

10 6 2000
10 1 2000 *



RESOLUTION NO. 3 1 3 6

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF AUBURN, WASHINGTON, AUTHORIZING THE CITY TO ENTER INTO AN INTERLOCAL AGREEMENT BETWEEN THE CITY OF AUBURN AND THE CITY OF ALGONA FOR SERVICES TO BE PROVIDED BY THE CITY OF AUBURN INFORMATION SERVICES SECTION AND THE AUBURN POLICE DEPARTMENT FOR USE OF THE SPILLMAN PUBLIC SAFETY SYSTEM.

WHEREAS, RCW 39.34 authorizes public agencies to enter into interlocal agreements; and

WHEREAS, it is beneficial to the public and to the citizens of the City of Auburn to cooperate with other jurisdictions in the sharing of law enforcement information; and

WHEREAS, this agreement will allow access to the City of Auburn Police Department computer programs and stored data contained in the Spillman Public Safety System; and

WHEREAS, that the City of Algona, as a condition of this agreement, will purchase Spillman, Inc. licensing for access to the computer programs and stored data of the City of Auburn's Spillman Public Safety System Server.

THE CITY COUNCIL OF THE CITY OF AUBURN, KING COUNTY, WASHINGTON, IN A REGULAR MEETING DULY ASSEMBLED, HEREWITH RESOLVES THAT:

Section 1. The proper officers of the City of Auburn are herewith authorized to execute an Interlocal Agreement between the City of Auburn, Washington and the City of Algona, Washington. A copy of said Interlocal Agreement is attached hereto as Exhibit "A" and is incorporated herein by this reference as though set forth in full.

Section 2. The Mayor is hereby authorized to implement such administrative procedures as may be necessary to carry out the directives of this legislation.

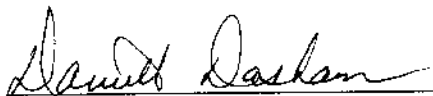
DATED and SIGNED this 20th day of December, 1999.

CITY OF AUBURN



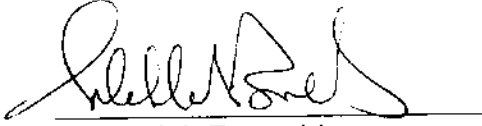
CHARLES A. BOOTH
MAYOR

ATTEST:



DANIELLE DASKAM,
City Clerk

APPROVED AS TO FORM:

A handwritten signature in cursive script, appearing to read "Michael J. Reynolds", written over a horizontal line.

Michael J. Reynolds,
City Attorney

Resolution No. 3136
December 16, 1999
Page 3

**CITY OF AUBURN INTERLOCAL AGREEMENT
Spillman Public Safety System**

This Agreement is executed pursuant to Resolution No. 3136. The parties acknowledge they have read and understand the terms and conditions contained therein. This Agreement sets forth provisions identifying services to be provided by the City of Auburn Information Services Section and the Auburn Police Department, to be performed for the City of Algona, hereinafter called "Customer."

For purposes of this Agreement, the "Provider" will be the City of Auburn.

These services are for the exclusive use by the Customer.

1. SCOPE OF AGREEMENT

This Agreement shall address Customer access to the Provider's Spillman Public Safety System, hereinafter known as the SPSS.

2. GENERAL CONDITIONS

2.1 USE OF SOFTWARE

Use of the SPSS shall be in accordance with the licensing policies of Spillman, Inc. and subject to current and subsequent policies set forth in the City of Auburn Information Services Policies and Procedures 100-32, Virus Protection, and Auburn Police Department Manual of Standards, 27.1.6, Passwords, Access Codes/Violations Audit, attached hereto and incorporated herein by this reference. (See Exhibits "C" and "D")

2.2 DATA AVAILABLE

The Provider shall allow the Customer access to computer programs and stored data for which Spillman, Inc. licensing has been purchased by the Customer. Access to the Customer's data and the data of other agencies will be established and directed by the Provider and in cooperation with each participating agency. Data entered into the system by any agency becomes a part of the SPSS database and will be subject to maintenance or archival procedures as determined by the Provider.

Extent of access shall conform to the regulations set forth in Chapters 10.97, 13.50, and 42.17 RCW and other applicable federal, state, and local law.

The Customer will not sell, give, loan, lease or otherwise transfer title, possession, or allow access or use of any of the data or screens by any person, firm, corporation or association without prior written approval of the Provider. Customer acknowledges that Provider may deny any of the aforementioned acts to be undertaken by Customer.

Dissemination of data or information is the responsibility of the agency recording the data or information in accordance with this Agreement and Public Disclosure Act, Chapter 42.17 RCW, and the Washington State Criminal Records Act, Chapter 10.97 RCW. Other entities will not disclose data except through specific contracts and agreements with application and data owners.

Exhibit "A", Resolution No. 3136
City of Auburn

2.3 PROPRIETARY INFORMATION

Proprietary information disclosed by either party to the other for the purposes of this Agreement, which is clearly so identified in writing as proprietary, shall be protected by the recipient in the same manner and to the same degree that the recipient protects its own proprietary information. Such information will be disclosed only to those employees of the recipient requiring access thereto in order to perform this Agreement. All information or data on the Provider's network shall be treated as proprietary regardless of ownership.

2.4 CUSTOMER NOT TO HAVE OR USE LIST OF INDIVIDUALS FOR COMMERCIAL PURPOSES

The Customer agrees, warrants, promises and swears under penalty of perjury that it shall not use or allow others to use directly or indirectly the data, screens, or access thereto as a list or lists of individuals for commercial purposes.

a) THE PROVIDER MAY PRIORITIZE PROVISION OF ACCESS

The Provider may limit, control or prioritize the access described herein to any extent necessary to prevent such from unreasonably disrupting the Provider's operations and to prevent excessive interference with other essential functions of the Provider and to the extent necessary to provide access to its public records by other members of the public.

This may include scheduled shutdowns for backups or maintenance and unscheduled shutdowns due to hardware or software malfunctions.

b) ASSIGNMENT

The customer agrees that it shall not assign any right or interest in the Agreement without the written permission of the Provider. Any attempted assignment by the Customer without written permission by the Provider, or its authorized agent, shall be wholly void and totally ineffective for all purposes of this agreement. Furthermore, the Customer and the Provider agree that neither shall delegate any obligation which it has under this Agreement without the written permission of the other party.

Any attempted delegation without written permission shall be wholly void and totally ineffective for all purposes.

2.6 LIMITATION OF LIABILITY

The information supplied by the Provider described herein is provided on an "as is" basis "with all faults".

Nothing contained herein shall be construed to require the Provider to maintain the information or data in a more current form than the Provider shall from time to time determine.

The obligations of the Provider and the rights and remedies of the Customer set forth in this clause are exclusive and in substitution for all the warranties, obligations and liabilities of the Provider and rights, claims and remedies of the

Customer against the Provider express or implied, arising by law or otherwise, with respect to any data provided hereunder, including but not limited to any implied warranty arising from course of performance, courses of dealing or uses of trade, and, any obligation, liability, right, claim or remedy for tort, or for any actual or alleged infringement of patents, copyrights or similar rights of third parties, or for any other direct, incidental or consequential damages.

2.6 TERMINATION OF AGREEMENT – EVENTS OF DEFAULT

This agreement may be immediately terminated without notice upon an event of default. Events of default include but are not limited to the following:

- a. The Customer wrongfully uses data provided by the Provider.
- b. Unauthorized copying of data
- c. In the event the Agreement is determined to be in conflict with federal or state law, City resolutions or ordinances which are in effect at the time of this Agreement or may be imposed in the future.
- d. The Customer uses or attempts to use information provided in such a manner as to violate a taxpayer's right to privacy or to create an unfair competitive disadvantage for a taxpayer.
- e. The Customer sells, gives, leases, or loans access to the screens of the data contained therein to any person or in any way, directly or indirectly, allows copies to be made by any person without the express written approval of the Provider.
- f. The Customer allows access to the screens of the data contained therein, or any part thereof, to be used as a list of individuals for commercial purposes.
- g. The Customer allows the connection of a computer network operated by any entity that is outside of the Provider's influence.
- h. The Customer violates any of the conditions set forth in the City's Computer Use Policies and Procedures, included as Exhibit "C".

3. SERVICE AGREEMENT PERIOD

This Agreement commences upon execution by signature of both parties and shall continue until terminated by the Customer, with a 30 day written notice; or by the Provider, with mutual agreement by both parties.

4. SERVICE PROVISIONING

Requests for new service, changes to existing service, or billing and service agreement changes should be submitted, in writing, to:

City of Auburn Information Services
Attention: Diane Supler
25 West Main St.
Auburn, WA 98001
Phone (253) 931- 3003
Fax: (253) 288-3132

5. SERVICE RATES

5.1 BASIC RATE FOR SPSS ACCESS

The basic rate for access to the SPSS is given in Exhibit A.

Basic support for the SPSS consists of SPSS account management, security management, name merges, application troubleshooting and capacity planning. Basic support shall apply to all Public Safety personnel who are employees of the Customer. Public Safety personnel, for the purposes of this Agreement, are considered Law Enforcement Personnel.

See Exhibit B, Hardware and Software Required to access the SPSS for hardware and software requirements. Please note that hardware and software requirements are subject to change. The Provider will review and publish requirements in December of each year.

5.2 RATES TO BE REVIEWED ON A YEARLY BASIS

All rates will be reviewed on a yearly basis. Rate schedules will be available in August of each year.

5.3 CUSTOMER EQUIPMENT COSTS

The Customer shall be totally responsible and liable for all costs incurred in the acquisition of its own equipment, including telephone lines and other supplemental equipment and the costs of connecting that equipment with the Provider's equipment. Where required by the Provider, the Customer will buy equipment specified by the Provider for their computer network access. The Customer will be responsible for trouble shooting and maintaining their equipment and data link.

6. BILLING GUIDELINES

The Provider will bill on a yearly or monthly basis dependent on the type of service being billed. Billing for basic Spillman access will be on a yearly basis in July of each year. Time and materials charges will be billed on a monthly basis for services rendered during the previous month. Payment is due within 30 days of the billing date.

6.1 SERVICE ADDS/CHANGES

Service additions or changes occurring on or before the 15th of the month will be charged for the full month. Additions or changes occurring after the 15th of the month will be invoiced starting the first day of the following month. All service additions or changes must be submitted in writing. All additions and changes will be billed on a time and materials basis.

6.2 SERVICE CANCELLATION

Services canceled on or before the 10th of the month will not be charged for the month. Services canceled after the 10th of the month will be charged the full month. All service cancellations must be submitted in writing.

7 SPSS/NETWORK AVAILABILITY

The SPSS availability objective is 99.8% seven days a week, 24 hours per day.

7.1 SPSS/NETWORK MAINTENANCE

The SPSS and the Provider networks will be available as set forth in Section 7 with the following exceptions:

7.1.1 SCHEDULED MAINTENANCE

The Provider's Information Services department reserves the right to schedule preventative maintenance on all systems. Preventative maintenance will be scheduled a minimum two weeks in advance and attempt to minimize impacts to each user agency. The Customer must notify the Provider's Information Services department one week prior to the scheduled maintenance window, if the Customer requires the SPSS to be available during scheduled maintenance. Scheduled maintenance may result in loss of service to the SPSS for a period of time.

7.1.2 SOFTWARE AND HARDWARE UPGRADES OR MODIFICATIONS

Software and Hardware upgrades or modifications differ from normally scheduled maintenance, in that the SPSS will be unavailable for the duration of the upgrade. It is conceivable that an upgrade may take a couple of days. In the event of an upgrade, the Customer will be informed a month prior to the scheduled upgrade time. The Provider will make every reasonable attempt to schedule the upgrade to minimize impacts to each Customer.

7.1.3 EMERGENCY MAINTENANCE

Emergency maintenance will be coordinated with the Customer whenever possible.

7.2 SPSS AND NETWORK SUPPORT COVERAGE

7.2.1 CITY OF AUBURN HELP DESK COVERAGE

The Provider's Help Desk is staffed approximately 8 hours per day, five days a week. Support hours are from 8:30 a.m. – 4:30 p.m. The telephone number is (253) 931-3004. Please use the options in the telephone message to reach the Help Desk. The Help Desk staff will log computer and network problems and dispatch problems to the appropriate personnel. SPSS users may also contact Cheryl Price at (253) 931-3042 on problems relating specifically to the SPSS application. The Customer is responsible for providing a current contact list to the Provider's Information Services department.

7.2.2 CONFIGURATION MANAGEMENT

All configuration changes to the SPSS will be made by the Provider's Information Services' department in coordination with the Customer. The Customer will provide

the Provider's Information Services department with a primary and alternate contact name of authorized personnel who can coordinate/request changes to the current network.

7.2.3 DISASTER RECOVERY

The Provider's Police Department backs up the SPSS to tape on a nightly basis. These tapes are saved for a period of three months and then rotated. The Provider will not maintain information longer than this time unless the Customer requires data be dumped to tape for archival purposes.

7.2.4 SECURITY AND INTEGRITY

The Provider's network is protected from the Internet with firewall security to prevent unauthorized access from the Internet. The Customer is responsible for securing their organization's computer resources against all unauthorized access.

8. AUTHORIZED USE

The Agreement is intended for use by the Customer's Public Safety employees only. The Provider's Information Services department must approve all accounts.

9. INDIRECT ACCESS

Customer will take measures to prevent unauthorized third party indirect access to the SPSS. Examples of this would be gateways, dial-up, or cascaded Telnet sessions where the originator is not a Customer authorized user of the Provider's network, but whose resultant IP address would appear to the network as being the Customer's address. Should unauthorized use of the Customer's access as described in Section 2.2 paragraph 3 occur, any damages or costs of litigation including attorney's fees incurred by the Provider shall become the financial responsibility of the Customer.

10. USER ACCOUNT ACCESS TO SPSS SYSTEM

Each user of the SPSS shall have a unique user account with a unique password. This account is used within the SPSS to determine system rights of the user and to provide a method of accounting for access to information. Sharing of accounts within an agency for the purposes of reducing access cost is expressly prohibited.

11. CUSTOMER FIELD OFFICE ENVIRONMENT

The Customer is responsible for providing an acceptable environment for all equipment used to access the SPSS. The Customer is responsible for the security, power quality and cleanliness of the equipment environment. Equipment replacement due to damage resulting from, but not limited to, power surges, water damage, improper handling or extremely high temperatures is the responsibility of the Customer.

12. SUPPLEMENT CHANGES

All changes to this Agreement shall be mutually agreed upon in writing in advance. All such changes shall take precedence over this original Agreement.

13. TERMINATION OF AGREEMENT

This Agreement may be terminated upon mutual agreement of all of the parties by providing written notice of such termination. Termination will be effective on the date stated in the notice so long as the notice is properly given at least 30 days prior to such date.

14. ACCEPTANCE

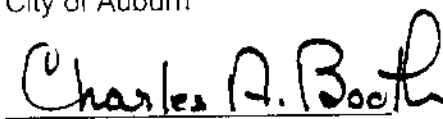
Customer hereby acknowledges and accepts the terms and conditions of this Agreement.

CUSTOMER:
City of AKGONA



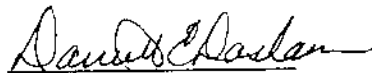
GLENN WILSON
Mayor

PROVIDER:
City of Auburn



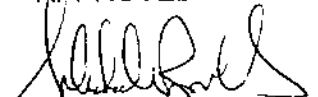
CHARLES A. BOOTH
Mayor

ATTEST:



Danielle E. Daskam,
City Clerk - Auburn

APPROVED AS TO FORM:



Michael J. Reynolds,
City Attorney

EXHIBIT "A"

Yearly Maintenance Contract Cost for 1999-2000 for all modules except PictureLink and StateLink (External Communications):

For Auburn PD only (size "C" agency)	\$16,200
Algona addition, due in July 2000	\$ 3,832

EXHIBIT "B"

Hardware requirements:

Cisco Router – 1 each at Customer and Provider location
Pentium Computers
Connection to the City of Auburn Server through either a T-1, ISDN or fiber-optic cable

Software Requirements:

Appropriate firewall software
Windows 95 OS (minimum)
Emulation Software such as TinyTerm, Reflections, Exceed



ADMINISTRATIVE POLICY AND PROCEDURE

TITLE: VIRUS PROTECTION			SUBJECT: COMPUTER	
			INDEX NO: 100-32	
EFFECTIVE DATE: 12/01/98	SUPERSEDES:	PAGE NO. OF: 1 2	PREPARED BY: Diane Supler	MAYOR'S APPROVAL: <i>Charles A. Booth</i>

1.0 PURPOSE

To establish policy and assign responsibility for virus protection and eradication from City-owned and non-owned computers used by any City of Auburn employee for City business.

2.0 ORGANIZATIONS AFFECTED

All Departments/Divisions

3.0 REFERENCES

4.0 POLICY

- 4.1 Departments shall ensure that all computer users know and understand safe computing practices. At a minimum, this shall include knowledge of the following:
- knowing the source of the software in use
 - performing frequent backups on data files
 - using anti-virus software
 - scanning for viruses on files that are downloaded from BBSs, the Internet, or any other outside source
 - scanning for viruses on all diskettes brought from home or any other outside source
 - booting only from a cleanly scanned diskette when not booting the workstation from the hard drive
- 4.2 The City shall purchase and install anti-virus software for all LAN servers and workstations. This software will be updated on a regular basis by the IS Division. Servers and workstations will be scanned for virus' periodically, either manually by the IS Division or via an automated program.
- 4.3 Departments shall report all virus outbreaks to the Finance Director. The Finance department shall be charged with logging all such outbreaks and the eradication methods used by departments, and will notify other departments, if appropriate, in the existence of a virus, along with effective measures used in its eradication if known.

5.0 DEFINITIONS

- 5.1 BBS is the acronym for "Bulletin Board System," which is a computer system used as an information source and message system. BBS is similar to a physical bulletin board, except that messages are posted electronically on a computer bulletin board system.

6.0 PROCEDURE

In the event of a serious virus outbreak, or in the event of a continued breach of this policy by a department, the Network Administrators will disconnect that department from the Citywide backbone (or any other Citywide network) until compliance with the policy.

27.1.5 Report Status

82.1.5

Case numbers are assigned by dispatch personnel at the time of the incident occurrence. Original copies of reports will be maintained by the Police Services unit in their appropriate case file, which has the corresponding case number. The Specialists will ascertain during records processing that the correct case number for the incident is on the written document submitted. The case numbers are listed in a computerized master file after it has been issued.

- A. An assigned Specialist will do a routine inventory of all outstanding reports to assure they are submitted in a timely fashion.

27.1.6 Passwords, Access Codes/Violations Audit

82.1.6

The Professional Standards Manager audits the central records computer system for verification of all passwords, access codes, or access violations.

27.1.7 Virus Protection

82.1.7

The Auburn Police Department adheres to City of Auburn Policy 100-32, Virus Protection, regarding the introduction of outside computer software and disks into agency-owned computer systems and workstations. The department discourages employees from bringing in programs from home and loading them on department computers. All employees are required to run a "virus scan" on all diskettes brought from home or any other outside source.

- A. The City of Auburn removed some "System Administrator" functions from department computers, to include the "Run" command that allows installation of new software.