

City of Detroit

CITY COUNCIL

DENZEL ANTON MCCAMPBELL
COUNCIL MEMBER, DISTRICT 7

MEMORANDUM

TO: David Whitaker, Director
Legislative Policy Division

Art Thompson, Chief Information Officer
Department of Innovation and Technology

Todd Bettison, Chief
Detroit Police Department

THRU: Council President James Tate

FROM: Council Member Denzel Anton McCampbell *D.A. McCampbell*

DATE: April 16, 2026

RE: Further Follow-Up on City Contracts Involving Data Sharing with Third Parties

Thank you for your report regarding third-party data-sharing agreements. As we continue working toward greater data transparency and safety, please provide a response to the following questions:

- 1) At the FY27 budget hearing, DoIT stated it has deployed SecureLink, a security tool that tracks and monitors vendor access to city systems, including clicks and file exports. Please provide responses to the following:
 - a. When was SecureLink deployed?
 - b. What conduct does DoIT consider malfeasance sufficient to void a contract?
 - c. How is unauthorized data use determined, and what are the steps taken when a potential violation is identified?
 - d. Are vendors aware of SecureLink? May vendors opt out of monitoring, and if so, what are the consequences (e.g., loss of data access or contract termination)?
 - e. Given that vendors are permitted to export data, what proactive oversight measures are in place to prevent malicious use? For example, when data breaches occur, does DoIT review the breach to determine whether Detroit data was compromised?
- 2) Please elaborate on the oversight process for data protection. In your March 20, 2026, response, you stated that “oversight is maintained through departmental controls and enforced through the City’s standardized contract provisions.” Specifically, what

City of Detroit

CITY COUNCIL

proactive steps are being taken, and how frequently? Does oversight responsibility rest with DoIT or with the lead department for each contract? What tools are used to conduct this oversight?

- 3) Does the city require vendors to notify DoIT or another department in the event of a data breach or suspected unauthorized access? If so, what is the required notification timeline, and what is the city's protocol upon receiving such notice?
- 4) Has the city conducted a comprehensive data inventory to identify what resident data is currently held, where it is stored, and which vendors have access to it? If so, when was it last updated, and is it available for council review?
 - a. Please provide a list of all current and expired contracts and vendors over the past ten years that have and had access to Detroit's data.
- 5) Please describe the process by which DoIT and DPD determined that Flock Safety did not use Detroit's data in a manner that breached the contract. Was this determination based solely on internal review, or were external audits or third-party assessments conducted?
- 6) Currently, what are the penalties, fines, and remedies, both contractual and legal, available to the city in the event of unauthorized data use by a vendor?
- 7) Please provide a status update on the data security working group, including:
 - a. Name of Working Group
 - b. Current membership (what departments, stakeholders (internal/external) make up the working group)
 - c. Meeting frequency
 - d. Meeting Schedule
 - e. Outcomes of meetings to include: identified shortfalls and solutions (including governance policies, ordinances, or frameworks) under development, implementation, or review
 - f. Timeline for adoption
 - g. How this working group will address data protection as the city expands its use of artificial intelligence, including safeguards to prevent city data from being used to train, troubleshoot, or improve AI models.

Please do not hesitate to contact my office if you have any questions. Thank you.

Cc: Honorable Detroit City Council
Louise Jones, City Clerk's Office
Malik Washington, Director of City Government Affairs