All employees must attend KDADS security awareness training upon initial hire and will be required to attend annually or as required.

Security practices are necessary to prevent the unintended creation, modification, disclosure or destruction of information entrusted to the Agency, whether that information is on paper, electronic, spoken or recorded. Protection of information entrusted to KDADS 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 also all other data on KDADS information systems.

1. **Minimum Requirements for Information - Passwords System Security Establish your own password(s).** New user accounts typically have a standard ("default") password associated with them; the same is true for voice mail security codes. Change this immediately to a secure password. If you forget your password contact the Help Desk.

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

- Minimum eight characters long (four 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. **Password Integrity. DO NOT REVEAL OR PROVIDE YOUR PASSWORD OR SECURITY CODE TO ANYONE. DO NOT MAKE YOUR PASSWORD ACCESSIBLE TO OTHERS.**

The KDADS Help Desk staff will never ask you to give them your password. If that information is needed, you will be asked to enter your password into the device yourself. If you have concerns that your secured password has been compromised, contact the Help Desk immediately.

4. **Change passwords regularly.** The KDADS network prompts you to change your password every 60 days. If the password isn't changed within a short grace period, it will expire and you will have to contact the Help Desk to re-establish your account. If an employee fails to input the correct password five (5) times, then the employee will be locked out of the system and will need to contact the KDADS Helpdesk to have the password rest. Once an employee has reset their password, the employee will have to wait a minimum of 15 days before they will be allowed to change their password again.

If you have a password within the KDADS 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.

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

- Emails should not be opened if they are suspicious; instead delete the e-mail or contact the Help Desk for advice.
- Do not run programs downloaded from the Internet. If such a program is needed, call the Help Desk for assistance first.
- Use your personal or group folders on the network server (like H, G and K drives) to store your data and documents, rather than your local hard disk (C: drive). KDADS network drives are backed up nightly, but C: drives are not.

6. **Protect against unauthorized computer use. Do not leave your computer unattended after you have logged in.**

7. **Log out when leaving your work area.** At the end of the day use the computer's "shutdown" and "restart" process to logout. 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.

8. **Protect your storage media.** Store portable data storage devices 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 KDADS information systems, notify the Information Services Help Desk immediately.

10. **Protecting KDADS' consumer information**
KDADS 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 Kansas Open Records Act. Accordingly, information must be categorized and managed according to its content. For more information about the type of information protected, how KDADS' employees safeguard this information, and the times when this information may be used and/or disclosed please see the KDADS Policy 4.1.C (HIPAA) and KDADS Policy 4.5 (Kansas Open Record Act), which are posted on KDADS Intranet.

11. **Protecting Confidential Information.** KDADS's consumer 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.

Protected information which must be electronically transmitted beyond the boundary of the KDADS firewall computer must be encrypted.

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

Additional Policies to consider: KDADS Policy 4.1.C (HIPAA) and KDADS Policy 4.5 (Kansas Open Record Act)