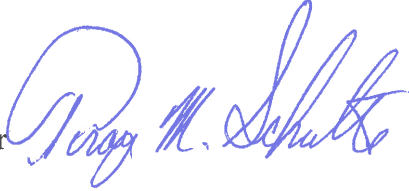
SECTION I: SUMMARY INFORMATION			
Audit Title:	The City Should Follow Recommended Practices to Protect Personally Identifiable Information	Audit Release Date:	04/26/2015
Department:	City Manager	Last Report Date:	06/06/2018
Department Director:	Troy Schulte	This Report Date:	08/21/2018
Contact Person/Phone:	Kimiko Gilmore/36558	Expected Presentation Date:	09/19/2018
SECTION II: RECORD OF IMPLEMENTED RECOMMENDATIONS			
1. Implemented 08/2018		3. Implemented 08/2018	
2. Implemented 08/2018		4. Implemented 08/2018	
SECTION III: SUMMARY OF IMPLEMENTATION EFFORTS			
Recommendation 1: The city manager should identify all personally identifiable information the city collects and stores and evaluate the confidentiality impact level of the information.			
<i>Status of Recommendation: Implemented</i>			
In mid-August 2018 Administrative Regulation 1-32 was approved by the City Manager. AR 1-32 outlines the process for Department Directors to initiate that a PII inventory is implemented in each department.			
Recommendation 2: The city manager should periodically review and eliminate the collection of unnecessary personally identifiable information.			
<i>Status of Recommendation: Implemented</i>			
The proposed system has been reviewed by Law. The recommendations have been incorporated in to AR 1-32.			
Recommendation 3: The city manager should develop citywide policies and procedures, including training and other safeguarding controls, for protecting the confidentiality of the personally identifiable information.			
<i>Status of Recommendation: Implemented</i>			
The proposed system has been reviewed by Law. The recommendations have been incorporated in to AR 1-32.			
Recommendation 4: The city manager should develop a response plan for incidents of misuse, unauthorized disclosure or access, or other breaches of personally identifiable information.			
<i>Status of Recommendation: Implemented</i>			
The proposed system has been reviewed by Law. The recommendations have been incorporated in to AR 1-32.			
SECTION IV: ADDITIONAL OUTCOMES			
Initial implementation of AR 1-32 will need to be monitored to ensure that Department Directors are following these guidelines. Other than the aforementioned concern we do not anticipate any unforeseen challenges.			

CITY OF FOUNTAINS
HEART OF THE NATION



KANSAS CITY
MISSOURI

Office of the City Manager

DATE: August 20, 2018
TO: Department Directors
FROM: Troy M. Schulte, City Manager 
SUBJECT: Personally Identifiable Information (PII) Administrative Regulation

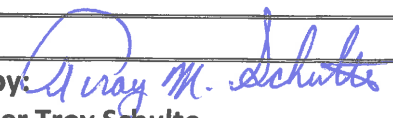
The purpose of the *Personally Identifiable Information (PII) Administrative Regulation 1-32* is to ensure that any information collected by the city is protected, in both paper and electronic forms, from loss, misuse or unauthorized disclosure. This information includes, but is not limited to social security numbers, financial account numbers, medial information, tax information, driving records and employment information.

According to the National Institute of Standards and Technology (NIST), Guide to Protecting Confidentiality of PII organizations should use a combination of measures, including operational safeguards, privacy specific safeguards and security controls.

- 1.1 Operational safeguards include policy and procedure creation, awareness, training and education.
- 1.2 Privacy safeguards include: minimizing the use, collection and retention of PII, conducting privacy impact assessments, de-identifying information and anonymizing information.

Per the adoption of AR 1-32, please implement the outlined processes to safeguard all sensitive information collected. Additional resources on the appropriate processes and procedures can be found in section 5.1 of the PII AR.

Cc: Alyssa Dinberg, Cookingham-Noll Management Fellow

Title: Personally Identifiable Information (PII)	
AR No. 1-32	Approved by:  City Manager Troy Schulte
Effective Date: 8-31-2018	Supersedes:

1.0 PURPOSE

To ensure that Personally Identifiable Information (PII) collected by the city is protected, in both paper and electronic forms, from loss, misuse or unauthorized disclosure.

2.0 ORGANIZATIONS AFFECTED

All departments, employees and contractors.

3.0 DEFINITIONS

3.1 Personally Identifiable Information (PII) - Any information that can be used to identify an individual or can be linked to an individual and that can be protected under the Missouri Sunshine Law (Sections 610.010-610.200, RSMo) or that must be protected by some other law.

3.1.1 Examples include, but are not limited to social security numbers, financial account numbers, medical information, tax information, driving records and employment information.

3.2 PII Confidentiality Safeguards – According to the National Institute of Standards and Technology (NIST), Guide to Protecting Confidentiality of PII organizations should use a combination of measures, including operational safeguards, privacy specific safeguards and security controls.

3.2.1 Operational safeguards include policy and procedure creation, awareness, training and education.

3.2.2 Privacy safeguards include: minimizing the use, collection and retention of PII, conducting privacy impact assessments, de-identifying information and anonymizing information.

3.3 PII Monitor – A staff person assigned by a department director to provide oversight and security of department PII.

3.4 PII Review – A periodic analysis of PII used by a department.

4.0 POLICY

Staff of the City of Kansas City, Missouri will employ reasonable and appropriate administrative, technical, and physical safeguards to protect the integrity, confidentiality, and security of all PII regardless of its source, ownership or the medium used to store it. All individuals who dispense, receive, and store PII have responsibilities to safeguard it. While the confidentiality of PII must be maintained, the City is bound to follow the Missouri Sunshine Law and its goals of transparency and openness in government. The Missouri Sunshine Law is to be liberally construed in favor of openness. Any questions regarding the Missouri Sunshine Law should be directed to the City Attorney's Office.

5.0 PROCEDURES

5.1 *Resources*

5.1.1 It is recommended that Department Directors (Director), PII Monitors (Monitor) and staff responsible for PII collection should use the following resources:

5.1.1.1 Guide to Protecting the Confidentiality of Personally Identifiable Information, Special Publication 800-122;
<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf> or latest version.

5.1.1.2 Administrative Regulation 1-16 at
<https://kcmo.sharepoint.com/Lists/Administrative%20Regulations/Attachments/17/AR%201-16%20Technology%20Procurement,%20Use%20and%20Security.pdf>

5.1.1.3 Manual of Instruction No. 3-28 Records & Information Management Instructions at
<https://kcmo.sharepoint.com/Lists/Manual%20of%20Instruction/Attachments/283/MI%203-28%20Revised%202-16-2015.pdf>

5.1.1.4 All staff should use additional department resources specific to state, federal and/or other requirements.

5.1.1.5 Any changes resulting from PII Reviews will be communicated by the Monitors to all staff at the time the change occurs and will be incorporated into future training sessions.

5.2 *Inventory*

5.2.1 All PII will be categorized according to the purpose, amount, types, locations, accessibility or other labels as deemed necessary.

5.2.1.1 Collection of PII will be terminated if said information ceases to be relevant and necessary for city purposes.

5.3 Monitoring

5.3.1 Directors will be responsible for ensuring that PII collected by department staff is protected, in both paper and electronic forms, from loss, misuse, or unauthorized disclosure.

5.3.1.1 Directors will ensure that staff is properly trained and familiar with PII as it relates to city and department operations.

5.3.2 Directors or their designees are required to conduct an annual PII Review to identify all PII collected by staff in the course of daily operations.

5.3.2.1 PII Review dates will follow the fiscal year; May 1st thru April 30th.

5.3.3 PII Monitors will provide oversight and security of PII.

5.3.3.1 Monitors should be notified of any issue regarding the loss, misuse or unauthorized disclosure of PII.

5.3.3.1.1 The Monitor will inform the Director of any issue that needs to be addressed.

5.3.3.1.2 The Monitor will inform IT and RM of any issue(s) and work with those divisions to resolve. When it is determined that the issue(s) have been adequately addressed the Monitor will report the outcome to the Director who will determine if any further action needs to be taken.