

THIS AGREEMENT is entered between the City of Tacoma and Pierce County, through Interlocal Agreement acting as the LAW ENFORCEMENT SUPPORT AGENCY (hereinafter "LESA") and "USER" to delineate the terms and conditions upon which "USER" will be allowed access to the information, data bases and/or computer systems controlled, operated or accessed by LESA.

A. The following definitions shall apply:

Agency: Means the Pierce County Sheriff's Department (PCSD), Tacoma Police Department (TPD), and the Law Enforcement Support Agency (LESA).

User: Means a criminal justice agency as defined in RCW 10.97, and who is a signatory to this Agreement.

Information: Means any data maintained by LESA (Law Enforcement Support Agency) in manual or automated files, and data obtained through LESA from other agency files or systems such as ACCESS (Washington Central Computerized Enforcement Service System).

Office of Record: LESA is the office of record for the incident data (CAD system - Computer Aided Dispatch, the historical CLEAR system - Consolidated Law Enforcement Automated Records), NetRMS, and Criminal History. Pierce County Corrections is the office of record for JMS (Jail Management System). The Washington State Patrol controls the ACCESS/WACIC (Washington Crime Information Center)/NCIC (National Crime Information Center) systems. Pierce County Juvenile Courts is the office of record for JUDI (Juvenile Detention Information).

Records Custodian: LESA is the records custodian for the Local Warrants data, applications residing on the LESA servers, and data residing in the data warehouse.

- B. It is understood and agreed that LESA has sole authority to determine which of its information, data bases and/or computer systems will be subject to access by USER.
- C. It is understood and agreed that the information maintained or obtained by LESA is solely for its Agency purposes and that USER shall have no right to require or request modifications to the method of retrieval of information. LESA will forward all suggestions for changes and revisions to the LESA Director or designee for review.
- D. It is understood and agreed that LESA reserves the right to impose reasonable charges to USER for the use of and/or connection to the Agency's system as now constituted or as it may be modified, and USER agrees to pay such reasonable charges.
- E. It is understood and agreed that USER shall at all times act in strict accordance with the provisions of the Criminal Records Privacy Act, RCW 10.97 and Public Disclosure Law, RCW 42.17, and further, to ensure security and privacy, USER agrees that:
1. All users shall treat information as confidential;
 2. Dissemination of information shall be pursuant to established Agency Policy and Procedures;
 3. Requesters for Agency Criminal History Information or copies of agency documents shall be directed to LESA Records for processing and dissemination, unless authorized by established Agency Policy and Procedures;

4. Secondary dissemination of information provided to USER by LESA shall not be made other than as required by law. If dissemination is contemplated, LESA is to be notified consistent with the law.
 5. Reproduction of information contained in computerized and manual files shall not be made except as required by law.
 6. Disposal of printed information shall be by destruction;
 7. USER shall insure that physical security measures are present to prevent loss, modification, and authorized access to information;
 8. It is further understood and agreed that USER shall abide by LESA Information Services Policy, which is attached hereto as "Attachment A" and made a part of hereof by this reference [Where this may apply].
 9. It is further understood and agreed that USER acknowledges all specific agreement clauses which are attached hereto as "Attachment B" and made a part of by this reference [Where this may apply].
 10. USER further agrees that it has executed and is bound by and shall abide by the ACCESS/WACIC/NCIC User Acknowledgment which is attached hereto as "Attachment C" and made a part of hereof by this reference [Where this may apply].
 11. It is further understood and agreed that USER acknowledges all clauses in the Dispatch Services Agreement which are attached hereto as "Attachment D" and made a part of by this reference [Where this may apply].
 12. It is further understood and agreed that USER acknowledges all clauses in the Records Management Services Agreement which are attached hereto as "Attachment E" and made a part of by this reference [Where this may apply].
- F. It is further understood and agreed that USER shall limit access to criminal justice employees who are authorized to access such information, and further, ensure that the use of such information is limited to the purposes of criminal justice, as set forth in RCW 10.97. Further, USER agrees that the placement of the computer shall be in secure location, with access limited to the aforementioned criminal justice employees whom shall have individually identified user accounts.
- G. It is further agreed between the parties that LESA is authorized to audit the use of the system by USER, and further, is authorized to immediately disconnect USER in the event of any perceived violation of the conditions of this Agreement herein.
- H. The USER agrees to defend, indemnify and hold harmless the Agency, including PCSD, TPD and LESA and its officers, agents and employees from and against any and all loss, damage, injury, liability suits and proceeding however caused, arising directly from, or indirectly out of, any action or conduct of the USER in the exercise or enjoyment of this Agreement.
- I. Either party may request changes in this Agreement. Any and all modifications shall be mutually agreed upon and incorporated by written amendment to this Agreement and executed by the parties hereto.
- J. This agreement will be effective on the effective date listed below and will remain in effect until canceled. Either the USER or LESA may terminate this Agreement at any time, with or without cause, by notice in writing to the other. This notice is to be given a minimum of four (4) weeks prior

Law Enforcement Support Agency

to the termination date, except as provided in paragraph G of this Agreement. Written notices shall be provided, in the case of LESA, to:

Director
Law Enforcement Support Agency
930 Tacoma Av S., Room 239
Tacoma, Washington 98402

K. This agreement represents the entire agreement between those parties and supersedes any prior oral agreements, discussions, or understandings between the parties.

DATED this 27 day of February, 2002.

EFFECTIVE the 12 day of February, 2002.

Law Enforcement Support Agency

By: John Pirak

Print Name: JOHN PIRAK, DIR.

USER:

CITY OF FIRCREST

Provide written notices to:

City Manager

City of Fircrest

115 Remondell
Fircrest, WA 98466

By: Susan Clough

Print Name: SUSAN CLOUGH

Approved as to Form:

Michael B. Smith

Assistant City Attorney

Attachment A
Information Services Policy

Purpose: The purpose of this policy is to delineate the responsibilities of LESA and user agencies in regard to Information Technology activities such as Internet access, security, acquisition and maintenance of applications, work stations, and printers, and to establish a protocol for connecting to the LESA network and computer systems.

1. Acquisition and Maintenance:

- A. Work stations, and printers presently in use by user agencies that have been supplied by LESA may continue in use. When such units need to be replaced, it is the responsibility of the user agency to provide the replacement. The unit supplied by LESA shall be returned to LESA for disposal and removal from inventory.
- B. Additional work stations, printers, and connectivity devices shall be the responsibility of the user agency. Any wiring, modems, phone lines, etc. required to connect the devices to the computer is the responsibility of the user agency, unless, specifically covered by this Agreement in "Attachment B". Any such items that relate to the LESA system shall be approved by LESA to insure that it is compatible with the system, will not degrade other users and that LESA's systems have the capacity to accept the device.
- C. Maintenance of both existing and additional user related equipment is the responsibility of the user unless specifically covered by Agreement in "Attachment B". User related equipment is defined as all items from the port on the computer to the particular device.
- D. Any user-supplied software that has the capability of impacting the LESA Systems shall be approved by LESA prior to installation.
- E. LESA will provide technical assistance through LESA Information Technology Staff, per the hourly cost set by the LESA Executive Board
- F. LESA is responsible for maintaining the LESA system, including the connectivity devices, work stations, monitors, and printers used solely in LESA. LESA is also responsible for CAD work stations and monitors that are owned by LESA.

2. Internet Access:

- A. Internet access will be for business purposes only. Entertainment or convenience use is not acceptable.
- B. Access to the Internet from any PC connected to the LESA's wide area network is only allowed via the LESA's centralized Internet connection. Alternate methods of Internet access, such as using a modem to access America On-Line, compromise the LESA's network security exposing it to potential harm from computer hackers. Alternate methods further violate access rights to other systems connected to LESA's wide area network. Requests for exceptions to this rule must be reviewed and approved by the LESA Information Technology Assistant Director.

3. Internet and Intranet Use:

- A. All USER employees are responsible for using computer resources in an ethical, responsible and legal manner.
- B. Use of the Internet, including e-mail to and from the Internet, through USER or LESA equipment will only be for USER employees, and/or only for USER business related purposes.
- C. USER Management is responsible for managing use of the Internet by their staff, restricting use or limiting time as they see appropriate.
- D. USER employees should consider their Internet activity as public information and manage their activity accordingly. All Internet traffic goes out beyond the protected LESA network into a wide reaching network that is not secured.
- E. LESA Information Technology monitors and reports on the Internet activity on the LESA's network.
- F. The viewing and downloading of offensive material from the Internet or any non-official (non-LESA) use is not allowed.
- G. All copyrighted information and software found on the Internet must be respected.
- H. Virus checks must be completed on all files and e-mail attachments downloaded from the Internet.
- I. When using the Internet through USER or the LESA resources, USER employees are representing the USER and the LESA, thus all communications across the Internet shall be professional and appropriate.
- J. Software packages, including screen savers, should not be configured to automatically retrieve updated information from the Internet during normal LESA business hours (7:30am to 5:00pm). Request for exceptions to this can be directed to the Information Technology Assistant Director for analysis of impact on LESA resources.

4. Electronic Mail:

- A. The LESA Electronic Mail system is to be used only for the LESA and USER business. As such, the LESA officials may inspect messages at any time.
- B. While in the office, all employees have the responsibility to check their mailbox once per day and to delete all old E-Mail envelopes in a timely manner.
- C. Do not send junk mail or other non-business mail. The E-mail system will not be used as a method of communicating non-essential, non-official or non-LESA information to other system users.
- D. System-wide messages will only be used by the E-Mail administrator.
- E. A username unique throughout LESA will be assigned to each LESA E-Mail user. This allows the LESA E-Mail system to work properly when sharing messages with other organizations and the Internet.
- F. Each message you receive and each message you send is stored on your server until you delete the envelope. Over time the accumulation of all these messages for all the users takes up quite a bit of disk space.
- G. All E-Mail messages can be requested from the system under legal actions and by the LESA system Administrators or as authorized by LESA Administration.

H. Generic names for E-Mail users will not be allowed except as authorized by the Information Technology Assistant Director.

5. General Use:

- A. USER will establish a central point of contact for the LESA so that USER can be notified of impending changes, system non-availability and other technical issues.
- B. USER is responsible for ensuring USER employees understand how to get assistance from the LESA should problems occur.
- C. The LESA will provide support in accordance with terms outlined above or as modified in Appendix B.

Attachment B
Specific Agreement Clauses

1. It is further understood and agreed that USER acknowledges all clauses in the Dispatch Services Agreement which are attached hereto as "Attachment D" and/or the Records Management Services Agreement which are attached hereto as "Attachment E" and made a part of by this reference. [Where this may apply].
2. It is further understood and agreed that USER desires LESA maintenance, repair and installation services of USER owned terminals, work stations, printers and communication devices connected to the LESA systems.
 - a. The LESA and its agents and representatives shall at all reasonable times be given access to the units connected to the LESA systems for the purpose of inspecting, altering, repairing, improving or removing the same.
 - b. The described work will be done on site, unless it can be more expediently done in the shop or at a vendor depot.
 - c. USER shall reimburse the LESA for these services at the current rate set forth in the LESA fee schedule as well as all materials, parts and vendor charges provided at the LESA cost. Payment shall be due within thirty (30) days of presentation of invoice, listing time, parts, materials and vendor charges.
 - d. The LESA fee schedule is available upon request and if changed by the LESA Executive Board action will be distributed to USER.
3. [Specific items that are particular to an agreement]



**ACCESS/WACIC/NCIC
USER ACKNOWLEDGMENT**

I. Introduction

Since its inception, the National Crime Information Center (NCIC) has operated under a shared management concept between the FBI and state users. The NCIC Advisory Policy Board established a goal of having a single state agency in each state assume responsibility as the NCIC Control Terminal Agency (CTA) for the state, through and by which NCIC users in that state would access NCIC. The CTA is responsible for the planning of necessary hardware, software, funding, and training all authorized agencies within the state for complete access to NCIC data services.

The Board approved the CTA concept in order to unify responsibility for system user discipline, and adherence to system procedures and policies within each state. The CTA also serves as a central point in its state for handling record validations, quality control matters, dissemination of manuals and other publications, security matters, user training, audits, and any other problems concerning system use that may arise.

The responsibilities of the Control Terminal Officer (CTO) are detailed in several documents related to the ACCESS/WACIC/NCIC system. This agreement outlines the varied responsibilities of a CTO as they pertain to the NCIC system.

FBI NCIC responsibilities under this shared management concept includes provision of:

- Operational, technical, and investigative assistance to NCIC users;
- Telecommunications lines to a state interface;
- Legal and Legislative review of matters pertaining to NCIC;

ACCESS/WACIC/NCIC USER ACKNOWLEDGEMENT

- Timely information on all NCIC aspects of system usage by means of the NCIC Operating Manual, Technical and Operational Updates, and related documents;
- Staff research assistance;
- Training and training materials to the control terminal agencies.

The following documents are incorporated by reference and made part of this user acknowledgment: WACIC Manual; ACCESS Manual; NCIC Computerized Criminal History (CCH) Program Background, Concept and Policy, as amended or superseded by implementation of the Interstate Identification Index (III) Program; code of Federal Regulations, Title 28, Part 20; NCIC Standards as recommended by the NCIC Advisory Policy board and approved by the FBI Director; applicable federal and state laws and regulations; ACCESS/WACIC rules, regulation, and policies as recommend by the Advisory Council on Criminal Justice Services.

II. DEFINITIONS

"Control Terminal Agency (CTA)"

In Washington, the CTA is the Washington State Patrol

"NCIC Control Terminal Officer (CTO)"

The NCIC CTO is the Commander of the Washington State Patrol's Criminal Records Division.

The CTO and his agency will be responsible for monitoring system use, enforcing system discipline, and assuring ACCESS, WACIC, and NCIC operating procedures are followed by all users of the respective telecommunications lines, as well as other related duties as outlined by this document.

"Terminal Agency Coordinator (TAC)"

A TAC shall be appointed at each terminal location and be Level II certified. The TAC shall be responsible for ensuring his/her agency is in compliance with state and NCIC policies and regulations, including validation requirements.

ACCESS/WACIC/NCIC USER ACKNOWLEDGEMENT

"Timeliness"

WACIC/NCIC records must be entered promptly to ensure maximum system effectiveness.

A timely entry in the Wanted Person File is made immediately once:

1. The decision to arrest or authorize arrest has been made; and
2. The terms of extradition have been established.

The date of want or warrant must be the date on which all those decisions were made.

A timely removal from the file means an immediate clearing of the record once the originating agency has documentation the fugitive has been arrested or is no longer wanted.

Timely system inquiry means initiation of the transaction before an officer releases a subject or begins writing an arrest or citation document of any kind; inquiry prior to the release of a person who has been incarcerated; or inquiry upon those who appear at a custodial facility to visit inmates.

Timeliness of entry/modification in the Missing Person File is generally the same as in the Wanted Person File.

Timely entry/modification of vehicle, license plate, and vehicle part data matches the wanted person standard, less the extradition considerations. Entry should be made as soon as a cross-check of the Department of Licensing's Registration File has been completed.

Timely entry of gun, article, and securities information means within a few hours of the time complete information is available.

"Validation"

Validation (vehicles, plates, fugitives, missing person entries) obliges the ORI to confirm the record is complete, accurate, and still outstanding or active. Validation procedures are defined in Section IV-C of this agreement.

ACCESS/WACIC/NCIC USER ACKNOWLEDGEMENT

"Completeness"

Complete records of any kind include all information available on the person or property at the time of entry. The validation process should include a review of whether additional information has become available (missing from original entry) that could be added.

Complete inquiries on persons include numbers that could be indexed in the record (i.e., Social Security, passport, VIN, license plates, driver's license, etc.). Inquiries should be made on all names/aliases used by the suspect. Complete vehicle inquiries include VIN and license plate numbers.

"Accuracy"

The accuracy of WACIC/NCIC data must be double-checked by a second party. The verification should include assuring the data in the WACIC/NCIC record matches the data in the investigative report and that other checks (VIN/licence numbers) were made. Agencies lacking support staff for this cross-checking should require the case officer to check the record, as he/she carries primary responsibility for seeking the fugitive or the stolen property.

III. OPERATIONAL RESPONSIBILITIES

To ensure the proper operation of WACIC/NCIC, the standards, procedures, formats, and criteria, as contained in ACCESS/WACIC operating manuals, will be followed. A specific operational situation is:

Hit Confirmation Policy

The agency that obtains a hit has the ability to designate to the entering agency one of two priorities for confirmation.

PRIORITY 1: URGENT

Confirm the hit within 10 minutes. In those instances where the hit is the only basis for detaining a suspect or the nature of a case requires urgent confirmation of a hit, the highest level of priority should be specified.

Each agency must, within 10 minutes, furnish to an agency requesting a record confirmation, a response indicating a positive or negative confirmation or a

ACCESS/WACIC/NCIC USER ACKNOWLEDGEMENT

notice of a specific amount of time necessary to provide a response to the request for record confirmation.

PRIORITY 2: ROUTINE

Confirm the hit within one hour. Generally, this priority will be used when the person is being held on local charges, property has been located under circumstances where immediate action is not necessary, or an urgent confirmation is not required.

Each agency must within one hour, furnish to an agency requesting a record confirmation, a response indicating a positive or negative confirmation or a notice of a specific amount of time necessary to provide a response to the request for record confirmation.

An agency requesting confirmation which fails to receive a response to the first request shall generate a second request with a copy to the CTO. The CTO will institute appropriate action to ensure proper response to a hit confirmation request and to comply to system standards. This appropriate action may include canceling the record by the CTA.

IV. QUALITY ASSURANCE RESPONSIBILITIES

A. Introduction

Criminal justice agencies have a specific duty to maintain records that are accurate, complete, and up-to-date. The CTA will ensure there are standards for security, audits, and personnel training; which would allow the dissemination of accurate and up-to-date records.

B. Record Quality

Errors discovered in WACIC/NCIC records are classified as serious errors, form errors, or an error trend.

- (1) Serious errors: WACIC/NCIC will advise the ORI via teletype message of an apparently erroneous record and request it be verified, changed, or canceled within 24 hours. The record will be canceled if neither a response is received nor corrective action has been taken during the allotted time.

ACCESS/WACIC/NCIC USER ACKNOWLEDGEMENT

- (2) Form errors or error trends: the CTA will notify the ORI by letter of the corrective action to be taken. No further notification or action will be taken by the CTA.

C. Record Validation

WACIC/NCIC periodically prepares listings of records on file for validation purposes. Validation listings are prepared pursuant to a schedule, as published in the WACIC Operating Manual. These listings are mailed to the originating agency.

Validation obliges the ORI to confirm the record is complete, accurate, and still outstanding or active. Validation is accomplished by reviewing the original entry and current supporting documents, and by recent consultation with any appropriate complainant, victim, prosecutor, court, motor vehicle registry files, or other appropriate source or individual. In the event the ORI is unsuccessful in its attempts to contact the victim, complainant, etc., the entering authority must make a determination based on the best information and knowledge available whether or not to retain the original entry in the file. Validation procedures must be formalized and copies of these procedures must be on file for review during an NCIC/ACCESS audit.

Each agency will receive a letter explaining what records are contained in the validation and general procedures for validating the records. A "REPLY REQUIRED" letter is included for the agency to certify the records have been validated.

Validation certification means: (1) the records contained on the validation listing have been reviewed by the originating agencies; (2) the records which are no longer current have been removed from WACIC/NCIC and all records remaining in the system are valid and active; (3) all records contain all available information; and (4) the information contained in each of the records is current and accurate, including appropriate extradition information.

If the CTA has not received a certification response from an agency within the specified period of time, the CTA will purge from WACIC/NCIC all records which are the subject of that agency's validation listings. (NOTE: If a CTA fails to certify any validation listing to the NCIC within the

ACCESS/WACIC/NCIC USER ACKNOWLEDGEMENT

specified time, all invalidated records from that state will be purged by the NCIC.)

V. SECURITY RESPONSIBILITIES

A. **General**

Security guidelines, relating to WASIS and NCIC III criminal history record information, are set forth in the NCIC Computerized Criminal History Program Background's Concept and Policy as superseded by the III program, in Title 28; Code of Federal Regulation; Part 20, Subparts A and C; and by state statute in RCW 10.97 and Washington's Administrative Code, chapter 446-20.

All agencies participating in the ACCESS system must comply with and enforce system security.

B. **Originating Agency Identifier (ORI)**

The assignment of an ORI to an agency is not a guarantee of access to the systems. The ultimate decision regarding who may access WACIC/NCIC lies with the CTA.

The CTO will coordinate the assignment of new ORI numbers, the change in ORI location or address, any other changes, cancellations, or retirements of ORIs accessing WACIC/NCIC. The agency shall notify the CTO of any such changes.

Application for assignment of new ORIs shall be made directly to the CTO. Such application shall contain documentation of the agency's statutory authority as a criminal justice agency and a statement that indicates the agency allocates more than 50 percent of its annual budget to the administration of criminal justice. Noncriminal justice agencies will be denied an ORI, unless under management control of a criminal justice agency, a copy of the management control agreement must be submitted to the CTO.

ACCESS/WACIC/NCIC USER ACKNOWLEDGEMENT

VI. COMPUTERIZED CRIMINAL HISTORY RECORD INFORMATION RESPONSIBILITIES

- A. Each agency shall conform with system policies, as established by the ACCESS/WACIC manuals, before access to criminal history record information is permitted. This will allow for control over the data and give assurance of system security.
- B. The CTA is responsible for the security throughout the system it services, including all places where terminal devices are located. Upon determination that a terminal is in non-conformance with system management or security policy, the CTA has the authority to impose sanctions, including termination of service.
- C. The rules and procedures governing direct terminal access to criminal history record information shall apply equally to all participants in the system.
- D. All criminal justice agencies having direct access to computerized CHRI data from the system shall permit an NCIC or WACIC audit team to conduct appropriate inquiries with regard to any allegations of security violations. Agencies must cooperate with these audits and respond promptly.
- E. All computers and manual terminals interfaced directly with the ACCESS/WACIC/NCIC systems for the exchange of criminal history record information must be under the management control of a criminal justice agency, as defined by the NCIC CCH background and policy document.
- F. Each agency shall have in place a system for logging all inquiries of the III, which log shall include the name of the individual within the criminal justice agency to whom the response is given. These logs shall be maintained for at least 12 months from the date of inquiry and must be available to assist in the State or National audit program.
- G. Each agency receiving an III response shall record any secondary dissemination. These logs shall be maintained for at least 12 months from the date of inquiry.

ACCESS/WACIC/NCIC USER ACKNOWLEDGEMENT

Agencies must institute a program of systematic self-audits as a means of guaranteeing the completeness and accuracy of the information in the system. These self-audits should be on a continual basis to ensure both quality assurance and compliance with standards.

Compliance audits will cover the following areas of the III, WACIC/NCIC stolen property, and person records:

Accuracy

All WACIC/NCIC entries shall contain no erroneous data.

Completeness

All information contained in a WACIC/NCIC entry or in a criminal history record shall contain the most pertinent information available.

Timeliness

All entries, modifications, updates, and removals of information shall be completed, processed, and transmitted as soon as possible, in accordance with established standards.

Locates

All wanted/missing persons, and property records, which are apprehended or recovered, shall be promptly placed in "located" status, except those located outside of the stated area of extradition or return.

Security

It is the responsibility of an agency to protect its information against unauthorized access, ensuring confidentiality of the information in accordance with laws, policies, regulations, and established standards.

Dissemination

All information released shall be in accordance with applicable laws and regulations, and a record of dissemination of criminal history records shall be maintained for one year and made available for NCIC/WACIC audit review.

ACCESS/WACIC/NCIC USER ACKNOWLEDGEMENT

VII. ADMINISTRATIVE RESPONSIBILITIES

- A. The agency shall respond to requests for information by the FBI NCIC or WACIC in the form of questionnaires, surveys, or similar methods, to the maximum extent possible, consistent with any fiscal, time, or personnel constraints of that agency.
- B. The CTO shall offer system training to agencies accessing WACIC/NCIC through the state computer. Agencies shall assign appropriate employees to attend classes When offered. If employees are using inquiry only functions, they must attend Level I certification training. Employees entering information into the NCIC/WACIC system and Terminal Agency Coordinators (TAC) must attend Level II certification training. All certifications must be renewed biennially.
- C. The CTO will distribute, within the state criminal justice community, the ACCESS/WACIC manuals, NCIC Code Manuals, and as requested, miscellaneous publications in order to enhance effective use of the WACIC/NCIC system. The agency shall incorporate such changes upon receipt.

ACCESS/WACIC/NCIC USER ACKNOWLEDGEMENT

ACKNOWLEDGMENT

As an agency head/director serving in the ACCESS/WACIC/NCIC system, I hereby acknowledge the duties and responsibilities as set out in this document, as well as those documents incorporated by reference. I acknowledge that these duties and responsibilities have been developed to ensure the reliability, confidentiality, completeness, and accuracy of all records contained in or obtained by means of the WACIC/NCIC system. I also acknowledge that a failure to comply with these duties and responsibilities will subject my agency to various sanctions. These sanctions may include the termination of ACCESS/WACIC/NCIC services to my agency.

John Cheesman 3/1/07
Agency Head (Please Print) Date

John Cheesman
Agency Head signature

Fircrest Police Dept.
Agency Name

Attachment D
Dispatch Services Agreement

Purpose: The purpose of this attachment is to delineate the responsibilities of LESA and USER in regard to police dispatch services and fees associated therewith.

1. Charges shall be based on cost allocations determined by the LESA Executive board.
2. In consideration of the services charges here after defined, LESA will receive and dispatch calls for police service. LESA will monitor the status of the assigned police units.
3. Each party is responsible for maintaining its own radio and communication equipment. Any phone line or device charges for LESA to receive calls shall be the responsibility of USER.

Attachment E
Records Management Services Agreement

Purpose: The purpose of this attachment is to delineate the responsibilities of LESA and USER in regard to RMS records management services and fees associated therewith.

1. Charges shall be based on cost allocations determined by the LESA Executive board.
2. In consideration of the service charges here after defined, LESA will provide records management support for RMS data entry and approvals using UCR/WIBR/NIBR standards in the form of training, problem solving, auditing and statistical gathering.
3. Each party is responsible for maintaining its own equipment. Any phone line or device charges for LESA to share data shall be the responsibility of USER.

LAW ENFORCEMENT SUPPORT AGENCY

FEE SCHEDULE	COST
1. Individual requests for inspection of local conviction criminal history records information, including fingerprinting for positive identification.	\$25.00
2. Individual requests for inspection of local conviction criminal history records information, by name and date of birth only.	\$15.00
3. Issuing or renewing a Concealed Pistol License.	Fee established By RCW9.41.070
4. Clearance letter for Immigration, Passport or VISA.	\$20.00
5. Traffic Accident report.	\$ 0.15
a. Cost per printed page	
b. Cost of postage if applicable	
6. Records search, furnish case control number and letter of loss.	\$ 5.00
7. Attachment of any insurance communication to a case record. (requires a \$5.00 check with each subrogation letter)	\$ 5.00
8. Public Disclosure and Subpoena requests.	\$ 0.15
a. Cost per printed page	
b. Cost of postage if applicable	
9. Taking fingerprints for other than County or City licensing purposes.	
a. First fingerprint card	\$ 5.00
b. Second and each additional card	\$ 3.00
10. Civil court appearance by LESA personnel, to include those court appearances as directed by Subpoena Ducus Tecum, per hour or fraction thereof.	\$75.00
11. Furnish magnetic tape cassette with recorded copy of original tape recording made in the Communications Center of telephone or radio conversations pertaining to a particular event or events as properly authorized. Fee shall be charged for the time actually spent in copying information from the original records at a cost of \$17.50 for each fifteen minutes or fraction thereof plus \$1.50 for each cassette tape furnished. Cost per hour or fraction thereof.	\$75.00
12. Preservation of 24 hour Master Audio tape: per tape, per each 6-month increment.	\$20.00
13. Communications, records, data processing and electronic equipment maintenance and service costs per hour plus parts and vendor repair charges at cost.	\$75.00
14. Copy of Crime Reports prepared by LESA, which includes Pierce County Sheriff, cities of Tacoma, Lakewood, University Place and Edgewood.	\$ 5.00
15. Laminating of wallet sized documents.	\$ 3.00
16. Postage Fees. \$1.00 for up to three pages (\$.35 for postage, \$.65 for handling) plus \$.15 postage for each additional page.	

Criminal Justice agencies are exempt from these fees except for items #12 and #13