INTERAGENCY CONNECTION AGREEMENT

BETWEEN

King County Regional Automated Fingerprint Identification System (AFIS),

a regional program of King County and under the administration of the

King County Sheriff's Office, hereinafter referred to as "KCRA",

AND

MERCER ISLAND PD, hereinafter

referred to as "AGENCY".

FOR THE USE OF

Electronic Fingerprint Capture Equipment to assist law enforcement personnel in the identification process hereinafter referred to as "livescan devices".

THIS AGREEMENT is entered into between KCRA and AGENCY, which may be referred to collectively as "Organizations."

WHEREAS, KCRA has proven to be an effective crime-fighting service in furtherance of the health, welfare, benefit and safety of the residents within King County; and

WHEREAS, Since January 1, 2019, the County has continued to provide effective AFIS services to public law enforcement agencies within King County, through a voter approved six (6) year levy, as authorized by King County Ordinance No. 18674;

WHEREAS, AGENCY wishes to use AFIS services through Electronic Fingerprint Capture Equipment ("Livescan devices") including the necessary software and computer equipment, and system maintenance services;

NOW, THEREFORE, for and in consideration of the promises and covenants contained in this Agreement, the organizations hereto agree as follows:

This agreement is for KCRA to unify responsibility and ensure adherence to system procedures and policies within the AGENCY approved for usage of the LIVESCAN DEVICES. This applies to LIVESCAN DEVICES previously approved for usage by the AGENCY and LIVESCAN DEVICES approved for usage by the AGENCY during the term of this agreement.

The interconnection between KCRA and AGENCY is for the express purpose of exchanging data on LIVESCAN DEVICES, owned by KCRA, and SYSTEMS owned by AGENCY.

The expected benefit of the specified interconnection is to provide regional agencies with LIVESCAN DEVICES for identification services with AFIS search capability at KCRA, and Western Identification Network (WIN).

Both ORGANIZATION's users, including system and security administrators, are expected to protect all data / information types described in this agreement in accordance with the latest CJIS Security Policy, this agreement, and any applicable agency security policies.

Period of Performance

This agreement replaces any previous Interagency Connection between the KCRA and the AGENCY. This agreement is effective on the date of the last signature and continues until the status of services changes.

Suspension and Termination

KCRA reserves the right to suspend services under this Agreement if, in its reasonable judgment, AGENCY has violated any material provision. A material breach includes any failure to comply with the terms outlined in this Agreement or any substantive requirement imposed by applicable federal or state laws, regulations, or rules.

If AGENCY commits a material breach and fails to remedy it within thirty (30) business days after receiving notice from KCRA, KCRA may terminate this Agreement without further notice.

Neither KCRA nor the AGENCY will be liable for any indirect, incidental, consequential or special damage under this agreement arising solely from the termination of this Agreement in accordance with its terms.

References

The following documents and procedures are incorporated by reference and made part of this agreement:

I. CJIS Security Policy;
II. Title 28, Code of Federal Regulations, Part 20;
III. Computer Incident Response Capability (CIRC);
IV. Applicable federal and state laws and regulations;
V. King County Information Classification Policy;
VI. Exhibit A: Livescan Requirements;
VII. Exhibit B: Livescan Contacts and References;
VIII. Exhibit C: Livescan User Policy.

Definitions

AFIS refers to Automated Fingerprint Information Services. It's the biometric system that uses a database to store fingerprint records and compare them for identification purposes.

CJI refers to Criminal Justice Information.

LIVESCAN SERVICES refers to services provided with LIVESCAN DEVICES such as (but not limited to) AFIS database searches, fingerprint capture, booking/demographic import.

SECURITY INCIDENT refers to an event or series of events that negatively impact information systems, data, or operations. It may involve unauthorized access, data breaches, malware infections, or other security threats that compromise confidentiality, integrity, or availability of information.

SYSTEMS refers to a combination of hardware and software electronic devices and components used to access the data described in this agreement. SYSTEMS includes, but is not limited to, computer terminals, networks, and firewalls.

WIN refers to the Western Identification Network, a group of state and local law enforcement agencies that have implemented a shared network and ABIS processing service bureau to provide the ability to search the criminal and civil fingerprint records of these member agencies.

SECTION 1: INTERCONNECTION INFORMATION

Information Types

The types of information to be exchanged are as follows:

- Fingerprint
- Demographic information
- Criminal Arrest Information

Information Impact Level

KCRA classifies data into designations based on sensitivity pursuant to King County's Information Classification Policy, shown in the table below.

Category 1	**Public Information**	**Public information is information that can be or currently is released to the public. It does not need protection from unauthorized disclosure, but may need integrity and availability protection controls.**
Category 2	Sensitive Information	Sensitive information may not be specifically protected from disclosure by law and is for official use only (FOUO). Sensitive information is generally not released to the public unless specifically requested. Sensitive or higher classification information may have been designated by third parties (e.g., federal government) using schemes like the Traffic Light Protocol (TLP) or other designation schemes.

Category 3	Confidential Information	Confidential information is information that is specifically protected from either release or disclosure by law. This includes, but is not limited to personal information as defined in RCW 42.56.230 and RCW 19.255.10, information about public employees as defined in RCW 42.56.250, information about infrastructure and the security of computer and telecommunication networks as defined in RCW 42.56.420(4).
Category 4	Confidential Information Requiring Special Handling	Confidential information requiring special handling is information that is specifically protected from disclosure by law and for which especially strict handling requirements are dictated, such as by statutes, regulations, or contractual agreements. Serious consequences could arise from unauthorized disclosure such as threats to health and safety, or legal sanctions.

Data exchange between KCRA and the AGENCY is classified below:

CJI data is classified as:

- Category 4 - Confidential Information Requiring Special Handling

Category 4 is the most sensitive classification and includes regulated data. As such, the data shall be handled in accordance with the FBI Criminal Justice Information Services (CJIS) Security Policy and applicable policies and procedures set by the AGENCY for handling CJI.

Identifiable non-CJI data is classified as:

- Category 3 - Confidential Information

Aggregate, non-identifiable data is classified as:

- Category 1 - Public Information

<u>Information exchange</u>

KCRA must provision the LIVESCAN DEVICES so that the AGENCY can submit fingerprints and palms (if applicable) to KCRA.

Credential access can be pass-through authentication using existing AGENCY identities, OR a separate identity account provided by KCRA.

KCRA shall use approved network encryption modules required for securely transmitting data from and to the LIVESCAN DEVICES, in accordance with CJIS policies.

SECTION 2: SYSTEMS MANAGEMENT

AGENCY shall ensure AGENCY SYSTEMS are maintained with the best practices including but not limited to:

I. Develop, or acquire, compatible and capable systems required for the interconnection. System requirements are documented in LIVESCAN REQUIREMENTS.
II. Management and security of user accounts and access to the LIVESCAN DEVICES.
III. Deployment and management of agency SYSTEMS, including but not limited to network firewalls, switches, and routers; where appropriate.
IV. Maintain and implement security controls to ensure that location of LIVESCAN remains physically secured as defined by CJIS security Policy.
V. Establish security measures to prevent unauthorized devices from connecting to the LIVESCAN device and/or the AGENCY SYSTEMS utilized by the LIVESCAN.

SECTION 3: SECURITY

Structure

The AGENCY must establish an information security structure that provides for a security point of contact. This contact information shall be provided to KCRA.

Physical Security

A physically secure location is a facility, a criminal justice conveyance, or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. The physically secure location is subject to criminal justice agency management control.

The perimeter of a physically secure location shall be prominently posted and separated from non-secure locations by physical controls.

All personnel with access to areas where unencrypted CJIS information is housed shall either be escorted by authorized personnel at all times or receive a fingerprint-based background check and view security awareness training prior to being granted access to the area.

The AGENCY is responsible for ensuring appropriate measures are in place to physically secure the LIVESCAN DEVICES and AGENCY SYSTEMS that can access the data described in this agreement. Measures shall be in accordance with the CJIS Security Policy.

KCRA shall provide a locked cabinet for LIVESCANS located in jail facilities. AGENCY will have the option to use a KCRA approved locked cabinet for the LIVESCAN if deemed necessary for physical security by both KCRA and AGENCY. This will be at the cost of the AGENCY.

KCRA shall provide privacy filters for the LIVESCAN monitor if deemed necessary for physical security by both KCRA and AGENCY. AGENCY will have the option to use a KCRA approved privacy filter at the cost of the AGENCY.

Personnel Security

The AGENCY is responsible for ensuring appropriate measures are taken to ensure that only authorized personnel can access the data described in this agreement. This includes background investigations and screenings in accordance with the CJIS Security Policy.

KCRA reserves the right to monitor, audit, or investigate the use of Confidential Information collected, used, or acquired by the data described in this agreement.

Data Security

The AGENCY will ensure appropriate and reasonable quality assurance procedures must be in place to ensure that only complete, accurate, and valid information is maintained in LIVESCAN records.

Auditing

The AGENCY shall be responsible for complying with the appropriate audit requirements in accordance with the CJIS Security Policy applicable to the AGENCY'S SYSTEMS and AGENCY'S USERS.

Training

The AGENCY shall be responsible for personnel security training requirements, including compliance with CJIS Security Policy training mandates and AGENCY applicable policies.

Incident Reporting

The AGENCY shall notify KCRA upon discovery of a security incident that may have an operational or security impact on data shared under this agreement. This notification must be completed within 24 hours of discovery.

The AGENCY shall refer to the LIVESCAN CONTACTS AND REFERENCES for contact information for security notifications.

The AGENCY shall also follow reporting procedures in compliance with the AGENCY and governing policies.

Users

Users must maintain strict compliance with applicable policies and procedures as identified in this agreement and the USER POLICY.

SECTION 4: ACKNOWLEDGMENT AND CERTIFICATION

As an AGENCY official serving in the CJIS system, I hereby acknowledge the duties and responsibilities as set out in this agreement. I acknowledge that these duties and responsibilities have been developed and approved by CJIS system users in order to ensure the reliability, confidentiality, completeness, and accuracy of all information contained in or obtained by means of the CJIS system. I further acknowledge that a failure to comply with these duties and responsibilities may subject our agency to terminate the LIVESCAN SERVICES provided by KCRA.

As an AGENCY official serving in the CJIS system, I hereby certify that I am familiar with the contents of the *Title 28, Code of Federal Regulations, Part 20; CJIS Security Policy; Computer Incident Response Capability;* and applicable federal or state laws and regulations for the dissemination of criminal history records for criminal and noncriminal justice purposes.

KING COUNTY REGIONAL AFIS	**AGENCY NAME**
Signature	Signature
Printed Name of Person Signing	Printed Name of Person Signing
Title of Person Signing	Title of Person Signing
Date Signed	Date Signed

EXHIBIT A: LIVESCAN REQUIREMENTS

Network

- An isolated network segment (e.g., VLAN) must be created for the livescan machine and livescan printer.
- No routing should be enabled to the livescan network.
- No other devices may be connected to the livescan network.
- Allow incoming traffic from our VPN servers to the livescan device, 146.129.241.116, 146.129.241.117 and 146.129.241.118.
- An explicit firewall rule that blocks all incoming traffic into livescan network other than KC's VPN servers.
- Allow outgoing traffic to 146.129.241.116, 146.129.241.117 and 146.129.241.118.

System

- To use agency's identities, agency must have Microsoft's Entra ID (formerly Azure Active Directory).
    - Agency will need to follow instructions provided by KCRA to configure authentication and authorization within Agency's Azure instance.
- Agency will manage user accounts and groups providing access to livescan devices.

Environmental Requirements

- Location for livescan and printer (if applicable) must be in a physically secure location as defined in CJIS Policy.
- Two network ports must be available (if no printer is required, then only one network port).
- Ethernet connections must be at least CAT5E or better.
- Allowing operation between 60 to 85 degrees and ensuring there is proper airflow in the room.
- Clean environment to avoid excessive dust that can damage electronic equipment.
- Small table or stand for printer (if included).
- Power outlet(s) must be within 3 feet from the Uninterrupted Power Supply (UPS)/Cabinet.
- Printer must be on its own dedicated circuit due to the power requirements.
- *Cabinet use only:* Tile or cement floor. If carpeted, must not contain padding to minimize tilting and allow proper wheel rolling.

Room Arrangement

- At least 8 inches of free space behind the livescan for cables and maintenance service.
- *Cabinet use only:* At least 15 inches (24 inches is ideal) of free space to the left and the right of the cabinet to allow operator to perform the fingerprinting functions.

EXHIBIT B: LIVESCAN CONTACT AND REFERENCES

General Help and Troubleshooting with livescan devices

- afisithelp@kingcounty.gov
- (206)263-2777

Program Information and Details

- afissect@kingcounty.gov

Training

- afissect@kingcounty.gov

Security Notifications

- afisitnotify@kingcounty.gov
- Lynda Kamrath (206)263-2663

Personnel Changes/Notifications

- afisithelp@kingcounty.gov
- (206)263-2777

EXHIBIT C: LIVESCAN USER POLICY

Purpose

This policy outlines the standards and guidelines for accessing, managing, and safeguarding criminal justice information applicable to the livescan system to ensure compliance with relevant laws, regulations, and security protocols.

Scope

This policy applies to all authorized users, including employees, contractors, and third-party service providers, who access or manage criminal justice information applicable to livescans.

User Responsibilities

- **Access Control:** Users shall access the system only with their assigned credentials and ensure their credentials remain confidential.
- **Data Protection:** Criminal justice information must be handled securely, ensuring it is stored, transmitted, and disposed of in accordance with established procedures.
- **Purpose Limitation:** Information must be used strictly for authorized purposes and not shared with unauthorized individuals.
- **System Integrity:** Users shall not attempt unauthorized access, modify system configurations, or introduce malicious software.
- **System Usage:** Users shall capture fingerprints for qualifying transactions that meet submission criteria.

System Training

All users must complete livescan training to understand their responsibilities and how to properly use the system.

Reporting Requirements

Users must promptly report any security incidents, data breaches, or suspicious activity to the designated security officer, following applicable policies and procedures.

Compliance

Failure to adhere to this policy may result in revocation of system access, and possible legal consequences.

Amendments

This policy is subject to review and amendment as necessary to remain in compliance with changing laws and regulations.