

Draft surveillance technology policy

1. Council approval required. Prior City Council approval is required for any acquisition, funding (including acceptance of grant funds), use or expansion of the use of surveillance technology. Any such Council approval shall clearly define the proposed technology and data to be collected and all purposes for which such technology and/or data may be used.

2. Technology requirements. Any surveillance technology must operate as a closed-loop system, be wholly owned by the City, reside within City-owned facilities and equipment, and have no cloud-based storage or third-party access.

3. Limits on Use of data. Any data collected by such a surveillance technology may be accessed only by licensed officers of the RWPd in connection with an active criminal pursuit or active criminal prosecution, or by the City Administrator in connection with access monitoring duties. The data may be shared with non-RWPd licensed peace officers only in connection with: (1) an active criminal pursuit with the approval of the RWPd Chief of Police, or (2) pursuant to a valid warrant, subpoena, or other legal compulsion specific to the data being sought, with the approval of the RWPd Chief of Police.

4. Deletion of data. All data must be permanently deleted after [60] days if not the subject of an active criminal case.

5. Log-in access required. No data may be accessed without the creation of a user log prior to access.

6. Monitoring of access. The City Administrator shall review the log every 30 days to ensure that all log-ins are authorized and access to the data is being maintained in a manner consistent with the policy.