**KEES End-User Security Agreement**

The KEES system is operated to administer the State of Kansas Medicaid and Human Services programs. All data contained in the KEES system, including personnel and client information, regardless of format or venue, is to be considered **confidential** and protected by State of Kansas and Federal law. By using any part of KEES, you agree to all the terms set forth below. These terms are consistent with State of Kansas IT Security policy and procedures, the Social Security Administration (SSA) Security requirements & Centers for Medicaid Services (CMS) security requirements and the Department of Health & Human Services (DHHS) requirements:

**User Access Control and Information Security**

I agree to:

1. Abide by all laws and regulations regarding information contained within KEES, including regulations defined by HIPAA (Health Insurance Portability and Accountability Act) and other Federal and State laws, policies and procedures.
2. Use the KEES system and any data contained within only for the purpose of determining eligibility for and administration of State of Kansas KEES-managed programs.
3. Use the KEES system only for those specific functions and at the specific locations for which I have been authorized.
4. Protect any and all information contained in KEES to which I have been given access and to handle and safeguard any and all such information in a manner that affords sufficient protection to prevent the unauthorized disclosure of or inadvertent access to such information to unauthorized persons or groups.
5. Protect any and all information available to me through interfaces with other agencies regardless of format (electronic, hard copy, etc.) or venue (State facility, remote office, in transit, etc.).
6. Protect passwords from disclosure or compromise. I will not provide my password to anyone, including system administrators. I will prevent others from obtaining my password via “shoulder surfing.” I will change my password(s) as required and immediately report to my supervisor and the KEES Security Coordinator [KEES.Security@ks.gov](mailto:KEES.Security@ks.gov) if I suspect my password has been compromised.
7. Honor and comply with any and all dissemination restrictions cited by the State of Kansas or sponsoring organizations.
8. Upon request, return all information obtained via KEES that is in my possession or control.
9. Ensure that I have appropriate authorization to install and use software on KEES systems that is properly licensed, approved, and free of malicious code.
10. Wear an identification badge at all times except when they are being used for system access in facilities.
11. Maintain awareness of risks involved with clicking e-mail or text message web links.
12. Collect information from members of the public only as required by my assigned duties and permitted by the Privacy Act of 1974, the paperwork Reduction Act, and other relevant laws.
13. Complete required annual IT Security Awareness & HIPAA Training in accordance with State of Kansas ITEC Policy 7400 & HIPAA CFR 164.308(a)(3) & (5).
14. Promptly report all IT security incidents including any suspected unauthorized disclosures of data to the KEES Helpdesk at (1-877-782-7358).
15. Log off the KEES system; lock my workstation or laptop computer whenever I step away from my work area, even for a short time. I will use a password-protected screensaver. I will terminate system access when I leave for the day.

**User Access Control and Information Security – Continued:**

I agree not to:

1. Use the KEES system, or sensitive information contained within, in any way not intended to assist in the operation of the KEES-managed programs.
2. Use any data contained in KEES to extract information concerning individuals who are neither applicants for nor recipients of benefits under KEES-managed programs.
3. Attempt to access systems I am not authorized to access.
4. Attempt to bypass access control measures.
5. Intentionally interfere with or disrupt the servers, networks or systems connected to KEES.
6. Disobey any requirements, procedures, policies or regulations of which I have been made aware of for networks connected to KEES.
7. Impersonate any person or entity or falsely state or otherwise misrepresent my affiliation with a person or entity.
8. Upload, post, email or otherwise make available any content that I am not authorized to make available under any law or contractual relationship. This Agreement does not release me from my responsibility to comply with applicable laws governing the disclosure of sensitive information.
9. Upload, post, email or otherwise make available any intellectual property or content protected by copyright or other proprietary rights without express permission of the owner of said rights. The burden of determining that any material is not copyright protected rests with the individual user.
10. Upload, post, email or otherwise make available any material which violates in any way upon the rights of others or which is unlawful, threatening, abusive, defamatory, or otherwise objectionable.
11. Upload, post, email or otherwise make available any material that contains software viruses or other computer code or programs designed to interrupt, destroy or limit the functionality of any computer software, hardware or telecommunications equipment.
12. Remove data or equipment from KEES premises without proper authorization.
13. Use sensitive KEES data for private gain or to misrepresent myself or KEES or for any other unauthorized purpose.
14. Store sensitive information in public folders or other insecure physical or electronic storage locations.
15. Intentionally conceal, remove, mutilate, obliterate, falsify, or destroy information stored in the KEES network.
16. Use systems without antivirus software, anti-spyware and personal firewalls, or approved encryption to protect sensitive information stored on recordable media such as laptops, USB drives, or external disks.
17. Perform any of the following activities:
    1. Unethical or illegal conduct;
    2. Sending or posting obscene or offensive material;
    3. Sending or forwarding chain letters, e-mail spam, inappropriate messages, or unapproved newsletters and broadcast messages;
    4. Sending messages supporting prohibited partisan political activity as restricted under the Hatch Act;
    5. Conducting any commercial or for-profit activity;
    6. Using peer-to-peer (P2P) software except for secure tools approved in writing by the KEES CIO to meet business or operational needs;
    7. Creating and/or operating unapproved Web sites or services;
    8. Allowing personal use of KEES resources to adversely affect KEES systems, services, and co-workers (such as using non-trivial amounts of storage space or bandwidth for personal digital photos, music, or video);
    9. Using the Internet or KEES workstation to play games or gamble; and
    10. Posting KEES information to external newsgroups, social media and/other types of third-party website applications, or other public forums without authority, including information which is at odds with departmental missions or positions. This includes any use that could create the perception that the communication was made in my official capacity as a federal government employee, unless I have previously obtained appropriate State of Kansas approval.

**User System Access Monitoring**

I agree to the following:

* I acknowledge that all system access can be monitored in accordance with state and federal law, for purposes including but not limited to network operations, quality control, employee misconduct investigation and in cooperation with any law enforcement investigation.
* I have no expectation of privacy regarding any communications or data transiting or stored within KEES.
* Any communications with or data transiting or stored within KEES may be disclosed for any lawful government purpose.

**User Acknowledgement and Consent**

By signing below, I acknowledge that I have read the terms of use above in their entirety, understand them, accept them and will comply with them. I understand that failure to comply with any of these rules can result in sanctions including verbal or written warning, termination of employment, removal of system access, fines as authorized by contractual agreements and/or applicable state and federal law, and criminal or civil prosecution.

Digital and Electronic signatures are acceptable.

|  |  |
| --- | --- |
| Click here to enter text. | Click here to enter text. |
| **PRINT User Name: First MI Last** | **Email Address** |
| Click here to enter text. | Click here to enter text. |
| **Function/Job Title** | **Phone Number** |
| Click here to enter text. | User is a State Employee  Yes  No |
| **Office/Company** | |
|  | Click here to enter text. |
| **Signature of User** | **Date** |
| Click here to enter text. | Click here to enter text. |
| **PRINT Supervisor Name: First MI Last** | **Email Address** |
| Click here to enter text. | Click here to enter text. |
| **Functional/Job Title** | **Phone Number** |
| Click here to enter text. | |
| **Office/Company** |  |
|  | Click here to enter text. |
| **Signature of Supervisor** | **Date** |

**Remember to attach your training certificates/transcript**

|  |
| --- |
| **Course Title** |
| Security Awareness Training for Information Provided by U.S Social Security Administration |
| HIPPA Awareness Training |
| IT Security Awareness Training |