

RESOLUTION R-5102

1 A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF KIRKLAND
2 APPROVING AN INTERLOCAL AGREEMENT BETWEEN KING COUNTY
3 AND THE CITY OF KIRKLAND FOR USE OF ELECTRONIC FINGERPRINT
4 CAPTURE EQUIPMENT.
5

6 WHEREAS, the Automated Fingerprint Identification System
7 (AFIS) has proven to be an effective crime-fighting tool in furtherance
8 of the health, welfare, benefit and safety of the residents within King
9 County; and
10

11 WHEREAS, since January 1, 2013, the County has continued to
12 provide effective AFIS services to public law enforcement agencies
13 within King County, through a voter approved six (6) year levy, as
14 authorized by King County Ordinance No. 17381; and
15

16 WHEREAS, the City of Kirkland wishes to use AFIS services
17 through Electronic Fingerprint Capture Equipment ("FP Equipment")
18 including the necessary software and computer equipment, and system
19 maintenance services; and
20


21 WHEREAS, Chapter 39.34 RCW authorizes the parties to enter
22 into an interlocal cooperation agreement to perform any governmental
23 service, activity or undertaking which each contracting party is
24 authorized by law to perform.
25

26 NOW, THEREFORE, be it resolved by the City Council of the City
27 of Kirkland as follows:
28

29 Section 1. The City Manager is authorized and directed to
30 execute on behalf of the City of Kirkland an interlocal agreement
31 substantially similar to that attached as Attachment "A", which is entitled
32 "Interlocal Agreement Between King County and the City of Kirkland for
33 Use of Electronic Fingerprint Capture Equipment."
34

35 Passed by majority vote of the Kirkland City Council in open
36 meeting this 3rd day of February, 2015.
37

38 Signed in authentication thereof this 3rd day of February, 2015.


MAYOR

Attest:


City Clerk

EXHIBIT A
FINGERPRINT EQUIPMENT
REQUIREMENTS

I. LIVESCAN SPECIFIC REQUIREMENTS

A. Environmental

The County shall provide an Uninterruptible Power Supply ("UPS") to be used with the Livescan equipment at no cost to the Agency.

The Agency shall provide the County with a minimum of two fixed IP addresses to be used only for the Livescan system and fingerprint card printer.

Cities must provide the proper environment for the Livescan, to include:

1. Consistent temperature ranging from 60 to 80 degrees Fahrenheit.
2. Consistent humidity ranging from 20% to 80% non-condensing.
3. Network connections no more than 3-4 feet from equipment.
4. Total of 4 power outlets within 3-4 feet of the Livescan system.

Note: It is recommended that Cities have a dedicated 120V, 15Amp, 60Hz power line for the Livescan to avoid circuit overload.

B. Local Interfaces

Livescans may be integrated with local records management systems provided that:

1. All development and installation costs are paid by the Agency
2. The integration specifications are provided for review and approval by the County prior to implementation
3. The integration is tested by the County prior to implementation

C. Fingerprint, Palmprint and Arrest Record Transmission

1. All Agency criminal misdemeanor, gross misdemeanor, and felony fingerprints and palmprints, on both adults and juveniles, will be electronically transmitted to the King County Regional AFIS database for search and registration.
2. The King County Regional AFIS will transmit the Agency's fingerprint images, charge and demographic data, electronically to the Washington State Patrol for processing.
3. The Agency will be solely responsible for the accuracy of all demographic and charge information on its fingerprint and palmprint submissions. The County will not edit any suburban Agency demographic or charge information prior to submitting to Washington State Patrol.

II. MOBILE IDENTIFICATION SPECIFIC REQUIREMENTS

The Agency must provide the proper environment for the Mobile ID software, to include:

- A. The Mobile Data Terminal or patrol vehicle mounted laptop running Windows 7 (32 or 64 bit) operating system.
- B. The patrol vehicle must be a physically secure location according to current Criminal Justice Information Services Security Policy.

III. QUALITY CONTROL

Maintaining the quality of the Regional AFIS database is important in order to continue our region's ability to identify criminals and solve crimes. The Agency shall submit electronically captured fingerprints and palmprints (where applicable) to the Regional AFIS database that are of the best possible quality. The County will provide training to Agency staff, either through the FP Equipment Contractor or the County. The Agency and County will work together to ensure that all users are trained to competency. The County will review the quality of electronically captured prints and inform Agency of operators not meeting standards. These operators may be required to repeat training, and must improve their overall quality, in order to maintain access to the FP Equipment.

IV. NETWORKING

The Agency will provide coordination of Agency IT staff, when needed, to ensure secure networking is in place.

The Agency shall report, in advance when possible, all network changes and/or outages which have the potential to disrupt FP Equipment connectivity. Reporting can be made via the King County Service Request Line (206-263-2777) or the AFIS IT mailbox (AFISITHelp@kingcounty.gov).

V. SECURITY

A. Roles and Responsibilities

Each participating Agency is responsible for establishing appropriate security control.

All member Cities shall provide security awareness briefing to all personnel who have access to King County FP Equipment.

B. Monitoring

All access attempts are logged and/or recorded and are subject to routine audit or review for detection of inappropriate or illegal activity.

Security-related incidents that impact County FP Equipment data or communications circuits shall be reported immediately upon discovery by the Agency to the King County Regional AFIS Program.

C. Physical Security

Cities must assume responsibility for and enforce the system's security standards with regard to all Cities and users it services. The Agency must have adequate physical security to protect against any unauthorized access to FP Equipment, or stored/printed data at all times.

D. Network Environment Security

Cities hosting the connection of FP Equipment shall ensure adequate security measures are taken to provide protection from all forms of unauthorized and unsolicited access to FP Equipment. These security measures will be in compliance with Federal Information Processing Standard (FIPS) 140-2.

Cities are required to provide, manage, and maintain a firewall that segments the FP Equipment from any foreign non-public safety networks.

Any exceptions to this or any other network security requirement must be approved by the Regional AFIS Manager under the guidance of King County by and through its Sheriff's Office Information Services Section and King County Information Technology.

If a security breach occurs and personal identifiable information or confidential data is released or compromised, the host Agency shall bear the responsibility and costs to notify affected individuals whose information was released or compromised. This will be completed in accordance with any applicable state or federal laws.

EXHIBIT B



**BIOMETRIC HANDHELD FINGERPRINT IDENTIFICATION POLICY
King County Regional Automated Fingerprint Identification System (AFIS)**

I. PURPOSE

To provide direction for the use of the biometric handheld fingerprint identification devices, more commonly known as a mobile identification device or Mobile ID. If an agency wishes to adopt its own or deviate from this policy, the agency must present its request to the Regional AFIS Manager.

II. PROGRAM

King County's regional AFIS program has initiated a Mobile ID project, involving the use of wireless remote fingerprint identification throughout the county. The project is designed to assist in identifying persons whose identities are in question. While the fingerprint verification process already exists in King County, Mobile ID moves this function to law enforcement first responders, resulting in a more timely identification process.

The system scans the fingerprints at the Mobile ID device and transmits wirelessly to the King County AFIS. If the fingerprints are in the AFIS database, a positive match returns the person's specific identifiers to the Mobile ID device or officer's mobile computer.

In the future, a simultaneous search may also be conducted to search Washington State Patrol's AFIS database and an FBI database known as the Repository for Individuals of Special Concern (RISC).

- A. Only officers trained by AFIS program staff and operating under the guidelines of the Mobile ID project may use the device.
- B. In the event that lack of usage by the assigned officer is a concern, the AFIS program will communicate with the agency and provide retraining and/or direct a reassignment of the device.
- C. Any use of the device not consistent with this policy and/or law enforcement purposes may result in reassignment or forfeiture of the device, and/or a deactivation of access to the AFIS database. Additionally, any violation of the Mobile ID policy/procedure, or of federal or state law, may subject the officer to internal discipline by his/her agency.

III. PROCEDURE

The use or retention of any Mobile ID-collected data shall conform to federal and state laws. It must also conform to individual agency policy as well as the AFIS program procedure as follows:

- A. An officer may use Mobile ID when there is probable cause to arrest a suspect.
- B. An officer may also use Mobile ID during a Terry Stop based upon reasonable suspicion. If a person provides a driver's license or other valid means of identification, or gives the officer a name that can be confirmed through a driver's license check, that form of identification should suffice without the use of Mobile ID. However, if there are articulable facts that give rise to reasonable suspicion regarding the accuracy of a person's identity, the officer may use Mobile ID to verify identity.
- C. Absent probable cause or reasonable suspicion of criminal activity, a person may consent to an officer's request to use Mobile ID. However, the consent must be voluntary as defined by current Washington case law; i.e., the person must be informed that he/she has a right to refuse the officer's request.
- D. Use of the device shall be documented in any report generated as a result of the contact. The officer must articulate the specific facts that support the basis for the use of Mobile ID and must state the voluntary compliance of the Mobile ID if used without arrest, probable cause, or reasonable suspicion.