Unified Government Human Resources Guide

Effective 04-01-05

RESPONSIBLE USE OF INFORMATION TECHNOLOGY

I. General: It is the policy of Unified Government that information technology (IT) resources provided to employees be used for the benefit of the Unified Government and that they be used productively.

II. Policy

A. Information technology resources, both hardware and software, which include, but are not limited to, computers, computer systems, printers, networks, software, electronic mail (e-mail), Internet and World Wide Web access, facsimile, voice mail, telephones, cell phones and future technologies are business tools and are to be used to promote the efficient conduct of Unified Government business.

B. All IT resources and all messages composed, sent or received using IT are and remain the property of the Unified Government. Employees do not have any right to privacy while using any of the Unified Government IT resources, and information contained on Unified Government IT hardware and software should not be considered confidential.

C. It is the responsibility of Unified Government employees to use IT in an efficient, ethical and lawful manner.

D. The Unified Government may monitor, audit, intercept, access, review and disclose all use of IT resources and all communications created, received or sent using IT resources. All employees of the Unified Government shall sign a consent form attached to this policy authorizing monitoring and stating that they have read and received a copy of this policy.

E. Supervisors are responsible for instructing employees on the proper use of Unified Government IT for both internal and external uses.

F. All employees who are given access to Unified Government IT shall respect the intended use of access privileges established for them. The Department of Technical Services (DOTS) can and will remove access when privileges are viewed as being abused.

1. The level of access to a department's IT resources shall be determined by the DOTS.

2. Requests for changes of access privileges shall be made in writing from a person designated to authorize the change and submitted to the DOTS.

3. Efforts to defeat the security systems of Unified Government IT to gain access without authorization, or to gain access for other than their intended purposes, are prohibited and punishable. (See 7.1 Rules and Discipline, Rule 39)

G. All employees who are given access to Unified Government IT shall not seek, provide, modify information in, or obtain copies of files, programs or passwords belonging to other IT users or departments without the written permission of those users or departments.

H. All employees who are given access to Unified Government IT shall not search through non-public directories, libraries or any other storage media to find unauthorized information.

I. The use of IT hardware and software is reserved for the conduct of Unified Government business. Incidental and occasional personal use is permitted as long as such use does not:

1. interfere with existing rules or policies pertaining to the Unified Government;
2. disrupt or distract the conduct of Unified Government business (e.g., due to volume or frequency);
3. involve a for-profit personal business activity;
4. have the potential to harm the Unified Government, or involve illegal activities;
5. solicit for commercial ventures, religious or political causes, outside organizations, or other non-job-related solicitations; or
6. consist of mass e-mailings of a non-business nature.

Employees must reimburse the Unified Government for any costs incurred by the Unified Government for an employee's personal use of any Unified Government IT resources.

J. Fraudulent, harassing, threatening, discriminatory, sexually explicit or obscene messages or materials shall not to be created, transmitted, printed, requested or stored using any Unified Government IT hardware and software.

K. Employees are not permitted to use encryption-coding devices or schemes on any Unified Government hardware and software without authorization from or direction by their supervisors. Any employee authorized to use encryption-coding devices or schemes must provide all codes or keys to his supervisor in a sealed envelope which shall be maintained in a secure environment. Any employee directed to use particular encryption-coding devices or schemes by his supervisor shall use it as directed and for its intended purpose.

L. Employees are responsible for protecting their own passwords which gives them access to all Unified Government hardware and software.

1. Sharing user IDs and passwords is prohibited. Employees will be held responsible for misuse that occurs through such unauthorized access.
2. Supervisors at any level shall not require the employee to share his/her password. Information that is generally shared within a department or unit may be stored on a shared space. Information that is password protected must be obtained in an employee's absence by an authorized person contacting the DOTS Help Desk.

M. All employees who are given access to Unified Government hardware and software shall not download software from the Internet or load software onto any Unified Government computer or server without the knowledge and specific approval of the DOTS. Software includes but is not limited to the following: department business software, screen savers, desktop patterns, utilities, word processors, games or any other commercial, shareware or freeware software. Introducing or using software designed to corrupt or destroy Unified Government's computer systems with viruses or cause other harmful effects is obviously prohibited. To prevent the accidental introduction of a virus or similar mechanism, software or malfunctions, such as worms, employees are required to work with the DOTS to use anti-virus software when introducing or downloading software or digital data or information.

N. The Unified Government has an obligation to prevent the use of "pirated" software or other use inconsistent with copyright law. Copying copy-righted software to a Unified Government computer is illegal and in violation of this policy.

O. All software loaded on a Unified Government computer must be legally licensed for that computer. This means a specific software license must be identifiable for all software loaded on each computer.

P. All employees who are given access to Unified Government hardware and software shall not use the equipment for radio, television, streaming audio or streaming video reception over the Internet except when specifically authorized by the DOTS.

Q. E-mail and voice mail communications are Unified Government records and must be treated as such. Employees shall follow all laws and Unified Government policies, including the Kansas Open Records Act and the Records Management Policy, and shall not disclose information in violation of any restrictions on such disclosure. Privileged electronic communications with attorneys should be labeled and treated as such. Employees shall not destroy any e-mail or voice mail communications which the Legal Department has instructed them to preserve.

R. Any employee who discovers a violation of this policy is to notify his supervisor and the DOTS.

S. Supervisors shall review all reports of violations of this policy and take the appropriate action.

T. Any employee who violates this policy or uses any hardware and/or software for improper purposes shall be subject to discipline, up to and including discharge.

RELATED FORM(S): Consent and Acknowledgment of Receipt form