KANSAS DEPARTMENT ON AGING

INFORMATION SYSTEMS GUIDE

Original: June 1, 2003
Revised: September 1, 2006

[This page intentionally left blank]

TABLE OF CONTENTS

INTRODUCTION

This Information Systems Guide for employees of the Kansas Department on Aging (KDOA) and other users of KDOA information systems explains agency policy on:

- **Acceptable use** – which actions are allowed and which are prohibited when people use KDOA information systems;

- **Security** – how we protect our information systems and the data they contain from accidental or deliberate damage, loss or disclosure;

- **Data confidentiality and integrity** – requirements that we safeguard the privacy of Kansas citizens whom we serve, and the correctness of data in our systems;

- **Electronic records** – our obligations to manage electronic documents and data as official records of state business;

- **Software protection** – observance of law and contracts in our use of software products; and

- **System administration** – the processes we follow to help employees observe requirements of these policies.

Since procedures will likely change over time, there are no "How To" steps in this Guide. Procedures are covered in separate documents provided in training courses for KDOA system users, and available on the KDOA Intranet Page (http://intra.aging.state.ks.us). See the Intranet page for information on available training courses, schedules and registration.

Questions or suggestions about this Guide may be referred to the KDOA Help Desk, voice telephone: **785-296-4987**; fax: 785-296-0256; e-mail: **HelpDesk@aging.state.ks.us**.

APPLICABILITY AND ACKNOWLEDGEMENT

The policy direction contained in this Guide applies to:

- All full-time and part-time employees of the Kansas Department on Aging.
- The following people while working temporarily or under instruction at the KDOA:
    - ➢ Employees of other state, federal or local-government agencies;
    - ➢ Employees of state-contracted staffing firms;
    - ➢ Employees of other organizations participating in Aging programs, specifically including Area Agencies on Aging and providers of aging-related services;
    - ➢ Volunteers.
- Individuals or employees of companies contracted by or on behalf of the KDOA.

The KDOA employee who supervises or coordinates activities of people in the above categories is responsible for making them aware of this Guide and its contents. This expectation can be met if the person attends the Information System Orientation for new employees.

Essential policies related to information and system security are also contained in the KDOA Employee Handbook. Each full- and part-time KDOA employee is required to acknowledge their receipt, reading and comprehension of these Employee Handbook policies by signing an Information Security Acknowledgement form, which is maintained in the employee's official personnel folder. This Information Systems Guide augments the Employee Handbook by providing additional explanation and guidance for the IS policies which it contains.

YOUR "IS" RESOURCES AND RESPONSIBILITY

Definition. Any device or service by which information is electronically created, communicated, used or stored is part of an "information system," abbreviated "IS." (You may also on occasion see the abbreviation "IT," which stands for "Information Technology.") The following items are all parts of information systems at KDOA:

- Telephones, including wireless and Blackberry devices, and fax machines
- Computers - whether desktop, laptop, handheld, or central server
- Printers, scanners and plotters
- The software that operates computers and other devices
- The data network by which computers and other devices communicate
- Data stored on computer disks and tapes (including documents, e-mail, graphics, etc.)
- Services used by KDOA employees, running on non-KDOA computers (for example, SRS software running on contractors' computers; the Internet; voice mail)

For purposes of managing our resources, the following are not considered to be part of a KDOA information system: photocopiers, printing white boards and audio tape recorders.

Your "IS" Resources and Responsibility, continued

Services Provided. As a KDOA employee, you will need to use information systems regularly. Here are typical features and services which are provided to you:

- A **telephone**, with your own telephone number, at your normal work area.

  Telephones have speakerphone capability; telephone use of the speakerphone in cubicles is to be kept to a minimum to minimize disruption of neighboring employees.

  In Topeka and Wichita offices, KDOA uses the voice mail service provided by the state Division of Information Systems and Communications (DISC). Since there is a monthly charge for DISC service, voice mail availability for each employee is at the discretion of the employee's supervisor and Commissioner. Other KDOA field offices have separate answering machines. Wireless telephones and Blackberry devices may be issued to you by the Procurement Division, depending on the need of the individual for the position. ISD maintains Blackberry devices.

- A **personal computer**, with common office software.

  Each KDOA computer is connected to the KDOA Local Area Network in Topeka. Computers at KDOA field offices in Kinsley, Columbus and Wichita connect to the Topeka network. Other field offices are still connected to KDHE network. LCE laptop users use their 1-800 DISC Dialup accounts to access their Groupwise e-mail and Lotus Notes ACESS application.

  Each authorized computer user has their own user name and password. The user name/password combination is the same for logging in to both the computer itself, and into the network. Field offices have an additional feature with their login - the Virtual Route Forwarding - which encrypts the data communicated between their computer and the network in the Topeka office. Virtual Private Network (VPN) is another technology used at KDOA to log in remotely to the system securely.

- **Network services** - features which are available to you because your computer is connected to the KDOA network:

  Printing - You can use one or more network attached printers located near your work area. Topeka office workers can also use central color laser printers.

  E-mail - Each KDOA employee receives an e-mail user name and storage area, along with their network user name.

  Faxing - KDOA provides the ability to send and receive fax documents as part of the agency e-mail system. There are also fax machines available, for sending images of paper documents.

(continued on next page)

Internet - Each KDOA employee has full access to the Internet; their KDOA login user name is also their Internet e-mail name, and the mail domain name is "aging.state.ks.us". Inappropriate use of the internet for unapproved unofficial uses, including but not limited to unauthorized access or distributing of pornographic materials is prohibited.

Streaming Media - Streaming media is blocked except for work related web casts such as legislative hearings, Centers for Medicare and Medicaid information sharing, etc. This service can cause considerable performance issues on the network.

Streaming Audio - Streaming audio is not supported and is discouraged. This would include the listening of online radio stations, satellite music programs, etc over the internet. This service can also cause considerable performance issues on the network.

Personal & shared data storage - Each KDOA employee is allocated space on a central server computer for storing their own data files (the H: drive). They are also provided access to folders and files shared throughout the agency (I: drive) and within their own workgroups (J:, and K: drives). All users have a J: (commission shared) drive. Some users have a G: drive.- (ISD and FilePro users)

System security - Security of the KDOA network from malicious attack and accidental damage is an important service provided to all KDOA employees. Part of this security comes from "firewall" appliances which separate the KDOA (Topeka) Local Area Network from the state network (KANWIN) and the Internet, allowing only authorized communication to pass. Another part is provided by regular backups (copies) of all data on KDOA server computers. Another part is our use of anti-virus software on all desktop, laptop and server computers. Yet another part of system security comes from password-protected screen savers. Spam email filtering and web filtering is also used. Security is covered in depth in a later section.

On-line system information - Each KDOA employee can obtain explanations and procedures about KDOA information systems from the KDOA Intranet Site. Web browsers on KDOA computers are initially set with this page as the one which opens when the browser is activated (the default page). The address is: http://intra.aging.state.ks.us

- **Training** - KDOA conducts in-house training for most aspects of computer and network use as needed by KDOA employees; see the KDOA Intranet Site for information on courses, schedules and signing up. Once signed up for a course, please make every attempt to attend as scheduled - no-shows and last-minute cancellations mean that not only does the original registrant miss out on useful training, but someone else in the agency may have been unnecessarily deprived of a training opportunity.

(continued on next page)

- **Help Desk** - If you have any questions or suggestions about KDOA information services; if you need to report a problem; or if you would like to check out special equipment (such as a laptop computer, projector, etc.), contact the KDOA Information Services Help Desk. The Help Desk is staffed from 7:00 AM to 5:00 PM each business day. You can call **785-296-4987** (there is voice mail in case lines are busy), or send e-mail to: **HelpDesk@aging.state.ks.us**

Your Responsibility. KDOA entrusts each employee with the equipment, software and services they need to do their job. In return, KDOA expects each employee to use these resources responsibly and appropriately. The following sections discuss some particular aspects of your responsibility.

Potential Consequences of Unacceptable Use or Other Violation. Violation by any KDOA employee of agency or state guidelines for use of information systems can put those systems and their data at risk, create a hostile work environment, or expose the agency to legal liability. Accordingly, the agency may respond to acts in violation of these policies and guidelines with disciplinary action, up to and including termination of employment, civil action, and/or, if applicable, criminal prosecution.

ACCEPTABLE USE

KDOA information systems and the data which they contain are state-owned resources for accomplishing official state business. Kansas Administrative Regulations (K.A.R.) 1-17-1 defines "official state business" as "the pursuit of a goal, obligation, function, or duty imposed upon or performed by a state officer or employee required by employment with this state." To preserve the intent of this regulation, while recognizing that KDOA employees and the agency benefit from a pleasant, safe and supportive work environment, the following policies apply:

- **Expected use.** The proper use of KDOA information systems for official state business is the responsibility of each employee. The Information Services Division shall provide regular training sessions for KDOA employees on use of and policies concerning KDOA information systems, to include an orientation session for each new employee.

- **Prohibitions.** The following activities using KDOA information systems are prohibited:

  - ➢ Random or purely recreational use of Internet access ("surfing", downloading movies or music);
  - ➢ Playing computer-based games;
  - ➢ Conduct of for-profit business;
  - ➢ Any action which is illegal, including introduction of "virus" or "worm" programs;

  Any action which could be construed by a reasonable person as intimidating, harassing or otherwise detrimental to professional conduct of state business;

(continued on next page)

<u>Acceptable Use</u> -Prohibitions, continued

- Willful transmission of anonymous e-mail (missing or misleading user name of the sender), unwarranted mass broadcasts of e-mail, or e-mail "chain letters";
- Any action which violates other regulation or policy of KDOA, the state of Kansas, or program-cognizant federal agencies (e.g., Centers for Medicare and Medicaid Services);
- Social, political, commercial or religious representation or solicitation which could in any way be associated with KDOA, Kansas state government, federal agencies, or KDOA business partners and contractors (Area Agencies on Aging, service providers, and associations thereof), unless specifically approved in writing by the Secretary;
- Modification or attempted modification of KDOA Network Operating Systems security settings and/or domain policies, local computer security policies, profiles, security settings, or user account privileges.
- Installation of software (executable programs) without the knowledge and participation of the KDOA Information Services Division.

- **Personal use**. Limited personal use of KDOA information systems is authorized for KDOA employees. The intent of this permission is to allow employees time and resources to conduct short-duration personal business which could not be accomplished outside of their regular hours of work (e.g., make a doctor's appointment, check on school closures). The following conditions apply:

  - <u>What does "limited" mean?</u> The definition of "limited" is a matter of discretion for the employee's supervisor. In general, personal use of KDOA information systems should not impinge on an employee's accomplishment of assigned tasks or completion of work products. Personal use also should not interfere with normal work routines of other KDOA employees.

  - <u>Reimbursement of cost</u>. An employee shall reimburse KDOA for any additional costs incurred by KDOA due to the employee's personal use of information systems. Replacement of equivalent-quality materials (e.g., printer paper) is an acceptable form of reimbursement. Since KDOA pays a flat rate for Internet access and local telephone calls, there is no additional cost associated with personal use of these services. See the KDOA Employee Handbook for policy on personal use of KDOA telephones for both local and long-distance calls.

- **Monitoring**. Oversight of acceptable use of information systems by KDOA employees is a supervisory responsibility. In addition, the agency may, without notice, install and use electronic monitoring capability to:

  - identify Internet sites contacted by KDOA employees;
  - examine routing information and contents of e-mail sent, received and stored with KDOA equipment; and
  - examine contents of data files and electronic documents stored on KDOA-owned devices and storage media.

(continued on next page)

Acceptable Use - Monitoring, continued

The purpose of such monitoring is to identify employees who may be violating this Acceptable Use policy or performing other acts of misconduct. Facts derived from such monitoring will not be used to evaluate an employee's professional performance, beyond counseling or disciplinary action which may be taken and noted.

Note: There is no expectation or guarantee of user privacy on KDOA information systems. Any information which passes through or is stored in KDOA systems may have its source identified and content reviewed, as a result of an agency management decision, request by an authorized external oversight organization, an Open Records request (subject to certain exceptions), or court-directed legal discovery.

- **Assistance**. If you are unsure about whether a particular activity falls within the bounds of "acceptable use" under this policy, check with your supervisor. Technical questions of procedure and capability should be referred to the KDOA Help Desk (785-296-4987).

KDOA employees are granted much autonomy in how they conduct their daily business. This reflects the trust placed by the agency in each employee's maturity, discretion, dedication and sense of responsibility. A handy rule of thumb: if what you are doing with a KDOA resource would make you feel uncomfortable if observed by your coworkers, supervisor, parents, spouse or children, then it probably is not considered an "acceptable use."

SECURITY

Protection of data entrusted to KDOA depends on the attention paid by each employee to proper system security. Careless practice by any one individual can jeopardize not only the data they normally work with (their e-mail and document folders), but all other data on KDOA information systems, as well.

Why do we worry about computer security?

The documents and data contained in KDOA information systems are invaluable to our business. Literally hundreds of thousands of staff hours went into creating the electronic information we have. While paper documents may have been the source for much information we have in the system, their electronic counterparts are easier to create, modify, share, search, recombine, store, communicate and archive. Some may exist in electronic format only (for example, many of your e-mail messages). Some of the information is highly confidential. Some of it will be used to make important decisions about how KDOA will spend program funds to best serve Kansas citizens.

Due to these considerations, each person to whom this Guide applies (see page 1) shall take steps as instructed to *prevent unauthorized people from erasing, damaging, or examining KDOA's business data.*

Even at a personal level, every KDOA employee should be aware of security risks. For example, while an employee is away from their desk, someone could use their unprotected computer to send embarrassing e-mail which appeared to be created by the employee.

What are some specific threats?

Each person to whom this Guide applies must remain aware of the following threats to systems security which are typically encountered within government and industry:

- **Disgruntled employee** – Most security violations are "inside jobs." Someone with a grudge against their employer, their supervisor or a coworker, or who is being terminated from employment, may take personal revenge by wiping out data or causing a system to fail.

- **Industrial espionage** – Someone may stand to gain materially or politically by finding out confidential information from a system, or by planting false information that leads to an incorrect action by the target organization.

- **Curious passerby** – An unattended computer without proper security features can be used by anyone passing by, even a complete stranger looking for a momentary diversion.

- **Criminal intent** – Information stolen from computer sources can be used to identify worthwhile targets for crime: property theft, blackmail, fraud, or, an increasing problem, identity theft, wherein the criminal uses personal information to masquerade as someone else, obtaining credit and running up bills in their name.

- **Malicious attack** – Technologically astute individuals who derive satisfaction from breaking into, manipulating or damaging computer systems are called "hackers" (if they try to cause damage) or "crackers" (if they just look). In one approach, a hacker will find computers with unprotected Internet connections, run hacking software on them without the owners' knowledge, and thus use these computers to launch an attack against the hacker's real target.

- **Random attack** – Some individuals may initiate computer or network damage with no particular target in mind; they do it just because they can. Virus code embedded or attached to e-mail, which perpetuates itself through recipients' e-mail address books, is a prime example.

Despite any perception that KDOA is immune from danger because "we're just a small state agency in Kansas," such threats need to be taken seriously. We have documented attempts by unknown parties to deliberately log on to KDOA computers with unprotected connections to the state's data network. And every year since 1999, the Kansas Bureau of Investigation has monitored systematic attempts by unknown parties outside the United State to access services on every network address assigned to Kansas state agencies.

What does each KDOA employee and "guest worker" need to do?

As explained in KDOA training courses, some of the key things you need to do are:

(continued on next page)

Security - What to do, continued

1. **Establish your own passwords.** New user accounts typically have a standard ("default") password associated with them; the same is true for voice mail security codes. Change this right away, so someone else isn't able to use the default security code to masquerade as you. Once you establish your own password, it is encrypted in the system - not even the Information Services Division can determine what your password is. The Help Desk can set a new password up for you if you forget it, but no one will be able to use the password you establish.

2. **Make passwords difficult for someone to guess.** Follow these guidelines for constructing your own passwords:

   - Minimum eight characters long (six numeric digits for voice mail security codes);
   - Includes at least one numeric digit;
   - Includes at least one lower case letter;
   - Includes at least one upper case letter;
   - No spaces;
   - No simple repetition of letters or numbers;
   - Is not the same as your user (logon) ID;
   - Does NOT include any "real world" information about you that someone else could use to guess your password (e.g., car license number, birth date, name of spouse/child/pet).

3. **DO NOT REVEAL YOUR PASSWORD OR SECURITY CODE TO ANYONE.** Do not write it down on a Post-It note stuck on your computer monitor. Do not tape it to the bottom of your telephone or keyboard. In other words, if it's convenient for you to check it, then it's also convenient for other KDOA employees, the evening cleaning crew, or anyone else who gains access to your office space to find and use it. Similarly, do not put your password into an online file. Do not put it in any automated command scripts (typically used to speed up a login process), including a speed-dial number for accessing your voice mail.

4. **Change passwords regularly.** You never know when someone else has discovered your password. To limit the chances of someone gaining advantage with your password, the KDOA network prompts you to change your password every 60 days. If this isn't done within a short grace period, your password expires and you must contact the Help Desk to re-establish your account. (Your e-mail and files will NOT be discarded if this happens; you just won't be able to get to them.) Your new password should be quite different from your previous ones, rather than a variation.

   If you have a password within the KDOA e-mail system (which allows you to access your e-mail through a web browser over the Internet), you must manually change it when you change your login password.

(continued on next page)

Security - What to do, continued

5. **Beware of "social engineering" attacks.** Individuals that employ the use of deceptive practices aimed at employees to reveal agency information they should not and then use that information to gain access to agency systems. Be especially wary of anyone who asks you for your password to "perform emergency system maintenance." This is a ruse frequently employed by malicious outsiders to gain access to a computer system. Always know the identity of who is requesting the information and why they need to know it. In fact, should you ever be requested to reveal your login user name, password, or network ("IP") address, please notify the Help Desk immediately, as someone is trying to gain unauthorized entry to KDOA systems.

6. **Guard against virus software.** To protect against attacks by computer viruses (malicious computer programs which can affect system performance or delete files):

   - Never open an e-mail attachment sent to you by someone you don't know, or even one sent unexpectedly by an acquaintance (check with them to confirm). Instead, delete the e-mail.
   - Use KDOA's anti-virus software to scan all diskettes or flash drives you use, before copying files. This procedure is covered in KDOA computer system training and related documentation.
   - Use your personal or group folders on the network server (H:, J: G: and K: drives) to store your data and documents, rather than your local hard disk (C: drive). KDOA's network drives are backed up nightly, but C: drives are not.

7. **Don't leave your computer unattended while you are logged in.** To protect against doing this unintentionally:

   - *Set up a password-protected screensaver.* Use features of your desktop computer's operating system (master program) to select a screensaver program, and establish password-protection. Set the screensaver to activate within no more than 20 minutes of keyboard inactivity. Entry of your password is then required to regain access to the computer. This procedure is covered in KDOA computer system training and related documentation.

   - *Manually activate your screensaver when leaving the work area.* The password-protected screensaver can be manually activated by a quick combination of keystrokes. This should become a habit whenever you leave your desk unattended, even for short periods. The procedure is covered in KDOA computer system training and related documentation.

   - *Log out when leaving at the end of the day.* Use the computer's "shutdown ->restart" process to log out. It is better to NOT shut down the computer all the way (turn off the power), since system updates are conducted over the network, after hours, and the computer must be active for this to occur. However, you do not need to remain logged in for these updates.

(continued on next page)

Security - What to do, continued

8. **Protect your storage media.** Store data diskettes and compact disks out of sight unless you are actively using them. Use a locking drawer, bin or storage area whenever possible.

9. **Report security breaches.** If you encounter any situation which looks like it might violate security guidelines for KDOA information systems, notify the Help Desk right away.

10. **Provide management direction.** If you supervise KDOA employees or coordinate the activities of other individuals who must comply with the policies in this Guide, then you have several responsibilities related to information system security:

    - *Classify "your" data.* Identify the category of confidentiality (see Data Confidentiality and Integrity section, below) and official record status (the schedule for record retention and disposition; see Electronic Records section, below) for data under your management control. Different types of data may have different categories or disposition schedules.

    - *Specify access rights.* As guided by the KDOA Help Desk, identify the type of access (Read and/or Write) each person under your oversight should have to system services and to the directories (folders) containing business data within your area of responsibility. If you approve Kansas Aging Management Information System (KAMIS) access for your organization as a KDOA Commissioner, Area Agency Executive Director, service provider Executive Director, or designated alternate, then you must complete the KAMIS Access Authorization form to identify for each of your intended KAMIS users whether they are to have Read, Write and/or Approve privileges for each KAMIS function.

    - *Ensure personnel receive system security training.* Everyone working or being trained at KDOA needs to understand the policies in this Guide. While necessary security training is conducted during new-employee Orientation, making sure people attend this training remains a supervisory responsibility. It is also the supervisor's responsibility to have each employee sign the Acknowledgement form for KDOA policy comprehension, and provide it to the Human Resources Division for filing in the employee's personnel folder.

    - *Watch for violations.* Supervisors have primary responsibility for identifying lapses in conformance to the policies in this Guide, for reporting breaches in system security to the KDOA Help Desk, and for counseling individuals under their supervision who violate these policies.

What does the KDOA Information Services Division do about system security?

The KDOA Information Services Division (ISD) has the following responsibilities:

(continued on next page)

Security - KDOA ISD responsibilities, continued

Firewalls. Establish, maintain and periodically test security "firewall" systems which isolate the KDOA (Topeka) Local Area Network and KDOA remote personal computers from the non-secure state data network (KANWIN) and the Internet. Prevent any external access to KDOA information resources which does not transit this firewall configuration (e.g., modems installed in firewall-protected computers).

- **System Security.** Apply file and directory protections as provided within the network operating system and individual computer operating systems, on all KDOA computers. Specify file and directory access privileges for classes of individual users, as well as user groups. Provide automated mechanisms for examining files, e-mail and active software for virus programs; keep virus data files current.

- **User Accounts.** Establish a user account and security profile for each new user identified by the Human Resources Division. Provide file and directory access, and user group affiliations, based on the individual's job-related "need to know," as established by the employee's supervisor. For users of the Kansas Aging Management Information System (KAMIS), establish user access profiles in the KAMIS User Directory (LDAP) and Oracle database, with privileges as identified by the requesting authority. For KDOA users of systems at DISC, SRS, Kansas Health Policy Authority (KHPA) and KHPA contractors (e.g., EDS), Federal CMS applications, and KDHE lotus notes applications, follow procedures prescribed by the sponsoring entity for obtaining user access.

- **Training and Assistance.** Conduct orientation training of all new users of KDOA systems, which includes the policies in this Guide, with their supporting procedures and documentation. Respond to user requests for information and assistance with respect to information system security policies, procedures and apparent breaches.

- **Documentation and Intranet Site.** Prepare and maintain user documentation, including all procedures necessary for complying with policies in this Guide. Make electronic versions of all such documentation available to authorized users of the KDOA Intranet site. Secure the intranet web site with user access control to access.

- **Authentication and Encryption Keys.** Issue or obtain public/private key combinations for KDOA system users (including users in related external organizations, such as Area Agencies on Aging and providers of aging services) for use in authenticating (digitally signing) electronic files and documents, and in encrypting data for transmission or storage. Provide detailed procedures for how these key pairs are to be used, managed and (for private keys) protected from disclosure.

Security Monitoring. Establish automated and manual procedures to detect attempts at unauthorized entry into protected KDOA computers and networks. Report apparent attacks to the DISC Network Control Center. Conduct tests to identify weaknesses in the security structure of KDOA information systems. When directed by senior management, monitor network communications (including e-mail and Internet site visits) to determine if KDOA employees are violating agency policies.

(continued on next page)

Security - KDOA ISD responsibilities, continued

- **Back Up Data.** Make backup copies of KDOA data in accordance with a prescribed schedule. Use backup copies to provide file recovery services for KDOA system users. Ensure backup copies are periodically stored away from KDOA facilities, for use in disaster recovery. Ensure that backup copies, whether stored on-site or off-site, are protected from accidental or deliberate loss, damage or disclosure of contents.

- Provide email system spam, spoofing, virus, automatic relay, and mailbomb protection.

- Provide internet web browsing protection from virus, spyware, adware, inappropriate site content browsing,

- Provide security procedure of the same at the off site disaster recovery site.

- Administer, install, and maintain up to date computer and network operating systems, third party application software's, and hardware appliance devices, up to date security patch updates.

- **Application Security.** Include security features in all application software purchased or developed, commensurate with the confidentiality category of the data being protected. Document these security features in a Security Plan, produced in accordance with the state Information Technology Architecture and project management guidelines. Ensure security features are tested along with business functionality during unit, integration and system testing. Use configuration control and two-party accountability to prevent unauthorized alteration of application code.

- **Audit Trail.** Preserve records of all security-related actions taken with KDOA systems.

DATA CONFIDENTIALITY AND INTEGRITY

KDOA deals with information which must be protected from loss, unauthorized alteration, or improper disclosure. Certain data about individual citizens must remain confidential under state and federal law; violation of this confidentiality may be subject to criminal penalties. However, the need for information protection is counterbalanced by the public's right to know how their government operates, as reflected in the state Open Records Act. Accordingly, information must be categorized and managed according to its content.

(continued on next page)

Data Confidentiality and Integrity - What information is confidential, continued

What information is considered confidential?

The policy of KDOA is to treat as "confidential" any information which is exempt from disclosure under the Kansas Open Records Act (K.S.A. 1999 Supp. 45-221). The first Open Records Act exemption forbids disclosure of records "specifically prohibited or restricted by federal law…" Significant federal laws which apply to data held by KDOA are the Privacy Act of 1974 (5 U.S.C. 552a) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA, 42 U.S.C. 1320d et. seq., codified in 45 CFR Parts 160, 162 and 164).

The Privacy Act protects information about individual people, "including, but not limited to, [their] education, financial transactions, medical history, and criminal or employment history and that contains [their] name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph…" HIPAA also identifies electronic-format "Protected Health Information" (PHI) about individuals, unauthorized disclosure of which is prohibited under the HIPAA Privacy Rule (45 CFR Parts 160 and 164). KDOA has determined the following information to be included within the scope of Privacy Act and HIPAA protection: Social Security Number and similar identifying numbers (e.g. Medicaid Beneficiary ID), residence address, residence telephone, functional and social status as determined during a formal intake or assessment, and the identity of program customers' associates (such as informal care providers, relatives, carriers of power of attorney, etc.).

Other Kansas Open Records Act exemptions, which are "confidential" within KDOA, include:

- Medical, psychiatric, psychological or alcoholism or drug dependency treatment records which pertain to identifiable patients;
- Personnel records, performance ratings or individually identifiable records pertaining to employees or applicants for employment [with certain exceptions];
- Records of agencies involved in adjudication or civil litigation [in certain conditions];
- Correspondence between a public agency and a private individual [with certain exceptions];
- Software programs for electronic data processing and documentation thereof [with certain conditions];
- Notes, preliminary drafts, research data in the process of analysis, unfunded grant proposals, memoranda, recommendations or other records in which opinions are expressed or policies or actions are proposed [unless revealed in a public forum];
- Records which are compiled for census or research purposes and which pertain to identifiable individuals;
- Specifications for competitive bidding [until the specifications are approved];
- Financial data submitted by contractors in qualification statements to any public agency.

See K.S.A. 1999 Supp. 45-221 for the full list of 43 exempt categories, and for the complete text alluded to in square bracket [ ] notations above.

(continued on next page)

Data Confidentiality and Integrity - What information is confidential, continued

Separate documentation and training is provided within KDOA regarding each employee's responsibilities under HIPAA.

How is confidential information to be protected?

Confidential information in electronic form is to be stored in directories (folders), files (documents) and databases which are accessible only by individuals with a business need to know the information. This access limitation is to be enforced with permission-granting features of operating system and database management software, and protected by user-specific passwords (see the Security section, above).

Confidential information which must be electronically transmitted beyond the boundary of the KDOA firewall computer must be encrypted.

Any paper to be discarded which contains confidential information must be shredded. Do NOT place such materials in either trash baskets or paper recycling bins.

How do we know that information in KDOA systems is trustworthy?

Persons to whom this Guide applies are responsible for protecting data stored in KDOA systems even if that data is not considered "confidential" as defined above.

For data (electronic or on paper; confidential or public) to be useful in carrying out agency business, it must be trustworthy. That is, it must be complete, accurate and current (and, hopefully, relevant). Data in its original, non-electronic form is presumed to possess these desirable attributes. The authenticity and correctness of source data (for example, a Uniform Assessment Instrument prepared about a customer) may be certified by the assessor's signature on the form. More frequently, the fact that data has been entered and approved in KAMIS by trusted personnel at an Area Agency on Aging is adequate authentication of the data. That is because KAMIS has security protections to ensure only authorized users are able to enter and modify data.

Once data has been established in an electronic version, the information system must provide safeguards that the data will not be accidentally or maliciously altered or damaged. The process of preventing unauthorized alteration of data is called protecting data integrity. Protections within KDOA information systems are covered in the Security section, above. Basically, data is kept in locations which are accessible only to trusted individuals who have a business need to create, view or modify the information. The identity of these individuals is confirmed by their knowledge of the unique, secret password associated with their login user name; this process is called user authentication.

To protect the integrity of data entrusted to KDOA, each user of KDOA systems must observe the requirements specified in the Security section, above.

What about information that comes from outside the agency?

As data files and electronic documents become more prevalent means of conducting business beyond the boundaries of KDOA, the security precautions of KDOA systems alone will not be enough to guarantee data integrity. It is important to confirm that an electronic file or document received in a transmission is complete, accurate, current and actually came from its apparent source. Digital signatures, based on public/private key combinations, provide this veracity. An electronic file or document authenticated by digital signature software can be proven to have come from a known single source, and not to have been modified since it was "signed." This type of authentication is so indisputable, it is said to provide non-repudiation – this is, the originator cannot deny having "signed" the file or document. Under Kansas statute, digital signatures with these characteristics have the force of law, just as do physical signatures on paper. For any document which is not authenticated through digital signature, physical signature on a paper version is required, whenever signature is called for by business rules or external mandate.

ELECTRONIC RECORDS

Many of the documents produced by KDOA employees contain information which is of long-term interest to state government and the citizens of Kansas. Such material is regularly archived - sent to the State Historical Society for permanent storage. Other materials are of only transitory concern, and may be discarded when no longer needed. KDOA has a retention and disposition schedule (available at http://intra.aging.state.ks.us/procedures/ProcedureInfo.htm) which describes which types of records need to be stored, and when records need to be discarded or archived. Electronic files, documents and e-mail are also public records which must comply with these guidelines.

What are "records," and why do we worry about them?

The definition of "records" and requirements for managing them are quite clear in Kansas law. The Government Records Preservation Act (K.S.A. 45-401 through 45-413) says the following:

> Government record means all volumes, documents, reports, maps, drawings, charts, indexes, plans, memoranda, sound recordings, microfilms, photographic records and other data, information or documentary material, regardless of physical form or characteristics, storage media or condition of use, made or received by an agency in pursuance of law or in connection with the transaction of official business or bearing on the official activities and functions of any governmental agency. Published material acquired and preserved solely for reference purposes, and stocks of publications, blank forms and duplicated documents are not included within the definition of government records.

Furthermore:

- Government records are public property and cannot be destroyed without authorization from the State Records Board or through an approved retention and disposition schedule (K.S.A. 45-403).

(continued on next page)

Electronic Records - What are records, continued

- Unless specifically exempted, government records are to be kept open for public inspection (K.S.A. 45-215 through 45-223).

These statutes, along with guidance from the State Records Board and the State Archivist at the Kansas State Historical Society, highlight the fact that government agencies have an obligation to document agency actions, decisions and interaction with Kansas citizens; to support the rule of law; and to preserve the history of our state.

KDOA has established record retention and disposition schedules, which have been approved by the State Records Board.

Is there anything special about electronic records?

From the standpoint of content, electronic records (files, documents, data sets, graphic images, audio clips, etc.) should be evaluated, classified and managed just as are their paper counterparts. The record format or media on which they are stored do not alone constitute a record series. For example, "e-mail" is not a record series – how and when individual e-mail messages should be retained, archived or destroyed depends entirely on their contents, not the fact that they are in an e-mail format. Neither are "CD-ROM disks" a record series.

That said, electronic records offer special challenges for records managers:

- They are easily changed or deleted.
- They frequently require special software just to view them.
- This software becomes obsolete (inoperative) over time, especially as new generations of hardware and operating system (control) software are put into place.
- The media used to store electronic records also becomes obsolete over time (e.g., certain formats of tape cartridge), or may physically degrade to the point of losing its contents.

Each state agency must provide the hardware and software needed to store and recover record material, in its complete and final form, during its period of retention.

Who is responsible for managing electronic records?

There are several roles performed which affect electronic records:

- **Data Owner** – While all record material at KDOA actually belongs to the state, the "Owner" of data is the individual who is ultimately responsible for its use, and who determines the ground rules for creating and managing the data:
  - ➢ Identifying types of data within their management scope;
  - ➢ Identifying legitimate business uses of the data;
  - ➢ Identifying the applicable record series;
  - ➢ Specifying how and when data is generated, collected and authenticated;

(continued on next page)

Electronic Records - Who is responsible, continued

- Specifying the level of confidentiality and what security protection is required;
- Specifying who may have what type of access to the data; and
- Periodically reviewing security and record management controls to ensure the data is being handled correctly.

- **Data Custodian** – A Custodian is someone who has been assigned control over particular records, either for a limited time period or permanently, and who must observe data management requirements specified by the Data Owner. A Data Custodian may be required to monitor who accesses the data, and under what security conditions. Typically, storage and retrieval of data during its retention period at KDOA is the Custodian's responsibility. For records created outside KDOA, but distributed or retained at KDOA for business purposes, the Custodian determines which record series designation applies to the record.

- **Originator** – The person who first creates an electronic record is its Originator. The originator could also be the Data Owner, a Data Custodian, or another individual with delegated authority to create the record. For records created within KDOA, the Originator determines which record series designation applies to the record. The Originator also retains the official copy of the record, unless the original record is deliberately transferred to a different Custodian.

- **User** – Anyone who accesses data to make use of its contents is a data User. A User is responsible for observing the management requirements established for electronic records, especially its security protections.

- **Data Administrator (DA)** – The KDOA Data Administrator is the individual who establishes and manages a single repository of data element definitions on behalf of the agency. The DA works with Data Owners to catalog the types of electronic records created and maintained within KDOA. The DA also serves as the authority on how data is to be interpreted within its business context, if there is no single KDOA Data Owner to make such determinations. The DA may also assist KDOA Database Administrators in determining the record series which apply to data elements within the DBAs' custody.

- **Database Administrator (DBA)** – Electronic data may be collected in one or more databases or repositories – data sets organized to be accessed and managed as a unit. Note that a database (the collection of data values or content) is different from the data element repository managed by the Data Administrator (the collection of data definitions, which describe how the data content is to be interpreted). The Database Administrator is the individual with responsibility for creating and managing a database, including its security, backups, and access authorizations for users. A DBA is a Custodian of data sets with any number of Owners and Originators.

- **KDOA Records Manager** – The Records Manager is the individual assigned to develop, publicize, and review conformance to KDOA's records management program. The Records Manager coordinates disposal or archiving of records when those actions become due.

SOFTWARE PROTECTION

Only software which has been legally procured and installed may be run on KDOA computers. The permission to operate commercial software, which is copyrighted material, is most often indicated by KDOA's receipt from the vendor of a license for the software. The license specifies what type of computer the software may run on, how many people can use it at one time, and how many computers it may be installed on at one time.

No illegal reproduction of software. According to the U.S. Copyright Law, illegal reproduction of software can be subject to civil damages of as much as $100,000 and criminal penalties including fines and imprisonment. KDOA employees who make, acquire, or use unauthorized copies of computer software on KDOA computer equipment shall be disciplined as appropriate under the circumstances. Such discipline may include termination of employment. KDOA does not condone the illegal duplication of software.

Software installation. To preserve the legality and integrity of KDOA computer systems, persons to whom this Guide applies may not install any software on any state-owned computer. Any needed software must be installed by KDOA Help Desk staff. Help Desk staff will ensure that only legally licensed software is installed on KDOA computers.

Software inventory. The KDOA Information Services Division (ISD) shall retain, when provided, the original distribution media, license certificates, and copies of download access codes for all software purchased or licensed by the Department on Aging. ISD shall also maintain records of the computer(s) on which each copy of licensed software is installed. ISD may employ automated procedures to detect and report software products installed on any KDOA computer.

Copying software. No person to whom this Guide applies may copy software from a state-owned computer. Backup copies of software may be made only by KDOA ISD.

Certain software products purchased or licensed by KDOA allow their use at alternate locations (e.g., an employee's home computer) under certain conditions. Such installation of software shall always be performed from original media, under supervision of the KDOA Help Desk. Any person who has state-licensed software installed on their non-state-owned computer shall, prior to leaving employment at KDOA, certify in writing that the software has been permanently deleted from their computer, without backup.

Software disposal. ISD shall delete licensed software (exception: operating system software being discarded) from any computer hard disk being sent to the state Surplus Property Division, or otherwise disposed of. Records of disposal shall reflect which software is removed. ISD shall also perform and document the destruction of distribution media for outdated software being discarded.

SYSTEM ADMINISTRATION

The Information Services Division (ISD) is responsible for assembling and managing hardware, software and network components of KDOA information systems. In so doing, ISD must provide the capabilities and protections necessary to allow system users to observe the policies in this Guide.

Granting user access. All requests for user access, or for changes in user security privileges or functional capability, must be made in writing (preferably e-mail) to the KDOA Help Desk by the Human Resources Division for new KDOA employees, or by the supervisor of a current KDOA employee. The Help Desk will establish user accounts and initial passwords for users of the KDOA Local Area Network (which includes the user's desktop personal computer, field office access through the Virtual– Route Forwarding - VRF), and for the following:

- Kansas Aging Management Information System (KAMIS)
- Automated Survey Processing Environment (ASPEN)
- Medicaid Management Information System (MMIS)
- Statewide Human Resources and Personnel system (SHaRP)
- State Accounting and Reporting System (STARS)
- SRS-sponsored systems (e.g., CTMS and DSS)
- KDHE-sponsored systems (e.g., ACCESS and Lotus Notes)
- Remote logins via the DISC mainframe computer
- DISC Dialup accounts for remote dialup access to state services
- Telephone number issuance, programming changes, and/or feature additions.

The Human Resources Division may directly obtain user names and passwords for SHaRP from the state Department of Administration. The Accounting and Financial Management Division may similarly obtain user names and passwords for STARS. In either of these situations, the Division separately registering users of non-KDOA systems must so notify the Help Desk.

Controlling system configuration. ISD is responsible for making sure information system features work as they are intended. The interrelationships of system components across the network may not always be apparent to users. Accordingly, only ISD personnel, or users operating under explicit guidance from the KDOA Help Desk, may alter the hardware connections and placement, or software settings, of information system components. This restriction applies even to special devices, such as printers which may have been purchased by a different KDOA Commission for the exclusive use of that Commission's staff, while those devices are attached to the KDOA network.

ISD is also accountable as the designated property custodian for all KDOA computer hardware and related devices, with the exception of portable equipment purchased by a KDOA Commission for that Commission's exclusive use. ISD shall maintain inventory and configuration records of where all system hardware and software components are installed or stored.

(continued on next page)

System Administration, continued

Reporting system errors. All operating errors detected or suspected within KDOA information systems shall be reported to the KDOA Information Services Help Desk by the person discovering the error condition. Persons reporting errors shall provide amplifying information as requested by the Help Desk, and shall perform simple diagnostic or corrective actions as directed by the Help Desk.

Requesting system changes. Changes to KDOA information systems may be easy to put in place, or may require substantial investment in new hardware, software and staff time. In order to evaluate such impacts and assist management in approving and prioritizing changes, all users of KDOA information systems who desire a change shall prepare and submit a System Change Request form in accordance with procedures published by KDOA ISD The forms can be found as templates in Microsoft Word under the ISD Forms tab or on the intranet site under the KDOA Forms section.

It is neither necessary nor appropriate to request correction of an error condition (i.e., loss of a system capability which existed previously) with a System Change Request.

Help is available! When in doubt about KDOA computers, telephones, software, or related services, please ASK FOR HELP. Your successful performance of work for KDOA and our customers may depend on how well you can operate the information resources you have been assigned. Please attend training in system use. When you encounter an obstacle, please contact the Help Desk for assistance (785-296-4987, e-mail HelpDesk@aging.state.ks.us).

REFERENCES

The authority and requirements for information systems security and general system management within Kansas state government are found in the following documents, sanctioned either by the Information Technology Executive Council (ITEC) or the state Department of Administration (DofA). The policies which govern this KDOA Information Systems Guide are located at http://www.da.ks.gov/itec/ITPoliciesMain.htm.

K.S.A 75-4709 provides that the Secretary of Administration shall make provision for and coordinate all telecommunications services for all divisions, departments and agencies of the state pursuant to policies established by the Information Technology Executive Council.

K.S.A. 1998 Supp. 75-7203 authorizes the ITEC to adopt information resource policies and procedures and provide direction and coordination for the application of the state's information technology resources for all state agencies.

K.S.A. 45-221(A)(16) identifies which public records are not required to be disclosed under the Open Records Act.

(continued on next page)

References, continued

The Legislative Division of Post-Audit evaluates IT performance and security within Kansas state agencies by applying Control Objectives for Information Technology (COBIT) international auditing standards.