

RESOLUTION NO. 14-1

WHEREAS, on June 14, 2006 Sangamon County (the County) and the Sangamon County Emergency Systems Board (the ETSB) entered into an agreement with the New World Systems Corporation (New World) for the procurement of an integrated criminal justice system (ICJS0, and

WHEREAS, the City of Springfield (the City) entered into a separate but similar procurement agreement at a later date, and

WHEREAS, Article VII, Section 10 of the Illinois Constitution of 1970 and the Intergovernmental Cooperation Act (5 ILCS 220/1 *et seq.*) provides that units of local government may contract or otherwise associate among themselves to obtain or share services;

WHEREAS, a critical component of the ICJS is the Intergovernmental Agency Agreement between the City of Springfield, Sangamon County and ETSB which covers the operating standards and obligations for services provided by New World, and

WHEREAS, the IGA between the County, the City and the ETSB has expired, and

WHEREAS, the County, the City and the ETSB have executed a contract with New World on a new joint SMSA that will include all three entities, with terms and conditions that are acceptable to those involved in the negotiations, and

WHEREAS, it is in the public's interest for the County, the City and ETSB to be provided the ESS ICJ/PSI Integrated Solution and associated information for its use, subject to certain limitations provided herein, for the Participants to contribute to the cost of procuring, developing, and maintaining this information through a joint initiative, for use of such information by anyone other than the Participant to be subject to certain limitations;

WHEREAS, a copy of the new five year IGA (retroactive to the date of the New World SMSA) is attached, and

RECEIVED
2660

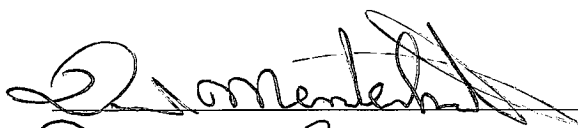
SEP 29 2015

Andy Goleman
SANGAMON COUNTY AUDITOR

FILED
SEP 30 2015
SEP 30 2015
Sangamon County Clerk

NOW THEREFORE BE IT RESOLVED, this 6th day of October, 2015 the Sangamon County Board finds that an execution of the Intergovernmental Agreement between the County, the City and ETSB is in the best interest of the health, safety and welfare of the citizens of Sangamon County.

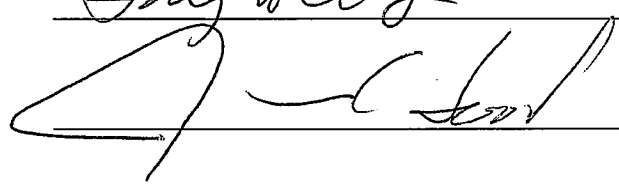
Respectfully Submitted,

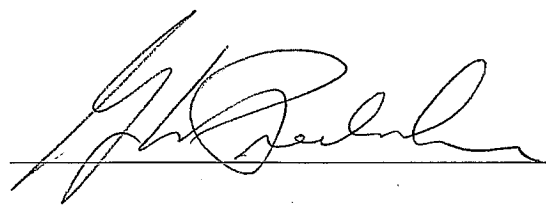


Jason Pitt

Tom E. Hull

Jay Bell





Intergovernmental Cooperation Agreement
with
E 9-1-1, Sangamon County, City of Springfield
for the
Integrated Criminal Justice/Public Safety Initiative

This Agreement (the "Agreement") is made as of this 6th day of October, 2015, (the "Effective Date"), pursuant to Article 7, Section 10 of the Illinois Constitution of 1970 and the Intergovernmental Cooperation Act (5 ILCS 220/1 *et seq.*) and the Emergency Telephone System Act (50 ILCS 750/0.01 *et seq.*), by and between the County of Sangamon, a body politic and corporate (the "County"), the City of Springfield, a municipal corporation, (the "City"), and The Sangamon County Emergency Telephone System Board, a board established pursuant to the Emergency Telephone System Act (50 ILCS 750/0.01 *et seq.*) ("E 9-1-1").

RECITALS:

WHEREAS, Article VII, Section 10 of the Illinois Constitution of 1970 and the Intergovernmental Cooperation Act (5 ILCS 220/1 *et seq.*) provide that units of local government may contract or otherwise associate among themselves to obtain or share services;

WHEREAS, E 9-1-1 and Sangamon County entered into an Intergovernmental Cooperation Agreement dated June 13, 2006 for the purpose of creating the E&S ICJ/PSI referenced herein as the "Original Intergovernmental Cooperation Agreement";

WHEREAS, execution of an Intergovernmental Cooperation Agreement adopting in part and modifying in part the original Intergovernmental Cooperation Agreement dated June 13, 2006, would most efficiently and clearly define roles, duties and costs of all participants.

WHEREAS, this Amended Intergovernmental Cooperation Agreement shall be referenced herein as the “Agreement”, the “Intergovernmental Agreement” or the “Intergovernmental Cooperation Agreement”;

WHEREAS, this Agreement is entered into for the purpose of setting forth the terms and conditions of developing and providing services as related to The E 9-1-1, Sangamon County, Springfield Integrated Criminal Justice/Public Safety Initiative (“the ESS ICJ/PSI”);

WHEREAS, the E 9-1-1, the County, and the City shall be referred cumulatively as “the Participants”;

WHEREAS, The ESS Governance Committee as sanctioned by Attachment A of this Agreement shall consist of representatives from the E 9-1-1, the County, and the City;

WHEREAS, The ESS Governance Committee shall be the single point of reference for all Participants and Third Parties;

WHEREAS, the Participants desire to share in the procurement, implementation, maintenance, and enhancements of an integrated computer hardware and software solution (the “Integrated Solution”), as part of the ESS ICJ/PSI;

WHEREAS, the Integrated Solution and associated information provided by the ESS ICJ/PSI shall only be available to the E 9-1-1, the County, the City and such other participants as may enter into Intergovernmental Cooperation Agreements with the Participants or for whom the Participants have regulatory governmental reporting responsibilities such as the State of Illinois and the Federal government;

WHEREAS, the Participants desire to participate in the costs of development, implementation, and on-going maintenance of this initiative; and

WHEREAS, it is in the public's interest for the Participants to be provided the ESS ICJ/PSI Integrated Solution and associated information for its use, subject to certain limitations provided herein, for the Participants to contribute to the cost of procuring, developing, and maintaining this information through a joint initiative, and for the use of such information by anyone other than the Participant to be subject to certain limitations;

AGREEMENTS:

NOW, THEREFORE, in consideration of the foregoing premises, mutual agreements hereinafter made and as identified as Attachments A through D, and other good and valuable consideration, the receipt and adequacy of which is hereby acknowledged, the parties agree as follows:

1. Definitions.

- (a) "Automated Field Reporting" (AFR) refers to a computer software and functional solution that: Automates the incident and other reporting processes from the patrol car. Optimally, AFR allows the capture of incident and report information and then

electronically sends the report to a supervisor for approval and submission to the Records Management System.

- (b) "City" refers to the City of Springfield, Illinois and its divisions and departments.
- (c) "Computer Aided Dispatch" (CAD) refers to a computer software and functional solution that: Fully automates the call-taking and dispatching functions of a law enforcement (Public Safety) agency and initiates and manages dispatch and incidents.
- (d) "Costs of Annual Maintenance" shall mean the amount of monetary and in-kind consideration paid to the Selected Vendor by the Participant(s) for its share of the external, non-Participant, charges for materials, labor, and services incurred in the annual maintenance of the Integrated Criminal Justice/Public Safety System to support the ESS ICJ/PSI.
- (e) "Costs of Enhancements" shall mean the amount of monetary and in-kind consideration paid to the Selected Vendor by the Participant(s) for its share of the external, non-Participant, charges for materials, labor, and services incurred in software or hardware enhancements requested of the Participants, Other Participants, or any Third Party.
- (f) "Costs of Procurement and Implementation" shall mean the amount of monetary and in-kind consideration paid to the Selected Vendor by the Participant(s) for its share of the external, non-Participant, charges for materials, labor, and services incurred in the identification, procurement, customization, and implementation of an Integrated Criminal Justice/Public Safety System to support the ESS ICJ/PSI.
- (g) "County" refers to the County of Sangamon, Illinois and its divisions and departments.
- (h) "Database Administrator" refers to the functions of an individual responsible for the implementation, maintenance, retrieval and structural integrity of the ESS ICJ/PSI databases.
- (i) "E 9-1-1" refers to the Sangamon County Emergency Telephone System Board and its divisions and departments.
- (j) "ESS Governance Committee" refers to those members responsible for direction and oversight of the Integrated Criminal Justice/Public Safety Initiative as appointed through Attachment A of this Agreement.
- (k) "ESS ICJ/PSI On-Going Personnel Support and Computer Hardware Upgrades" describes the Participant's commitment of staff resources and Computer Hardware Upgrades to ensure the long-term continuance of the ESS ICJ/PSI integration program.

- (l) "Fire Management System" (FMS) refers to a computer software and functional solution that: Captures and maintains incident related events and event investigation for Fire and EMS support including tracking and inspection of public safety equipment.
- (m) "Full Time Equivalent (FTE)" shall mean one person (or a group of persons whose total time commitment equals that of one person) dedicated to the assigned activity or task during the entire scheduled workday.
- (n) "Jail Management System" (JMS) refers to a computer software and functional solution that: Assists with the full management of a jail or correctional facility, including tracking inmate and facility data.
- (o) "Mobile Data Computing" (MDC) refers to a computer software and functional solution: Comprised of several hardware and software technologies working together to allow law enforcement, fire and EMS (Public Safety) officers to access, receive, create and exchange information wirelessly in the field.
- (p) "Network Infrastructure" shall include the computer server hardware and operating software, additional third party network support software and physical devices (i.e. back-up/recovery), physical wiring, data base support, Local or Wide Area Network (LAN or WAN) telecommunications support for the ESS ICJ/PSI.
- (q) "Other Participants" shall mean one or more individuals or entities that enter into Intergovernmental Cooperation Agreements with the Participants and does not include the Participants that execute this Agreement.
- (r) "Participant" shall mean the parties identified in the first paragraph of this Agreement.
- (s) "Selected Vendor" shall mean the vendor selected and approved by the Participants to provide the ESS ICJ/PSI.
- (t) "Records Management System" (RMS) refers to a computer software and functional solution that: Captures, maintains and analyzes all law enforcement agency and incident-related event information and is vital to the day-to-day operations of tracking and managing criminal and non-criminal events, investigations, and personnel.
- (u) "Third Party" shall mean a person or entity other than a party to this Agreement.

2. Term of Agreement. This Agreement is effective from the date first written above and will remain in effect for a period of five (5) years retroactive to the date of the Standard Software Maintenance Agreement executed by the parties hereto with a start date of 1/1/2013, and may be

renegotiated between the Participants to coincide with future maintenance agreements. Nothing herein authorizes a Participant to grant software licensing beyond the scope authorized by the Participant's contractual agreement with Selected Vendor.

3. ESS Governance Committee. The Participants of this Agreement do hereby sanction the formation of The E 9-1-1, Sangamon County, Springfield Integrated Criminal Justice/Public Safety Governance Committee, referenced in brief throughout this document as "The ESS Governance Committee", established to oversee the implementation and execution of the Integrated Criminal Justice/Public Safety Initiative and to provide recommendations to the Participants as necessary. The ESS Governance Committee shall adhere to the bylaws established in Attachment A of this Agreement and made a part hereof. Participants of this agreement shall adhere to and abide by the decisions properly before the ESS Governance Committee.

4. This paragraph left intentionally blank.

5. Costs of Enhancements. In consideration of the rights and obligations of the parties as provided in this Agreement, each Participant agrees to pay the Selected Vendor the Costs of one-time charges accrued from requests by that Participant for enhancements to ESS ICJ/PSI software modules and/or Network Infrastructure.

6. Additional Costs. Participants agree to share equally in any administrative costs associated with the ESS Governance Committee.

7. ESS ICJ/PSI On-Going Personnel Support and Computer Hardware Upgrades.
The Participants shall each provide departmental personnel, or contractual personnel at their

discretion and funding, to support the ESS ICJ/PSI Integrated Solution and Network Infrastructure. This personnel commitment has been defined in Attachment B "ESS ICJ/PSI On-Going Personnel Support" of this Agreement and made a part hereof. The Participants acknowledge that the support requirements on Attachment B are crucial to the ESS ICJ/PSI, and agree to use their best efforts to comply with those requirements.

Any variation from the required personnel support as documented in Attachment B must be presented to and approved by the ESS Governance Committee. In the event that one or more support personnel become unavailable, the Participant will be required to provide a qualified replacement(s), as identified through the job description, within three months.

The Participants shall each be equally responsible for maintaining and upgrading the computer hardware necessary to effectively and efficiently operate the ESS ICJ/PSI Integrated Solution and Network Infrastructure as determined by the ESS Integration Support Sub-Committee. The Participants acknowledge that maintenance and upgrades are crucial to the ESS ICJ/PSI, and agree to use their best efforts to comply with the system demands.

8. ESS Sub-Committees. The ESS Governance Committee is authorized to create sub-committees as needed.

9. ESS Integration Support Sub-Committee. An ESS Integration Support Sub-Committee shall be created before or during implementation of the first software module of the ESS ICJ/PSI project. The purpose of the ESS Integration Support Sub-Committee shall be to provide recommendations for the efficient and effective operation of the ESS ICJ/PSI Integrated Solution and Network Infrastructure. The Sub-Committee is directly responsible to the ESS Governance Committee and as such shares in the charter of that Committee. Activities of the Sub-Committee shall focus on, but not be limited to, the following as they relate to the ESS ICJ/PSI:

- (a) Identify and recommend resolution for outstanding functional or operational integration issues,
- (b) Determine computer software enhancement recommendations and priorities,
- (c) Identify and prioritize additional Integration Solution educational and training needs,
- (d) Resolve daily computer hardware and software functional and operational support concerns,
- (e) Schedule Third Party computer software upgrades,
- (f) Identify, recommend, and prioritize computer hardware and network upgrades,
- (g) Resolve outstanding data and or user security issues related to the Integrated Solution,
- (h) Document and present any unresolved issues to the ESS Governance Committee for resolution.

The Participants shall provide representative membership for an ESS Integration Support Sub-Committee. The total number of committee members for the initial Sub-Committee shall be at least nine (9) and not exceed fifteen (15), with membership comprised as follows. One each shall be selected as a permanent member from: the ESS Governance Committee; the E 9-1-1; the County Sheriff's Office; the County Information System Department; the County Board Office; the City Mayor's Office; the City Police Department; the City Fire Department; City Water, Light and Power Department; and a maximum of six nominated representatives selected by the nine permanent members described above from a list of nominees provided by the Participants, and the Other Participants collectively. The nine (9) permanent members from the Sub-Committee shall determine the appropriate number of, and candidates for, membership in the ESS Integration Support Sub-Committee from the nominees at its initial meeting. Replacement and additional (not to exceed the

maximum) members, may be nominated and selected as circumstances warrant or Other Participants enter into similar Intergovernmental Cooperation Agreements with the Participants, as provided for in Paragraph 17. The selected individuals shall serve two-year terms and may serve successive terms.

An existing ESS Integration Support Sub-Committee member may be removed from office by a two-thirds vote of the remaining ESS Integration Support Sub-Committee members. Once a two-thirds vote has been rendered, the ESS Integration Support Sub-Committee Chairman shall immediately draft and submit written notification to the ESS Governance Committee and to the affected organization explaining the reasoning for the removal of the member and requesting a new appointment be made within a reasonable period.

The ESS Integration Support Sub-Committee shall select a Chairman during its initial meeting. The Chairman may serve successive terms and shall be selected by internal majority vote on an annual basis.

The ESS Integration Support Sub-Committee will meet on an as needed basis and such other times as called by the Chairman. It shall be the responsibility of the Chairman to publish an agenda prior to the meeting and to publish results of the meeting within a reasonable period of time to all Sub-Committee representatives and to the ESS Governance Committee. A majority of Sub-Committee members shall be required for the transaction of business at any meeting, and the act of the majority of members at any meeting shall be the act of the Sub-Committee. All meetings shall be subject to the Illinois Open Meetings Act.

10. Security. The Participants shall adhere to the Data and User Security Policy outlined in Attachment C and made a part hereof.

11. Ownership. The exchange of data as provided in this Agreement shall not constitute a transfer of title or interest in the respective Participants' ESS ICJ/PSI computer software, the associated data, or other data provided by the Participants. If the ESS ICJ/PSI data is modified or merged into another computer file or program by one of the Participants or is integrated with other programs or data to form derivative products, it shall continue to be subject to the provisions of this Agreement. Sangamon County and E 9-1-1 shall retain ownership of its ESS ICJ/PSI computer software and all such modified, merged, derivative, or integrated programs or products. The City of Springfield shall retain ownership of its ESS ICJ/PSI computer software and all such modified, merged, derivative, or integrated programs or products. The Participants shall jointly own associated data.

The Participants acknowledge and agree that they may collectively enter into negotiations with Other Participants for the use of any Third Party software modules. Any and all agreements for the use of Third Party software modules shall require an amendment to this Agreement and a subsequent Intergovernmental Cooperation Agreement with the Other Participants for the use of this software. The Participants of this Agreement shall then become signatories of the Intergovernmental Cooperation Agreement with the Other Participants. Any increased costs caused by the joining of Other Participants shall be borne solely by the Other Participant and so reflected in an Intergovernmental Cooperation Agreement with the Other Participant.

The Participants acknowledge and agree that their respective computer network equipment, data and software backup computer equipment, network operating systems, desktop computer hardware, and mobile computing equipment shall be owned by the Participant where the physical equipment resides.

The Participants acknowledge and agree that their respective ESS ICJ/PSI data may be provided to representatives of The E 9-1-1, The County and The City, without amendment or other negotiation, while in the duty of administering the laws of the land. It shall be the responsibility of the ESS Governance Committee to ensure The E 9-1-1, The County and The City recipients of ESS ICJ/PSI data adhere to the polices as set forth by the Network Usage Policy outlined in Attachment D.

The Participants acknowledge and agree that their respective ESS ICJ/PSI data may be provided by the ESS Governance Committee to Other Participants that have entered into Intergovernmental Cooperation Agreements with the Participants and, additionally, to Third Parties as indicated in this Agreement providing all recipients adhere to the polices as set forth by the Network Security Policy outlined in Attachment D.

The Participants acknowledge and agree that integration system data may be released though subpoena and or through a Freedom of Information Act (FOIA). It will be the responsibility of each Participant to immediately notify Participants of any such subpoena or FOIA request.

12. Distribution of Information. The computer software and ESS ICJ/PSI associated data is to be solely retained and used by the Participants as provided in this Agreement. In no instance, except as provided in Paragraph 11 of this Agreement, is the computer software or ESS ICJ/PSI data to be sold, leased, copied, loaned, or transferred, in whole or in part, to other public agencies, private individuals, private entities, or non-profit entities. Nothing contained herein shall preclude off-site redundancy.

Security access – 3rd party products

The New World System Application provides for proper security controls to restrict each agencies user access to their data.

However, other software vendor products, sometimes referred to as "3rd party software products", such as "Crystal Reports", will not utilize the New World System Application Security, but will be forced to adhere to the New World System Data Base Security.

Therefore, the following policy is being included here to provide a means for one of the ICJS partners, that is a signer to this document, to formally request more extensive data access using a "3rd party software product".

Step 1

The Party wishing to make the Data Base Access submits a written request to the ICJS Infrastructure Committee. The request should include the specific program to be used to extract the requested data along with a list of the data to be extracted. The request should also include the safeguards to be used to insure only the requested data will be extracted.

Step 2

Representatives of all three ICJS partners represented on the Infrastructure Committee sign for receipt of the request and retain a copy of the receipt signed by all Partners.

Step 3

All three Partner representatives on the Infrastructure Committee discuss and either approve or disapprove the request. If approved, all Partners acknowledge the approval on the receipt document and each party retains a copy of the approval signed by all three Partners. If denied, the requester may take the request to the Governance Committee for consideration. The Governance Committee will have the final approval or denial authority.

13. Requests for ESS ICJ/PSI Data. The Participants hereby acknowledge and agree to notify the ESS Governance Committee in the event it receives a request for ESS ICJ/PSI Data.

14. Limitation of Liability. All liability, loss, or damage as a result of any and all claims, demands, costs, expenses, or judgments arising out of, or relating to, activities of the Participants or Other Participants will be the sole responsibility of said party. Nothing herein will be construed as a waiver by the Participants or the Other Participants of any governmental immunity as provided by statute or modified by court decision.

THE PARTICIPANTS HEREBY ACKNOWLEDGE AND AGREE THAT THE RESPECTIVE PARTIES OF THIS AGREEMENT MAKE NO WARRANTY TO EACH OTHER, EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE REGARDING THE INTEGRATED SOLUTION OR THE ASSOCIATED ESS ICJ/PSI DATA DELIVERED HEREOF, NOR ASSUMES ANY LEGAL LIABILITY OR RESPONSIBILITY FOR THE ACCURACY, FUNCTIONING, COMPLETENESS, OR USEFULNESS THEREOF.

The Participants acknowledge and agree that the software solution and ESS ICJ/PSI data are subject to constant change and are shared by each as is, with all faults and without warranty of any kind as to its accuracy, completeness, or correctness.

The Participants acknowledge and agree that the respective parties of this Agreement shall not be subject to liability to each other for human errors, defects or failure of machines, or any material used in connection with the machines, including, but not limited to, tapes, disks, and energy. Furthermore, the Participants shall be not be subject to liability for damages due to any lost profits or consequential damages, or claims of any kind by virtue of entering into this Agreement.

The Participants acknowledge and agree that the respective parties of this Agreement, their officers, agents, consultants, contractors, and employees are hereby released from any and all claims, third party claims, actions, or causes of action for damages, including, but not limited to, the costs of

recovering, reprogramming, or reproducing any information or data, damage to property, damages for personal injury, loss of life, lost savings, or other special, incidental or consequential damages arising from or related to the use of, or inability to use, the ESS ICJ/PSI Integrated Solution and associated data.

15. This paragraph intentionally left blank.

16. Relationship of Parties. The relationship of the Participants is and will continue to be that of independent governmental entities. No liability or benefits, such as workers' compensation, pension rights, or insurance rights, arising out of or related to a contract for hire or employee/employer relationship accrues to the Participants by virtue of this Agreement.

17. Additional Participants. It is understood and acknowledged by the Participants that the Participants may enter into similar Intergovernmental Cooperation Agreements with Third Parties to provide additional integrated criminal justice and public safety computer software and data support; to further integrate the proposed software modules and ESS ICJ/PSI data with the court services of The County; or to integrate software modules and ESS ICJ/PSI data with peer agency, state agency or federal agency Criminal Justice/Public Safety initiatives. The fee charged to said unit(s) shall be determined by the ESS Governance Committee depending on, but not limited to:

- (a) The computer software modules and network infrastructure requested by these units;
- (b) The development activities, if any, necessary to integrate the software, hardware, and/or data;
- (c) The number and division of units of work such as dispatch seats, patrol cars, etc.;
- (d) The type and duration of computer software and hardware coverage;
- (e) The additional fees charged by the Third Party software vendor.

18. Assignment. This Agreement may not be assigned, transferred, or in any way disposed of by any of the Participants without the prior written consent of the ESS Governance Committee, and the ESS Governance Committee may not assign without consent of the Participants.

19. Governing Law. This Agreement and all actions arising from it must be governed by, subject to, and construed in accordance with the laws of the State of Illinois.

20. Notice. All notices, consents, approvals, and other communications under this Agreement must be in writing and will be deemed to have been duly given when received by the addressee if sent by nationally recognized overnight delivery service (return receipt requested) or five (5) business days after the postmark if sent via regular U.S. mail to the appropriate addresses as set forth below:

If to the E 9-1-1:
Executive Director,
Sangamon Co Emergency
Telephone System Dept
2000 Shale Street
Springfield, IL. 62703

If to the County:
Chairman, Sangamon County
County Board Office
200 S. Ninth, Room 201
Springfield, IL. 62701

If to the City:
Office of the Mayor
Municipal Center East
800 East Monroe
Springfield, IL. 62701

21. Dispute Resolution. Should any dispute arise between any of the Participants concerning the terms, conditions, or requirements of this Agreement, the parties will attempt to resolve the dispute through discussions and negotiations with the members of the ESS Governance Committee. The parties shall be required to undertake a minimum of six (6) hours of discussion and negotiation with the members of the ESS Governance Committee prior to initiating judicial proceedings.

22. General.

(a) Binding Effect. This Agreement shall inure to the benefit of and shall be binding upon The E 9-1-1, The County, and The City and their respective successors and assigns.

(b) Integrated Agreement. This Agreement, and its attachments, constitute the entire agreement between the parties hereto concerning identification, procurement, customization, implementation, enhancement and maintenance of the ESS ICJ/PSI solution and associated data and the use of this solution and data; and supersedes all previous agreements, promises, representations, understandings, and negotiations, whether written or oral, among the parties with respect to the subject matter hereof. By execution of this agreement, Sangamon County and E 9-1-1 does hereby terminate the Intergovernmental Cooperation Agreement dated June 13, 2006 adopting this Agreement in its place.

(c) Amendments. No amendment to this Agreement is effective unless it references this Agreement and is written, signed, and acknowledged by duly authorized representatives of all parties hereto.

The Participants agree that they will, from time to time, execute, acknowledge and deliver, or cause to be executed, acknowledged and delivered, such supplements hereto and such further instruments as may reasonably be required for carrying out the expressed intention of this Agreement.

(d) Severability. If any provision of this Agreement is held invalid or unenforceable by any court of competent jurisdiction, the other provisions of this Agreement will remain in full force and effect. Any provision of this Agreement held invalid or

unenforceable only in part or degree will remain in full force and effect to the extent not held invalid or unenforceable.

(e) Time of the Essence. With regard to all dates and time periods set forth or referred to in this Agreement, time is of the essence.

(f) Execution of Counterparts. This Agreement may be executed in one or more counterparts, each of which will be deemed to be an original copy of this Agreement, and all of which, when taken together, will be deemed to constitute one and the same Agreement.

23. Nature of Obligations. All terms and conditions contained herein are intended to be absolute and irrevocable conditions hereof and are agreed to by the Participants. All Participants shall cooperate with and abide by all Federal Rules, Regulations, and Certifications required of a Participant for implementation and continued operation of the ESS ICJ/PSI, including but not limited to 28 C.F.R. Parts 23 and 66, and as amended.

IN WITNESS WHEREOF, the parties have caused this Intergovernmental Cooperation Agreement to be executed by their duly authorized officers as of the date first above written.

<u>THE E 9-1-1,</u>
By: _____ Its Board Chairman
Attest: _____ E 9-1-1 Executive Director

<u>THE County</u>
By: _____ Its Board Chairman
Attest: _____ County Clerk

<u>THE City</u>
By: _____ Its Mayor
Attest: _____ City Clerk

Attachment A:

ESS Governance Committee Bylaws

This document supersedes all previous agreements, promises, representations, understandings, and negotiations, whether written or oral, among the parties with respect to the ESS Governance Committee and its prior appointments. The Intergovernmental Cooperation Agreement authorizes the formation of an E 9-1-1, Sangamon County, Springfield Integrated Criminal Justice/Public Safety Governance Committee, which shall be referenced throughout the remainder of this document as the “ESS Governance Committee” or “Committee”. This Committee is created to administer, facilitate, and promote the long-term success of the Integrated Criminal Justice/Public Safety Initiative for its Participants.

Membership: Each Participant of this same Agreement shall appoint a single representative for membership on the ESS Governance Committee. The representatives will serve a term of four (4) years, and may serve successive terms, beginning immediately as of the first day of execution of the Intergovernmental Cooperation Agreement. Upon conclusion of their term, or at such time as the appointee is no longer able to serve as an ESS Governance Committee member, the Participant shall appoint another representative to fill the remainder of the uncompleted term or the next full term.

An existing ESS Governance Committee member may be removed from office by a majority vote of the remaining ESS Governance Committee members. Once a majority vote has been rendered, the remaining ESS Governance Committee members shall immediately draft and submit written notification to the affected Intergovernmental Cooperation Agreement Participant, explaining reasoning for the removal of the member and requesting a new appointment be made by the Participant within 30 days of the date of removal.

Organizational Structure: Upon the initial meeting, the ESS Governance Committee shall select a single member to chair and organize the meetings. This Chairman shall be assigned on an annual basis from within the participating Committee members and may not serve in successive terms. The Chairman will provide the liaison function between the ESS Governance Committee, Participants and Other Participants of the Intergovernmental Cooperation Agreement, the ESS

Integration Support Sub-Committee, and Third Party resources. The Chairman may appoint a Secretary from within the membership, for the purpose of scheduling the meetings, preparing and distributing the minutes from the meetings, and other miscellaneous administrative duties.

Meetings: The ESS Governance Committee will meet on an as needed basis as determined by its members on an as needed basis. All ESS Governance Committee meetings shall have published minutes, which will, at a minimum, include the meeting date and time, meeting agenda, a list of meeting participants, policies discussed, issues addressed, and the outcome of any voting decisions. The ESS Governance Committee Chairman shall prepare and route a meeting agenda to each ESS Governance Committee member at least 48 hours prior to the upcoming meeting. All meetings shall be conducted in accordance with the Open Meetings Act. Each member, or the member's proxy representative, shall be required to be in attendance at each meeting. The members may bring additional non-voting representatives to the meeting as subject matter experts or listeners. Meetings shall not be conducted without a quorum being present, and a quorum consists of three (3) members.

At the initial meeting, the ESS Governance Committee will establish the format for submission, status, and resolution of outstanding issues to be presented before the ESS Governance Committee. During the meetings, at a minimum the Committee will address old business, current issue status, and new business including issues to be brought before the Committee. As issues are presented, each ESS Governance Committee member (or their designated expert) shall be granted reasonable time to present their position related to the policy or issue at hand. The Chairman will call for a vote and each ESS Governance Committee member will cast a single vote with no abstentions. A majority vote will be required for resolution of a policy or issue. Any additional rules or guidelines pertaining to the meeting, its content, or management shall be established and administered internally by the ESS Governance Committee.

These bylaws may be amended by unanimous approval between the Participants. They are created to ensure fair and equitable management of human and technical resources in support of the implementation and ongoing maintenance of the Integrated Criminal Justice/Public Safety Initiative (ESS ICJ/PSI) while providing dynamic resolution to outstanding personnel, functional, and/or technical issues. The ESS Governance Committee shall not make any decisions or require any actions which would violate the provisions as set forth in their respective Vendor contracts.

The powers and duties of the committee are:

- (a) Providing a minimum of one ESS Governance Committee member as representation on the ESS Integration Support Sub-Committee as designated in the Intergovernmental Cooperation Agreement;
- (b) The formation and execution of procedures for the timely resolution of outstanding issues as presented by Participants or Other Participants of the Intergovernmental Cooperation Agreement, the ESS Integration Support Sub-Committee, and other governing and/or legislative bodies.
- (c) The formation and execution of procedures to evaluate enhancements or modification and make recommendations to the Participants for these enhancements or modifications to the ESS ICJ/PSI software modules and or Network Infrastructure.
- (d) To provide recommendations for personnel staffing and computer hardware upgrades to the Participants.
- (e) Providing a communication conduit for all Participants and Other Participants; seeking internal top-level understanding and approval on controversial issues; and conveying the ESS ICJ/PSI direction and decisions to all appropriate internal personnel.

Attachment B:

ESS ICJ/PSI On-Going Personnel Support

The following chart represents the responsibilities necessary to support the identified information technology software and hardware activities for each Participant:

- (a) The E 9-1-1.
 - System / Security Administrator
 - CAD Administrator
 - Mobile Administrator

- (b) The County.
 - System / Security Administrator
 - Records Administrator
 - JMS Administrator
 - Mobile / Field Reporting Administrator

- (c) The City.
 - System / Security Administrator
 - CAD/Records Administrator
 - Fire Administrator
 - Mobile / Field Reporting Administrator

Attachment C

ESS Criminal Justice/Public Safety Operation

The following reflects obligations of the City of Springfield for integration with the E 9-1-1 / Sangamon County Criminal Justice/Public Safety Information Systems Upgrade Project:

1. Additional Computer Equipment:

The E 9-1-1 , Sangamon County and City of Springfield agree to divide equally between all three parties the cost of additional hardware to upgrade the existing Criminal Justice / Public Safety solution throughout the duration of this Agreement. This includes server equipment, networking equipment, routers, switches, and other peripheral equipment. The hardware described herein does not include locally installed personal computers, internal networks, mobile computing, bar coding, scanning, video recording, imaging devices, or other technical equipment used solely for the individual agency and not specifically for the Criminal Justice / Public Safety project. The agency(s) seeking the additional equipment must document and submit their request to the ESS Governance Committee. Once approved, the ESS Governance Committee will coordinate, through the appropriate authorities within their respective agency, for reimbursement to the procuring agency(s).

2. Springfield Emergency Operations Center:

The City of Springfield shall provide necessary equipment and software, as authorized by

New World Systems, to support the Emergency Dispatch Stations within the City of Springfield Emergency Operations Center.

3. System Security:

E 9-1-1 , Sangamon County and the City of Springfield shall each assign a single individual that will be granted New World Systems' Superuser rights in the production Criminal Justice / Public Safety system. The City of Springfield may assign one additional Superuser. The Superuser for each agency shall adhere to the Data and User Security Policies. Superuser authority shall exceed the limitations placed in Attachment D. Furthermore, the Superuser shall be responsible to fulfill the obligations and constraints as negotiated in their agency specific contract with New World Systems.

NETWORK USAGE POLICY

Integrated Criminal Justice System
NETWORK USAGE POLICY

NETWORK USAGE POLICY

POLICY DEVELOPMENT PROCESS

This Network Usage policy is intended to be a policy and procedure which outlines computer, computer use, data storage, data use, networking, and security of data files and hardware for Client Users of the ICJS. Consequently, as result of technological advances as well as ever changing security risks, this policy will be reviewed as needed. Such reviews are intended to assess the efficiency and effectiveness of the policy and provide an established process for amending the policy. The policy as amended and approved by the ESS Governance Committee will be in effect upon its approval.

POLICY STATEMENT

Sangamon County expects Users of the Public Safety Data System computer, network, and/or data resources to utilize such resources in a responsible and professional manner. This policy provides guidelines for the appropriate use of ICJS computer, network, and/or data resources. The privilege to use the computing resources is associated with specific responsibilities outlined in this policy.

POLICY PURPOSE

The ICJS is designed to provide technical and technological support to the infrastructure. To provide administrative, technical and technological support to the ICJS and other Users computers, computer systems, and networks for both hardware and software functions.

These policies are intended to provide for the security and functionality of that portion of the Computer Network under the direct control of Sangamon County Public Safety Data System. This Computer and Network Policy governs use of computer systems including all computers owned and operated by the Sangamon County Public Safety Data System, and that access the ICJS; and, includes hardware, software, data, communication networks associated with those systems, and password protected accounts assigned to City of Springfield, Sangamon County, and User client computer users. The scope of the policy is limited to employees, administrators, and staff of the City of Springfield, County, ETSD, SCCDS, and those employees of any client agency using any computer, other network equipment, or resources owned or operated by the Sangamon County Public Safety Data System. Acceptance and use of any City of Springfield or Sangamon County owned equipment implies agreement to the policies stated herein.

DEFINITIONS

Authorized use: Authorized use of City of Springfield or Sangamon County owned equipment and network resources consistent with the Public Safety Mission of ICJS and this policy.

Authorized User: An authorized user is an employee granted access to the ICJS network, equipment and/or resources.

NETWORK USAGE POLICY

Authorized users include, but are not limited to employees of the City of Springfield, County, ETSD and SCCDS, and other Client Agency employees. Personnel who are considered authorized users will change periodically according to this policy or changes in employment or position status.

An authorized user is a person who has been issued a valid account allowing access to a particular piece of equipment, program, or system. A valid account is an account issued by the employee(s) designated by the ICJS to administer access to the programs. Generally this will be the System Administrators. A valid account is an account issued by the personnel designated to administer access to the programs. Generally this will be the Security Officers.

Guidelines for Appropriate Use

Access to the Sangamon County Public Safety Data System, whether local or remote, is a privilege requiring individuals to act in a responsible, courteous manner while respecting the rights of other users and the integrity of the computing system and related resources. The following privileges are conditional upon acceptance of the ensuing responsibilities.

User Privileges – Privacy

Computer users must respect the privacy of other computer users. Attempts (electronic or otherwise) to gain unauthorized access to the system or to unauthorized departmental information violate ICJS policy and may violate applicable law.

User Responsibilities

Access to resources infrastructure both within and beyond the ICJS requires that each user accept the responsibility to protect the rights of the Sangamon County Public Safety Data System. Sangamon County and City of Springfield expects each user affiliated with the Client Departments to be a responsible user of its resources, and as such, each user is accountable for his or her actions, and those originating from his or her computer or Department assigned computer as a condition of continued use.

Privacy of Information

A user must not intentionally seek or provide information on, obtain copies of, or modify data files, programs, or passwords belonging to the ICJS without the permission of ESS Governance Committee. Users who are authorized access to Departmental information are required to preserve the confidentiality of such information.

Property Rights

A user must attribute and honor the property rights of the County and City of Springfield.

Harassment

No User of the ICJS may, under any circumstances, use access to ICJS computers or networks to libel, slander, or harass any person.

NETWORK USAGE POLICY

Computer Harassment includes but is not limited to:

Intentionally using a computer to trouble, intimidate, or threaten another person by conveying obscene language, pictures, or other materials, or threaten bodily harm to the recipient or the recipient's immediate family.

Intentionally using a computer to contact another person repeatedly with the intent to harass, whether or not any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease.

Integrity and Security of Information System Resources

A computer user must respect the integrity of computer-based information system resources and is strictly prohibited from attempting to circumvent or subvert any of the City of Springfield or Sangamon County computer and network security measures. This does not preclude use of security tools by ICJS Administration personnel.

New World Systems Database Access

Direct Database Connections to the ICJS are limited to properly designated Super Users, System Administrators, and Security Officers. No other personnel are authorized to make a direct database connection without prior authorization and approval of the ICJS Infrastructure Committee and must be under direct supervision by one or more of the Super Users, System Administrators or Security Officers.

Portable Data Files/Media

A computer user is not to insert and access any portable data/media disk, tape, or CD into the drive or drives of any ICJS computer with the intent to install software without the permission of the ICJS Administration personnel. (Not applicable to System Administration Personnel when performing their normal duties)

Unauthorized or Destructive Programs

A computer user must not intentionally develop or use programs, which disrupt other computer users, damage hardware or software, or access restricted portions of the Sangamon County Public Safety Data System. Such unauthorized use may result in civil and or criminal action.

Unauthorized Access

A computer user must not seek to gain unauthorized access to information resources or to facilitate unauthorized access by others. Accessing the ICJS via an unauthorized IP address constitutes unauthorized access.

Sharing Access

NETWORK USAGE POLICY

Computer passwords and/or password protected accounts are assigned to an individual user and must not be shared with others. A computer user is responsible for any use of his or her account. A computer user must report any unauthorized use of his or her account immediately to system administration personnel.

Permitting Unauthorized Access

A computer user must not run or otherwise configure software or hardware to intercept or decode passwords to intentionally allow access by unauthorized users.

Unauthorized Monitoring

A computer user may not use computing resources for unauthorized monitoring of electronic communication.

Privileged Access

A computer user who is provided special access to information or other special computing privileges will use such access and privileges only in performing official duties. Information accessed in this manner is considered confidential.

Adding New Authorized Users

Access to the ICJS will be limited to the County, SCCDS, and ETSD personnel except as otherwise specified in the following.

Police and Fire and EMS personnel requiring access to certain programs and records to perform their regularly assigned duties. These personnel will be designated by the Chiefs of the various Departments and the Sheriff of Sangamon County. Each has the authority to designate personnel within his/her own department or grant access to other departments for accessing certain records available only in his/her department's records.

Each Department Head grants Administrator Access to the ICJS Technical Support Personnel for the purpose of upgrading, troubleshooting, and repair of programs under direct control of the Sangamon County Public Safety Data System. Further, each Department Head authorizes the ICJS Technical Support Personnel to grant access to Program Vendor Technical Personnel for upgrading, troubleshooting, and repair of the Vendor's programs. This implied authority is granted by each department's acceptance and use of these programs.

New personnel or personnel with new duties requiring access can be added as need at any time. New access requests will be submitted in written form to the ICJS Technical Support.

Review/Termination of Access

When a computer user ceases to be an employee of the City of Springfield, County, ETSD, or SCCDS or a Client Agency, his or her access will be terminated. This information will be transmitted in writing to ICJS Administration personnel within 24 hours of termination. Access for such personnel will be removed immediately upon receipt of official termination. To ensure

NETWORK USAGE POLICY

minimum possibility of unauthorized access by retired, resigned, or terminated personnel, User Accounts will be automatically disabled after 90 days of no sign-in activity.

If a computer user is assigned a new position and/or responsibilities within the City of Springfield, County, ETSD, SCCDS, or a Client Agency, his or her access authorization must be reviewed. Individuals must not use facilities, accounts, access codes, privileges, or information for which they are not **authorized** in their new assignment.

Annual Security Access Audit

On an annual basis, an audit of all users will be conducted to insure only authorized personnel retain access to the system. This audit will include the City of Springfield, County, ETSD, SCCDS, and all Client Agencies. Each agency will provide in written or acceptable electronic form to ICJS Administration, a list of all authorized users, and a list of all personnel terminated, resigned, or retired since the last Annual Security Access Audit. The format and date of this audit will be provided to each agency in sufficient time for completion prior to the audit date. The designated ICJS Security Officers will conduct this audit.

Use of Copyrighted Information

A computer user is prohibited from using, copying, and storing copyrighted computer software except as specifically stipulated by the owner of the copyright or otherwise permitted by copyright law.

Use of Licensed Software

A computer user may not install, copy, or use licensed or unlicensed software on the ICJS computing resources. All software is to be installed and supplied by authorized computer support technicians.

Information Integrity

A computer user should be aware of the potential for and possible effects of manipulating information in electronic form. A computer user should understand the changeable nature of electronically stored information and be prepared to take the appropriate steps to verify the integrity and completeness of information that the user complies or uses.

Personal Use

The ICJS information system resources are not intended for activities unrelated to the City of Springfield, County, ETSD, SCCDS or proper Client Agency functions. Incidental personal use is not allowed.

NETWORK USAGE POLICY

Allocation of Resources

The City of Springfield, County, ETSD or SCCDS may allocate resources in different ways in order to achieve its overall mission. This includes all physical assets and personnel resources associated with the computer and network system. The City of Springfield, County, ETSD and SCCDS reserve the right to determine computer and network use priorities.

In the event that the ICJS computer and network resources become limited (e.g. large volume processes, system upgrades, and maintenance etc.) access to specific computing services may be temporarily restricted.

Network/Workstation Utilization

The City of Springfield, County, or ETSD Network Administrator will monitor utilization of the Department's computers and network resources to determine any additional needs, as well as policy and procedure compliance.

Control of Access to Information

The City of Springfield, County, and ETSD will control access to its information and the devices on which it is stored, manipulated, and transmitted.

Connection of Private Machines

An owner of a private computer who holds a valid user account and who is granted access to the ICJS host machine assumes the privileges and responsibilities specified in this policy.

Internet Connection to Mobile Data Computers

All MDC's which are allowed an internet connection will maintain up to date Antivirus Antimalware protection software. The machines are also required to maintain up to date operating system patches.

The allowed connections to the Internet will be controlled by allowing connection only to specific and necessary URLs. Access beyond these URLs will be blocked and a message stating the block is in place will appear on the user's screen. Since there, currently is no method of grouping users, a list of the allowed URLs will be submitted for the approval of all member agencies. If an agency objects, the URL will not be available to any member agency.

Computer and Network System Administration Policy Administration

The City of Springfield, County, and ETSD, as owner and operator of all computers and networks purchased or leased within the Sangamon County Public Safety Data System, has the authority to delegate oversight of the computer and network systems located at or attached to

NETWORK USAGE POLICY

the ICJS to one or more appropriate individuals within the City of Springfield, County, and ETSD. Each Client Agency retains this right within their agency.

The Computer and Network Policy Administrator shall be responsible for:

1. Administration of the Network Usage Policy.
2. Communication with the appropriate individuals, responsible for insuring compliance with the Network Usage Policy.
3. Designating authority to inspect data, gather electronic evidence, or monitor electronic activity when there is legitimate cause to suspect improper use of computer or network resources.

The standing Administrator of the Network Usage Policy is the ESS Governance Committee.

System Administration

The ESS Governance Committee may designate or authorize another person or persons to manage the computer and network system(s). Such individuals, known as System or Network Administrators, are typically responsible for the technical operations of a particular machine. A System Administrator may access any file and/or folder for the maintenance of network and computing and storage systems.

A System Administrator should use reasonable efforts to:

1. Take precautions against theft of, or damage to, computer and network system components.
2. Execute all hardware and software licensing agreements applicable to the system.
3. Treat information about and information stored by the system's users in an appropriate manner and take precautions to protect the security of a system or network and the information contained therein.
4. Promulgate information about specific policies and procedures that govern access to and use of the system, and services provided or not provided to the user. A written document or electronic message posted on a computer system shall be considered adequate notice. Cooperate with the City of Springfield, County, ETSD and other System Administrators of the computer system or networks within and outside of the Sangamon County Public Safety Data System, to find and correct problems caused on another system by use of the system under the System Administrator's authority.
5. Take reasonable action as authorized by the ESS Governance Committee and the provisions of this policy to implement and enforce the usage and service policies of the system and to provide for the security of the system.

NETWORK USAGE POLICY

6. Take reasonable action as authorized by the ESS Governance Committee and the provisions of this policy to inspect, monitor, or temporarily suspend access privileges in the event that such action is determined as necessary or appropriate to maintain the integrity of the computer system, network, or the protection of other users and individuals.

A System Administrator is equally accountable to the Network Usage Policy as any other user. A System Administrator who violates any provision of the Network Usage Policy, or who misuses his or her authority, is subject to disciplinary action.

System Security

The ESS Governance Committee may designate or authorize another person or persons to secure the computer and network system(s). Such individuals, known as Security Officers, are responsible for:

1. Security Administration of the Network Usage Policy.
2. Communication with the appropriate individuals, responsible for insuring compliance with the Network Usage Policy.
3. Grant authority for all personnel requiring access to the system, based on requirements of the authorizing agency.
4. Monitor compliance with the security procedures in this policy.
5. Conduct the Annual Security Access Audit, and certify completion to the ESS Governance Committee, not later than 1 January each year.
6. Designating authority to inspect data, gather electronic evidence, or monitor electronic activity when there is legitimate cause to suspect improper use of computer or network resources.
7. Conduct an annual Audit of all MDC Telephone Numbers.

Sangamon County Responsibilities

User Security

The City of Springfield, County and ETSD have the responsibility to develop, implement, maintain, and enforce appropriate security procedures to ensure the integrity of the ICJS information, however stored, and to take appropriate action when privacy is intentionally violated.

Protection from Harassment

NETWORK USAGE POLICY

The City of Springfield, County and ETSD has the responsibility to develop, implement, maintain, and enforce appropriate anti-harassment procedures for users of its computers or networks and to take appropriate action when harassment occurs.

Copyright and License Provisions

The City of Springfield, County and ETSD have the responsibility to respect and enforce all copyright and license agreements and all laws governing the acquisition and use of such information.

Procedures Related to Alleged Misuse of Computing Privileges

Filing a Complaint

All alleged violations of this policy, shall be reported to ESS Governance Committee.

Response to Alleged Misuse of Computing Privileges

Upon receipt of a complaint, the Infrastructure Committee will gather information relevant to the complaint and take appropriate action. In doing so, the ESS Governance Committee will communicate with appropriate individuals regarding the complaint.

If the ESS Governance Committee has persuasive evidence of misuse of computer and network resources, and if that evidence implicates the computing activities or the computer files of an individual, the ESS Governance Committee is authorized to:

Request that a System Administrator take the necessary technical steps to preserve the user's files for inspection by ESS Governance Committee or authorized authorities.

Determine the nature and immediacy of corrective action.

If a person appears to have violated this policy, and the violation is deemed to be minor by the ESS Governance Committee, and the individual has not been implicated in prior incidents, then the incident may be addressed by the ESS Governance Committee or by the employee's supervisor.

In the case of repeated violations, or if the violation threatens the security of the computer and network system, the ESS Governance Committee may authorize the appropriate System Administrator to temporarily disable any offending or apparently compromised computer accounts, or to temporarily disconnect or block offending computers/users from the network. A user found in violation of this policy is subject to a full range of sanctions, including the loss of computer or network privileges, disciplinary action consistent with the City of Springfield, County, ETSD, and Client Agency rules and regulations, collective bargaining agreements, and legal action. The City of Springfield, County, ETSD, and Client Agencies will meet their responsibility to report violations that may constitute criminal offenses to the appropriate authorities.

NETWORK USAGE POLICY

Archive and backups

ARCHIVE-The copying of certain data to tape or optical media for the purpose of retaining in storage should it be needed in the future. Once the copy is made the data is removed from the Primary system.

BACKUP-The copying of certain data to tape or optical media for the purpose of retaining in storage should it be needed in the future. The data is not removed from the Primary System after the copy is made.

ICJS will be backed up to another media on a daily basis. The backup schedule will be as follows:

Full data backup - Weekly (day to be determined)

Monthly (One Weekly Media will be designated as the Monthly Backup)

Changed Data only - Daily (except on the day of the Weekly backup)

Retention of Backup Media

Daily Media will be retained until the next Weekly Backup.

Weekly Media will be retained until the next designated Monthly Backup.

Monthly Media will be retained until the next Monthly Backup.

Archiving of Data

Archive media will be retained in compliance with the City of Springfield or Sangamon County File retention policies.

DATA DESTRUCTION

This Data Destruction policy is intended to be a policy and procedure which outlines the disposal of hardware for the City of Springfield, SCSO, ETSD, or SCCDS. Consequently, as result of technological advances as well as ever changing security risks, this policy will be reviewed as needed. Such reviews are intended to assess the efficiency and effectiveness of the policy and provide an established process for amending the policy.

Policy Statement

NETWORK USAGE POLICY

Sangamon County expects Users of the Data Destruction policy to dispose of all hardware in a correct and responsible fashion. This policy provides guidelines for the destruction of hardware. The privilege to use the computing resources is associated with specific responsibilities outlined in this policy.

Policy Purpose

The Sangamon County Public Data Destruction policy is designed to provide a guideline for disposing of hardware, insuring data security.

These policies are intended to provide for the security of all information stored on hard drives disposed of by the Sangamon County ETSD. This Data Destruction Policy governs disposal of hardware including all computers owned and operated by the City of Springfield, SCSO, ETSD, SCCDS. The scope of the policy is limited to employees, administrators, and staff of the City of Springfield, SCSO, ETSD, SCCDS, and those employees of any client agency using any computer, other network equipment, or resources owned or operated by the City of Springfield, SCSO, ETSD, or SCCDS. Acceptance and use of any City of Springfield or Sangamon County owned equipment implies agreement to the policies stated herein.

User Privileges – Privacy

Those disposing of Hardware must respect the privacy of former users. Attempts to gain unauthorized access to the system before its purging violates the Data destruction policy and may violate applicable law.

Property Rights

A user must attribute and honor the property rights of the County and City of Springfield.

Integrity and Security of Information System Resources

A computer user must respect the integrity of computer-based information system resources and is strictly prohibited from attempting to circumvent or subvert any of the City of Springfield or Sangamon County computer and network security measures.

Unauthorized Access

A computer user must not seek to gain unauthorized access to information resources or to facilitate unauthorized access by others to critical information before disposal.

Privileged Access

NETWORK USAGE POLICY

A computer user who is provided special access to information or other special computing privileges will use such access and privileges only in performing official duties. Information accessed in this manner is considered confidential.

Sanitation

All electronic media must be properly sanitized before it is transferred from the custody of its current owner. The proper sanitization involves one of two methods that depend on the type of media and the intended disposition of the media.

Overwriting Information

Overwriting of data means replacing previously stored data on a drive or disk with a random pattern of meaningless information. This effectively renders the data unrecoverable and is an acceptable Sanitation method.

Disruption/Destruction of Hardware

Destruction is the process of physically damaging a medium so that it is not usable by any device that may normally be used to read electronic information on the medium, such as a computer, personal hand held device, audio or video player. Operable hard drives must be overwritten prior to disposal. The use of a magnet or other electronic disruption device is also recommended. Documentation of proper sanitization for hard drives is recommended.

Transfer of Hard Drives

Before a hard drive is transferred from one owner to another appropriate care must be taken to ensure that no unauthorized person can access data by ordinary means. All hard drives should be sanitized, however; since the drive is remaining within the department, the hard drive may instead be formatted prior to transfer. While data may still be accessed by using special means, doing so violates Sangamon county code.

Disposal of damaged or inoperable hard drives

The owner must first attempt to overwrite the storage device. If the device cannot be overwritten, the device must be disassembled and mechanically damaged so that it is not usable by a computer.

Procedures Related to Alleged Misuse of Computing Privileges

All alleged violations of this policy, shall be reported to ESS Governance Committee.

Response to Alleged Misuse of Computing Privileges

Upon receipt of a complaint, the ESS Governance Committee will gather information relevant to the complaint and take appropriate action. In doing so, the ESS Governance Committee will communicate with appropriate individuals regarding the complaint.

NETWORK USAGE POLICY

If the ESS Governance Committee has persuasive evidence of misuse of computer and network resources, and if that evidence implicates the computing activities or the computer files of an individual, the ESS Governance Committee is authorized to:

Request that a System Administrator take the necessary technical steps to preserve the user's files for inspection by ESS Governance Committee or authorized authorities.

Determine the nature and immediacy of corrective action.

If a person appears to have violated this policy, and the violation is deemed to be minor by the ESS Governance Committee, and the individual has not been implicated in prior incidents, then the incident may be addressed by the ESS Governance Committee or by the employee's supervisor.

In the case of repeated violations, or if the violation threatens the security of the computer and network system, the ESS Governance Committee may authorize the appropriate System Administrator to temporarily disable any offending or apparently compromised computer accounts, or to temporarily disconnect or block offending computers/users from the network.

A user found in violation of this policy is subject to a full range of sanctions, including the loss of computer or network privileges, disciplinary action consistent with the City of Springfield, SCSO, ETSD, and Client Agency rules and regulations, collective bargaining agreements, and legal action. The City of Springfield, SCSO, ETSD, and Client Agencies will meet their responsibility to report violations that may constitute criminal offenses to the appropriate authorities

Revised 3/05/2015