Approved Lisa Thomas 3/24
Date

MINUTES OF THE SELECT COMMITTEE ON INFORMATION MANAGEMENT

The meeting was called to order by Chairperson Morrison at 3:30 p.m. on March 18, 1999, in Room 526-S of the Capitol.

All members were present except Representatives McKinney, Burroughs, and Dean, who were excused.

Committee Staff Present:
Julian Efird, Kansas Legislative Research Department
Audrey Nogle, Kansas Legislative Research Department
Norman Furse, Revisor of Statutes' Office
Gary Deeter, Committee Secretary

Conferees: None.

Others Attending: See attached list.

The SCIM continued the discussion of the Legislative Coordinating Council (LCC) computer policies. (See SCIM minutes for March 16, 1999.) (Attachment 1)

#10: Reporting of Problems.
#11: Off-season use of systems.

Dave Larson, Director, Legislative Computer Services, said # 11 originally anticipated some legislators who might want to take legislative computers home during the off-season.

#12: Privacy of E-mail.

The Chair referred the committee to the Joint Committee on Information Technology policy on e-mail, (Attachment 2) which he said had been adopted by the JCIT but not yet adopted by the LCC.

The consensus of the SCIM was to change the second sentence of Policy #11: "There ~~is~~ *shall be* no capturing and archiving of messages on the Legislative Email system." Representative Farmer noted that e-mail remains temporarily on the network server until retrieved by legislators. Answering questions, Dave Larson said when a legislator retrieves email, the message(s) are automatically deleted from the network server. He said the system is capable of backup or archiving, but neither is done. The consensus of the committee was to continue the present policy to protect the confidentiality of legislative communications.

Staff raised the issue of confidentiality of e-mail through the Information Network of Kansas (INK), which is also available to legislators. Staff will obtain that information and report back to the committee.

#13: Establishment of a "user group."

The Chair expressed hope to establish a user group or list server by January 1, 2000. He said either type

of system could provide interaction between members of a group, such as a committee or a caucus. Staff said other entities outside the legislature had offered to host such a system. Staff noted that user groups and list servers for specific legislative groups may violate the Kansas Open Meetings Act and may take an amendment to the law in order for members to participate in a user group. Further, a user group, if it falls under the jurisdiction of the Open Meetings Act, must provide public access to its communications. Committee discussion focused on ways to provide access, such as a dumb terminal located in the Capitol or statewide public libraries through INK. Representative Farmer noted that committee members communicating by laptops, if they constituted a majority of a quorum, would also raise questions with regard to the Open Meetings Act.

Representative Holmes questioned #8 (b), which prohibits legislative e-mail with other state agencies unless authorized by the LCC. Staff noted that LCC minutes over the years would reflect adjustments in the policy that would effectively nullify the prohibition. The Chair said the LCC adoption of the JCIT e-mail policy would supersede Policy #8.

The members agreed to read the JCIT policies on E-mail and the Internet (Attachments 2 and 3) and discuss them at the next meeting, proposing to join the JCIT in recommending them to the LCC.

The minutes for March 16 were unanimously approved. (Motion, Representative Farmer, second, Representative Holmes.)

The meeting was adjourned at 3:45 p.m. **The next meeting is scheduled for Tuesday, March 23, 1999, at 3:30 p.m. in Room 526-S.**

SELECT COMMITTEE ON
INFORMATION MANAGEMENT

GUEST LIST

DATE: March 18 1999

NAME	REPRESENTING
Dave Larson	legislature
Jeff Russell	LAS

POLICIES AND PROCEDURES FOR COMPUTERS
KANSAS LEGISLATURE
Adopted by the LCC September 1993
Last Amended September 16, 1998

#1 Policy and Procedure: Assignment of machines and other equipment.

Information technology hardware and software is assigned to a legislator's office or a committee office. Regardless of who originally specified and acquired the system, once assigned to an office that configuration remains with that office.

Reassignments are made through the President of the Senate for the Senate and the Speaker of the House for the House of Representatives. All reassignments are coordinated with the Director of Legislative Computer Services and the LAS inventory clerk.

#2. Policy and Procedure: Relocation and movement of hardware or software.

The relocation or movement of information technology hardware and software is to be coordinated through the Director of Legislative Computer Services. Proper reinstallation and reinstallation is important to ensure correct operation and avoid damage to State property. The proper procedure is to contact the Director of Legislative Computer Services and request the service.

#3. Policy and Procedure: Taking information technology hardware and software off-site.

To be determined.

#4. Policy and Procedure: Backup and preservation of data.

The backup and preservation of data on any machine is the responsibility of the operator. There is no system-wide backup procedure or facility. The Legislature does not have the resources to provide backup or preservation of data for every computer in the Legislature.

It is therefore the responsibility of the person using the computer to make the appropriate backups of important data and maintain those backups in a secure environment. This ensures recoverability of data and maintains privacy. Training will be provided all new computer users as to how to make backup copies of data. Anyone needing refresher training for making backups will be readily accommodated. Backing up data is an important activity and should be a part of the normal office procedure. Backup diskettes can be procured through Secretarial Typing Pool.

#5. Policy and Procedure: Security

Various security measures are available to every legislative computer user. Private data should be protected by security measures. It is the responsibility of the computer user to protect their data with the proper use of security. Training in the range of security measures and their application will be provided all new legislative computer users. Any legislative computer user needing refresher training in the use of

Attachment 1
SCIM 3-18-99

security measures will be readily accommodated.

E-Mail provides additional security with the use of a password assigned to every legislator at the beginning of each session.

Many security methods resort to the use of passwords. The password is the key that unlocks security and allows access to the data. Passwords are only effective if they are sufficiently complex and hard to crack, remain confidential and are changed reasonably often.

Every legislative computer user is responsible for the protection and privacy of their password.

Office security is also the responsibility of the legislative offices. Locking doors, desks and cabinets is the responsibility of the office inhabitants. Access to important data is first secured by protecting the computer and backups of data from unauthorized hands.

No legislative computer user shall create a TCP/IP connection with a modem while connected to the legislative network. (Amended September 16, 1998.)

#6. Policy and Procedure: Standard Software at the Legislature.

The standard software in use at the Legislature is determined by the Director of Computer Services. The list of standard software is maintained and published by the office. The Director of Legislative Computer Services or his designee periodically arranges training and provides support for these applications. Other software that may be within the Legislature can not be guaranteed on-site assistance.

The Director of Legislative Computer Services or his designee will always attempt to assist any legislative staff with a software question but can not guarantee an answer for non-supported products.

Training in the standard software will be provided and encouraged. Training for non-supported products will be authorized by the President of the Senate for the Senate and the Speaker of the House for the House of Representatives.

#7. **Policy and Procedure: Copying Software.**

The Legislature does not approve of unauthorized copying of software. Software licenses are to be honored. In general, most software licenses allow copying of software for backup and archival purposes only.

#8. **Policy and Procedure: Access to the Legislative Network.**

The Legislature has developed and implemented a network of computers for the benefit of the Legislature. There may be instances where individuals may request access to the Legislative network. Possible requests for access may come from:

(a) Legislators - Any Legislator that desires to network their personal computer to the Legislative network must first request permission from the President of the Senate for the Senate and the Speaker of the House for the House of Representatives. Upon receiving this approval, the requestor must contact the Director of Legislative Computer Services for coordination of the access. The legislator will bear all costs for hardware and software required to network their personal computer plus a one time fee of $100 to cover the incremental costs to the Legislature of expanding its network.

Support of the legislator's computer is still the responsibility of the legislator, however the Director of Legislative Computer Services will assist the legislator with networking issues and possible resolution. It may be in some rare instances impossible to network a legislators personal computer to the Legislative network. Although rare and hard to predict, this possibility must be understood by the legislator before they undertake the expense of networking and the Legislature will not be responsible for results.

(b) Other State agencies - The Legislative network is for the benefit of the Legislature, access by other state agencies is not permitted. However, the exchange of electronic mail with personnel of executive branch agencies may be authorized by the LCC. The LCC shall decide which electronic mail transactions shall be beneficial to the Legislature and therefore authorized. (Amended December 19, 1994.)

(c) Lobbyists, associations, businesses and other entities. The Legislative network is for the benefit of the Legislature and access by other entities is not permitted.

#9. Policy and Procedure: Computer supplies.

The Legislature will provide computer supplies for the legislative computer network. Legislators with personal computers who wish to use them at the Capitol during session will also receive supplies from Legislative Administrative Services. Supplies for legislator's personal computers will be tracked and limits are set by the LCC. These limits can not be exceeded without permission of the Senate President for the Senate and the Speaker of the House for the House of Representatives.

Computer supplies are defined as consumables such as ribbons, printer cartridges, floppy disks, paper etc. Legislative Administrative Services will acquire these supplies but may not stock every item. A stock of computer supplies will be maintained for the technology used by the legislative computer network. Legislators with personal computers may find that supplies for their particular configuration may need to be ordered.

Computer supplies for legislator's personal computers are provided only during the legislative session.

#10. Policy and Procedure: Reporting of problems.

As it is inevitable that problems will arise, the following procedure for problem resolution must be followed in order:

(1) Check the obvious. Is the electricity on? Has something jiggled loose? What was I doing, did I really do what I intended? Was there anything in my training, my training handouts or my manual that addresses this problem?

(2) Call a "first responder". A First Responder is an individual who has both the computer experience and legislative office experience to answer most problems. Check your Legislative Staff directory for the phone number.

(3) All problems not resolved at this point should be forwarded to the Director of Legislative Computer Services. The First Responder will forward the request to the Director and provide a history of actions to date. The Director will determine who and how to proceed.

This policy will allow quicker resolution, ability to track major problems, avoid duplicate reporting of problems and minimize charges for outside repair services.

#11. Policy and Procedure: Off season use of systems

To be decided

#12. Policy and Procedure: Privacy of EMail.

The exchange of messages and other information on the Legislative network is considered private. There is no capturing and archiving of messages on the Legislative Email system. Any unforeseen "crash" of the Legislative network could result in a few lost messages which under this policy could not be recovered and would need to be resent. Such occurrences will be very infrequent.

#13. Policy and Procedure: Establishment of a "user group".

To be decided

#14. Policy and Procedure: Access to INK

The legislative network provides, as a service, access to the Information Network of Kansas (INK). This service is for the benefit of the legislature and as such, use is restricted to official legislative business. No member of the legislature or any staff member of the legislative branch shall provide access through the legislative network to the Information Network of Kansas to any individual or entity who is not a member of the legislature or a staff member of the legislative branch. (Adopted December 13, 1993.)

JCIT
12/15/98
FINAL

SUBJECT: Electronic Mail Policy

1. Purpose. The purpose of this policy is to establish a common understanding of the policies, guidelines and responsibilities for e-mail in the Kansas legislature. The advantages of e-mail include the ease and speed of preparation and transmission, very low cost and the ability to process transmitted documents and data on another computer. E-mail and other forms of electronic communications play a major role in the efficiency with which government conducts its business. Therefore the legislature advocates the use of this technology within applicable law and policies.

2. Definitions.

a. **Archive.** An archive is very long-term storage system for records that are no longer in active use but may be required in the future. An archive should have the attributes of a record keeping system except that query capabilities, convenience features and retrieval speed may be reduced to provide very low cost, very long-term storage.

b. **Certification authority.** Certification authorities issue, securely store and electronically verify the validity of certificates or digital IDs.

c. **Chat.** Chat is a function of some software packages that permits one or more parties to communicate with messages in real time with each other. Thus, chat is a groupware product that offers the opportunity to establish a virtual meeting.

d. **Directory.** An electronic directory provides contact and other information about its members.

e. **Electronic mail.** An electronic message or a document between one party and one or more other parties is called electronic mail or e-mail. E-mail may contain attachments in text, audio, or video format.

f. **Electronic mail system.** A computer system used to create, send and receive messages that may contain other electronic documents, files, or information as attachments. An e-mail system is not a repository with the attributes of a record keeping system.

g. **Electronic signature**. A common form of electronic signature is based upon a pair of electronic keys, one private and one public, that when used with appropriate software attach an ID or certificate to the message to enable authentication of message content and identification of the originator. Keys may also be used to encrypt the contents of e-mail to insure that the contents are readable only by intended addressees.

Attachment 2
SCIM 3-18-99

h. **Encryption.** Software that applies a mathematical process to a message, file or document, makes it unreadable to everyone except to those with the proper key to decrypt it into readable form.

3. E-mail Policy Provisions.

a. **E-mail accounts.** Legislative agencies will provide each staff member with an e-mail account for that period of time during which the origination and receipt of e-mail is an appropriate part of the staff member's job function.

b. **Legislator e-mail accounts.** Legislators may obtain Internet service and an e-mail account from the provider of their choice and may be reimbursed for some or all of this expense in accordance with the direction of the LCC.

c. **Directory maintenance.** All persons provided with legislative e-mail accounts on either internal or external systems will have an e-mail address in the agencies' and the state's electronic directory with name, position and contact information. Agencies are responsible to maintain current and accurate directory information.

d. **Agency responsibilities.** Legislative agencies are responsible for the maintenance of directories for all assigned accounts. Legislative agencies are required to provide their staff with guidance regarding law and legislative policies related to e-mail.

e. **Account-holder responsibilities.** The person to whom a legislative e-mail account is assigned is responsible for compliance with law and legislative policies applicable to e-mail. An account holder shall not reassign their account to another person. Account holders shall protect passwords, personal identification numbers and any other security devices entrusted to their care from disclosure or compromise. Account holders shall use electronic communications in a responsible and professional manner.

f. **Anonymous/misidentified e-mail prohibited.** Legislative e-mail accounts shall not be used: (1) To send e-mail anonymously; (2) in a manner that disguises the origination of a message; or (3) in conjunction with any device or service that causes the apparent originator of the message to be other than the real originator. E-mail from constituents and others may be referred to in a manner that protects their identity from disclosure.

g. **Personal use.** Legislative e-mail services may be used for incidental personal purposes provided that, in addition to compliance with state law and policies, such use does not: (1) Directly or indirectly interfere with state agency operations of computer or communications systems; (2) burden a state agency with noticeable incremental cost; (3) interfere with the user's employment or other obligations to the state; and (4) state or imply that the content is a communication identified with, endorsed by or approved by a state government agency or official or employee.

h. **Privacy.** Unless required by court order, the state will not inspect or monitor the content of e-mail sent to or from members or staff of the legislature. Nevertheless, account holders must be aware that temporary storage of e-mail records may occur to insure against loss until deleted by the recipient and incidental analysis of network traffic may occur for performance or problem solving reasons.

i. **Legislators' communications**. E-mail communications addressed to or from legislators are private papers not state records. E-mail between staff concerning matters related to communications with a legislator that have not been released for the record are confidential until made public or released by the legislator.

j. **E-mail electronic logs and back-up storage**. In order to protect these communications, e-mail messages and attachments may be stored for limited periods for recovery purposes so long as the content is not viewed, monitored or disclosed. When the temporary records are disposed of, the disposition will be done in a manner that does not permit subsequent inspection of the storage media and recovery of any of the records.

k. **E-mail included in legislative agency records management programs.** Legislative agencies shall incorporate e-mail into their records management program, policies and procedures. Before a document is placed into an electronic record keeping system that will maintain official file copy on electronic media, each document shall be identified sufficiently to enable authorized personnel to retrieve, protect and carry out the disposition of documents in the system. Appropriate identifying information for each document maintained on the electronic media may include: Office of origin, file code, key words for retrieval, addresses, signature, author, date, authorized disposition and security or sensitivity.

l. **Chat.** Chat policies and procedures are not covered in this policy.

4. Improper communications. The legislative e-mail system shall not be used to send material that the sender knows or should know will be offensive to the recipient or material that promotes sexual harassment. The legislative e-mail system shall not be used for content that contains slurs or promotes discrimination on the basis of race, religion, color, sex, disability, national origin or ancestry. It is unprofessional to send e-mail having: (1) Content that would generally be considered inflammatory when received by others or if published or (2) content that would generally be considered to be disrespectful to those in authority. Although the legislature does not condone use of its facilities for offensive materials, it cannot protect users from receiving, from outside sources, e-mail that users may find offensive.

5. Restrictions on use of the e-mail system. Legislative e-mail services will not be used for unlawful activities, commercial purposes not under the auspices of the legislature, personal financial gain or in a manner that abridges the legal intellectual property rights of others.

6. Confidential and sensitive material. In sending confidential or sensitive materials, care must be exercised to insure that such mail is not sent to the wrong recipient or printed in a location where individuals other than the intended recipient can view the message. Although the legislature will make every effort to maintain a secure system, it cannot protect users from disclosure of confidential information by authorized recipients.

7. Administration of the E-mail System. The Legislative Chief Information Technology Officer shall be responsible for the central administration of the legislative e-mail system. This administration shall consist of the following matters:

a. **Naming conventions.** Naming conventions for state owned e-mail accounts shall be specified to insure that the system functions in accordance with policy and does so effectively and efficiently. These conventions will be established in a manner to support a central state government directory.

b. **Network administration.** Central network administration shall be established to support implementation and integration of e-mail and associated services policies and effective operations. Although agencies may be responsible to maintain their directories to reflect current information, central network administration shall coordinate and insure synchronization of all e-mail directories, including those directories serving other branches of state government. All software necessary for effective e-mail and associated services, access and security shall be coordinated and published to insure consistency of product and software release and service packages and timing of updates. Technical personnel with access to or maintenance privileges for operating and system software occupy a very trusted position and should have a criminal history record check and background check through the KBI.

c. **Remote Access and security.** Remote access shall be provided to legislative staff and legislators. Such access shall be secure for both the account holder and the legislative network resources and shall be easy for a novice account holder to operate. Software for access and security shall be centrally administered.

d. **Electronic signatures and public/private keys.** The Legislative Chief Information Technology Officer will establish certificate authority services and provide public and private keys so that confidential communications may be encrypted in a manner to be private between the author and the intended recipients. The email system shall be established in a manner to accommodate such services easily with limited user training.

e. **E-mail guidelines.** The Legislative Chief Information Technology Officer shall prepare guidelines and training for the use of the legislative e-mail system to all legislative agencies and users of the legislative e-mail system.

JCIT
12/15/98
FINAL

Subject: Internet Policy

1. **Purpose**. To provide a common understanding of the Internet policies and practices applicable to all users of the legislative network services and computer systems.

2. **Communications with the public**. It is the intent of the Kansas legislature that all of its organizations will proactively develop and provide electronic access to the public for all information and services permitted by law and policy. Use of the Internet, Internet standard technologies and industry standard electronic commerce services is cost effective for the government and convenient and cost effective for the public.

   a. **Common gateway**. All public information and services will be available through the State of Kansas Internet gateway, the Information Network of Kansas (INK). Agencies may develop and host information and services internally, through any agency or commercial provider, as long as such services are consistent with INK services and appearance standards and are not distinguishable from other state services provided through INK. Only fully tested, operational, production versions of site and information or services will be made available for public access.

   b. **Current and accurate information.** All information provided by legislative agencies through the Internet will be current or clearly dated file information and all informatin will be maintained in as accurate a state as possible. Each legislative agency head will establish and implement the necessary procedures to meet this requirement.

   c. **Privacy for the public**. A privacy statement will be provided on each legislative agency's web site and clearly indicated wherever personal identifying information is obtained from the public. Such information will only be solicited when appropriate to the government or public function being provided and only the minimum information necessary to carry out that function will be solicited. As a minimum, such information will only be used for the declared purposes when it was collected and will not be further disclosed to business entities or the public unless so indicated when and where it was collected or unless otherwise required bylaw.

   d. **Copyright, trademark and registration laws**. Legislative agencies' web sites and the actions of legislative staff shall be in compliance with copyright, trademark and registration laws.

   e. **ADA compliance**. All legislative agencies' web sites will be designed and developed to be compliant with the Americans with Disabilities Act.

Attachment 3
SCIM 3-18-99

f. **Public communications**. All legislative agencies' web sites will provide a means for public communications to the agency via e-mail. Each legislative agency shall establish procedures for review and appropriate response, where called for, to such communications.

g. **Agency review and approval of site content**. The head of each legislative agency shall review site content for consistency with law and legislative policies and for appropriateness of content. Agencies shall record statistics on the usage of web site information and services.

h. **Security**. Each legislative agency's web site shall be protected by software to monitor and report what may be unauthorized electronic access or modifications to the site and should be operated according to a written security plan. The security plan will include the physical security of the web server, the network security for the web site including mechanisms employed to monitor electronic access to the server, the identity of people authorized to access the server for maintenance of content and technical management and the identity of the site security manager. The plan should identify to whom reports of attempted unauthorized access are promptly provided and expectation of response thereto. If the web site host is on the state network, the Legislative Chief Information Technology Officer must approve the security plan, including firewall configurations. All transactions involving sensitive data will be encrypted. Legislative agency heads will insure that the requisite plans and procedures are established and maintained.

i. **Backup**. Legislative agencies' web servers providing information and services to the public shall be backed up at least daily and a plan to reconstitute the site in the event of a disaster shall be developed, tested, and maintained.

3. **Legislator use of the Internet**. Legislators may use an Internet Services Provider (ISP) of their choice and are not bound by any of the administrative requirements of this policy. Legislators are encouraged to observe and to support the legislature's use of electronic information and services for the benefit of Kansas citizens.

4. **Appropriate staff use of the Internet**. Internet access and tools shall be provided to those legislative staff wherever it may enhance the individual staff member's assignment and services to the state. Use of the provided Internet access shall be consistent with state law and legislative policies. This legislative policy incorporates the attached Internet Code of Conduct.

a. **Personal use**. Incidental personal use of the provided Internet services is permitted as long as such use does not: (1) Directly or indirectly interfere with the government's computer or communications systems; (2) burden an agency or the legislature with noticeable incremental cost; (3) interfere with the user's employment, assignment or other obligations to the state; (4) constitute or support a commercial activity associated with the user; and (5) state or imply that the content is a communication identified with, endorsed by or approved by a state government agency, official or employee.

b. **Monitoring and inspection of use**. Staff use of the Internet will not be routinely monitored, inspected or disclosed to any party unless required by court order.

c. **Incidental monitoring**. The construction, maintenance, repairs, and operation of the legislative computer systems network may occasionally result in incidental random monitoring of Internet access lines by diagnostic equipment. No record of such monitoring may be kept beyond the time necessary to correct the problem.

5. **Webmaster**. The Legislative Chief Information Technology Officer shall designate a webmaster who has the skills necessary for the design, development and administration of Internet web sites. The webmaster shall coordinate the web services of all legislative agencies with the INK and with other organizations that may be associated with the development or providing of web services for legislative agencies.

6. **Responsibilities**. The head of each legislative agency shall be responsible for compliance of the agency and its staff with the provisions of this policy and shall be responsible for training to effectively use the tools and capabilities of the Internet for the agency's mission and responsibilities under this policy. The Legislative Chief Information Technology Officer is responsible for the publication and maintenance of this policy, providing the services of a webmaster and contracting for commonly needed training services. Basic training in the use of Internet "browser" software, basic search techniques and identification of some sites of interest to those in government will be made available for legislators on a scheduled group basis.

7. **Effective date**. This policy is effective January 1, 1999.

INTERNET CODE OF CONDUCT

Legislative Staff

General use. Internet access and tools provided to legislative staff shall be used to enhance the individual staff member's assignment and services to the state. Use of the provided Internet access shall be consistent with state law and legislative policies.

1. **Incidental personal use**. Incidental personal use of the provided Internet services is permitted as long as such use does not: (1) Directly or indirectly interfere with the government's computer or communications systems; (2) burden an agency or the legislature with noticeable incremental cost; (3) interfere with the user's employment, assignment or other obligations to the state; (4) constitute or support a commercial activity associated with the user; and (5) state or imply that the content is identified with, endorsed by or approved by a state government agency, official or employee.

2. **Prohibited use**. Legislative staff shall not use the provided Internet access for commercial use unless it is a legislative enterprise approved by the Legislative Coordinating Council. Legislative staff shall not use state Internet access for campaign purposes. Legislative staff shall not establish any web site that may appear to be official unless the site is approved by their legislative agency head and the site resides on a computer system that is owned or leased by or under a contractual agreement to a state agency. Legislative staff will not publish confidential or restricted information or data on the Internet. Legislative staff will not make state provided Internet access available to non-legislative staff unless appropriate to conducting the business of the state.

3. **Accurate representation**. Legislative staff shall represent themselves, their agency and the state legislature accurately and honestly through electronic information or service content.

4. **Copyright, trademark, and registration laws**. Legislative staff will comply with copyright, trademark and registration laws.