



Kansas Health Policy Authority Operational Policy

Title: Acceptable Use Policy

Number: POL-IT:2007-02

Effective date: 3-15-07

Date Revised: None

Date of Annual Review: 5-15-08

Authority: POL-EX:2006-01

CATEGORY

Information Technology

SUBJECT

Information Technology Security

BACKGROUND

Kansas Health Policy Authority is responsible for properly protecting State assets. The misuse of government assets violate State ethics practices, may violate other legal requirements, and could have a serious adverse impact on State government. This policy describes the appropriate use of KHPA computer assets, including information technology resources. In applying the acceptable use policy, the use of good business judgment, ethics, and the perception of others will also be considered. This policy applies to all officials, employees, contract labor, and any agents and representatives of KHPA.

Assets refers to all resources owned or controlled by KHPA. The term includes tangible property and intangible property. Assets include, but are not limited to, the following tangible items: offices, facilities, equipment, systems, supplies, financial data, government records, and other machines. Equipment includes, but is not limited to, phones, copiers, fax, and computers. Assets also include intellectual or intangible property such as technologies, ideas, inventions, concepts, business practices and methods, strategies and plans, vendor and employee lists, opportunities, trademarks, internal KHPA information, and the time and talent of KHPA employees.

Personal use means the use of equipment or systems by a KHPA employee for the benefit of an individual, entity or organization rather than for the direct benefit of KHPA.

Personal use includes, but is not limited to, use of assets by an individual for the benefit of or to communicate with family or friends. Personal use also includes, but is not limited to, the use of assets by an individual for the benefit of a charity, athletic, political, religious, or any other entity other than KHPA without prior management authorization.

POLICY STATEMENT

KHPA employees have an obligation to safeguard KHPA assets from loss, misuse, waste, damage, and theft. KHPA assets are intended for use to support and conduct State government business, but KHPA permits limited personal use of its equipment and systems. Personal use of KHPA resources is a limited privilege, not an entitlement. When using KHPA resources for personal use, employees are expected to exercise good judgment and keep personal use to a minimum.

Personal use of KHPA resources is limited to basic office services and systems, such as telephones, photocopiers, facsimile machines, Internet access, and computers. Employees accessing the Internet while on the KHPA network must recognize that Internet sites can pose a threat to their workstation as well as the KHPA network. Employees are to adhere to the following guidelines designed to maintain a secure operating environment.

HIPAA regulations require that physical safeguards be implemented for all workstations that access electronic protected health information (ePHI). The necessary safeguards include taking action to restrict access to only authorized users and restrict the level of access.

Personal use of KHPA resources must conform to the following guidelines. The personal use:

- Must not interfere with work responsibilities.
- Must not interfere with required business communications.
- Must not be used in the support or operation of any business other than that of State government.
- Must not be used in a manner or for a purpose that would reflect unfavorably upon KHPA's reputation, such as use for illegal, unethical, or sexual activities, and gambling or organized wagering.
- Must not result in monetary charges to KHPA such as long-distance calling charges.
- Must not generate inappropriate sounds or images for a work setting
- Must comply with any laws, regulations, and KHPA policies, standards, and guidelines.

Roles and Responsibilities:

- Employees, whether permanent, temporary, or contract labor, are responsible for reading, understanding, and complying with this policy. Additional responsibilities include:
 - Mobile computers and devices must not be left unattended in public locations.
 - Only authorized users are permitted to access device which stores KHPA business information or protected health information.
 - Must not disrupt or disable software update distributions from DISC.

- Must properly reimburse any costs such as paper or long-distance telephone charges associated with appropriate use, if permitted.
- Information Security Officer (ISO)
 - Defines and maintains this policy.
 - Assists supervisors/managers in clearly explaining and enforcing this policy.
 - Assists leaders in investigating violations of this policy.
- Supervisors/Managers
 - Communicate the proper user of KHPA assets based upon business needs.
 - Explain and enforce this policy.
 - Investigate suspected violations of this policy.
- Employees
 - Only authorized workstations may be connected to the KHPA network.
 - Virus protection software and signature files must be maintained at the latest vendor level.
 - Personal firewall software and virus protection must remain active at all times.
 - Screensavers must be enabled to use the screen lock feature for locking workstations.
 - Contact supervisor/manager for direction if in doubt whether a personal use of KHPA assets is acceptable.
 - Ensure that use of KHPA computer assets is ethical, legal, and within policy guidelines.
 - May access the Internet for business research and communication.
 - Will not download, copy, or access copyrighted or patented material that KHPA does not have license or title to, including musical or video recordings.
 - Will not install software including shareware or freeware on any KHPA computer asset without the written approval of the ISO.
 - Will not use Instant Messenger software (i.e. AIM, MSN Messenger, etc.) without the approval of their manager.
 - Will report suspected violations of this policy.
 - Unattended workstations must be physically and logically locked. Upon the employee's return, re-authentication must occur for the employee to access KHPA systems and data.
 - Must not open e-mails or e-mail attachments from unknown sources.

Violations of these requirements are addressed in the sanction policy.

Where not prohibited by law or regulation, KHPA reserves the right to monitor the use and contents of its resources and systems including, but not limited to, computing and telecommunications systems and access to and use of equipment and facilities. KHPA employees shall have no expectation of privacy using KHPA resources, whether for business or personal use. KHPA may inspect KHPA's records and systems, including electronic systems, and inspect the information contained in them with or without

advance notice to employees, even when information is stored under an individual's personal identification code or password.

SPONSOR/CONTACT
Chief Operations Officer