Department of Administration
Information Technology
Security Policy

An Employee Guide to Using Technology at Work

Developed by
The Department of Administration
Security Council

TABLE OF CONTENTS

1. Introduction

The purpose of the Department of Administration *Information Technology Security Policy Guide for Employees* is to explain your role in protecting and supporting the information technology systems used in the Department of Administration.

Information is a State of Kansas asset requiring protection equal to its value. Measures must be taken by each of us to protect information from unauthorized modification, destruction, or disclosure, whether accidental or intentional, as well as to assure its authenticity, integrity, availability and confidentiality.

A. The Department of Administration Security Council

The Security Council is a group of employees representing all Divisions within the Department of Administration. Besides developing policy manuals, the Security Council reviews project plans that include information resources, responds to security concerns of employees and assists in the planning and implementation of security policies within the Department of Administration. In Appendix A you will find a list of Security Council members, their e-mail addresses and their phone numbers.

B. Security Acknowledgement Form

A Security Acknowledgement Form is located in Appendix B of this document. You are responsible for following the policies contained in this document, signing this document and returning it to your supervisor. Since information technology changes quickly, the Security Council requires that you read this policy and sign the form annually.

2. Your Responsibility

A. Security

When you use e-mail and the *Internet* at work you should be aware that these systems represent potentially significant security risks for the State of Kansas communications networks. While the Security Council believes that the state networks are basically secure from outside intrusion, you must follow responsible computing to protect the information and systems you use in your job.

One of the most serious dangers the State of Kansas network faces is from employees themselves. Employees have the advantage of having logons and passwords that the outside "hacker" does not have. If this information is shared with unauthorized users, or the employee uses the information to gain access to systems and information they are not authorized to use, they have placed the State of Kansas networks and information systems in serious danger.

You may not use State of Kansas facilities and connections to make unauthorized connections to, break in to, or adversely affect the performance of other computer systems on the network. You should not "test the doors" or "probe" security mechanisms at either the Department of Administration or other Internet sites unless you have first obtained permission from the Department of Administration Security Council.

You are also required to use all available methods to prevent unauthorized connections to State of Kansas networks. This includes taking such precautions as enabling approved virus protection software when connected to the *Internet* or receiving e-mails. This also includes prohibiting unauthorized people from accessing the State of Kansas systems through your user logon or password, using password protected screen savers when the work area is unsupervised and taking any other prudent security precautions.

If you do suspect that sensitive information has been lost or intercepted by unauthorized parties you are required to notify your supervisor immediately.

B. Privacy

The Department of Administration cannot guarantee the privacy of electronic communications for two reasons. First, electronic communications, especially e-mail and the *Internet* are not private by nature. Second, the Department of Administration routinely monitors some types of communications by employees that use E-mail and the *Internet*. While passwords protect confidentiality to some extent, e-mail and *Internet* messages and attachments can be read, altered or deleted by unknown parties without your permission. You should be aware that even when e-mail messages or *Internet* files are deleted or erased it is still possible to recreate the original message or file.

C. E-mail and *Internet* Use:

The following is the message displayed on your computer each day as you log on:

> "WARNING: This technology is provided for official state business only. Inappropriate use (including, but not limited to the e-mail system and the Internet), may result in monitoring. Inappropriate use may result in the proposal of disciplinary action up to and including termination of employment in accordance with K.S. A. 78-2949(a)(3) and other appropriate statutes. System-wide checks will be conducted on a periodic basis to assure that pornographic sites are not being utilized. Internet/e-mail activity of this highly inappropriate nature that is substantiated will result in the proposal of termination of employment.

D. Voice Mail Use

Voice mail is used to receive and retrieve messages when employees are unable to answer their telephones. The voice mail system provides security protection through the use of the user security codes; however, there is a potential for unauthorized message receiving or fraudulent calling.

You can protect yourself from fraudulent use of voice mail by using good security codes and changing them often (at least every 30 days). You can also make sure your office notifies the voice mail administrator in DISC when a coworker leaves for another employer or agency.

E. Passwords

Passwords are pre-stored combinations of characters used by the host computer to authenticate the identity of an individual user. Passwords are only effective if they remain confidential. Depending on the number of systems you use, you may have one or several passwords.

When employees leave or transfer to another Division within the Department of Administration, their immediate supervisor should notify the technical liaison in their Division. The technical liaison will notify DISC Customer Support who will contact the security staff for all systems so they can remove or modify the security profile for that user.

Most Department of Administration systems require that the user enter a password change every thirty days. For those systems that do not require a password change, users should change their password frequently. Some suggestions when creating passwords:

Don't use names of persons, places or things that can be closely identified with you (i.e., your spouse's name, children's names or pets).

Don't use your userid as your password.

Don't share your password with anyone other than an authorized PC support staff member.

Don't write your password down and leave it in an obvious location.

Do use passwords with a minimum of eight characters and include at least one uppercase and one lowercase letter, one number, and one special character.

Do use passwords only once

Do change passwords frequently

F. Virus Protection Software

Virus protection software is installed on all Department of Administration personal computers connected to State of Kansas networks and should be enabled when you logon. If it is enabled, you'll see the icon for it on your toolbar. Virus protection software should never be disabled, since you may be receiving files anytime you use your e-mail or log on to the *Internet*. If you are a home PC user and bring files to work, make sure you are using updated virus protection software on your home PC as well.

G. Encryption

Encryption is the process of character substitution or transposition in a sequence determined by an encryption formula. Data encryption techniques are used to control access to information, protect the transaction, disguise data during transmission and verify or authenticate the users of the system.

Do you need to encrypt the data you send? The answer may be yes, depending on what you are transmitting and how you are sending it. If you are sending your information across public networks (the *Internet* and external addresses in E-mail), then here are some questions you can ask to determine if your data should be encrypted:

Could interception of the information result in:

- Loss of state funds
- Violation of individual expectations of privacy
- Violation of state or federal law
- Civil liability for the agency
- Compromise any legal investigation
- Cause a loss of business to the affected party
- Give an undue advantage to one party in competitive business relations.

If you need information on how to encrypt a file you are sending please contact DISC Customer Support. They can assist you.

H. Remote Access

A few Department of Administration users have direct (other than *Internet*) dial-up access from home via a modem. This poses a high risk of possible intrusion to the State of Kansas network. State of Kansas networked systems should never be accessed without approval and authorization from the Department of Administration. Employees with direct dial access have a responsibility to protect State of Kansas networked systems with appropriate virus protection software installed on their home PC's and using only authorized procedures for dial-up. Any equipment (desktops, laptops, PDA's used for direct access to the network should not be used to attach to any other network. This means that you should not directly access the State network with any machine that is also used for direct access to an internet service provider. Home machines that have been used for direct access to both the State network and an internet service provider have been a common source of virus infection.

I. Software Installation and De-Installation

You may use Department of Administration approved software on your computer. All software must be owned or properly licensed to the Department of Administration.

When computer equipment and software is de-installed and ready to be surplused, notify the technical liaison in your Division. They will purge the machine. You should also notify your inventory control officer to ensure that it is removed from the inventory.

J. How to Protect the Information You Have

Like all communications conducted on behalf of the State of Kansas, you must use good judgement in *Internet* and e-mail use. Like any memo you write, each use of the *Internet* and each e-mail must be able to withstand public scrutiny without embarrassment to the Department of Administration or the State of Kansas.

Users should exercise good judgment in guarding the information they access. Just as you would not think of leaving valuables unattended in a public area, you must protect both the paper and electronic information in your office. This includes restricting physical access to computers, paper files, FAX machines and printers in your area, following guidelines on encrypting sensitive information, using a screen saver with a password protector and following the guidelines on password creation and use. Besides your computer and files, your printer and FAX machine may produce sensitive information. Make sure access is restricted to printers and FAX machines in your office and immediately remove any sensitive documents coming from a printer or FAX. If there are files in your office that contain confidential information, make sure they are kept locked and restrict access to that area.

The information you work with should also be protected from accidental destruction. Store electronic information on Division servers rather than individual personal computers and make frequent backups or copies of important files and store in a secure location. It is a good practice to periodically make archival copies of your data to CD or DVD and remove infrequently accessed files from the servers to free up disk space.

K. Attaching Equipment to the State Network

Any user equipment, (whether State owned, vendor owned, or employee owned) that will be used to attach to the State network must be authorized by the Division management in which it will be used and approved by DISC Customer Support prior to attachment.

Equipment that is periodically attached to the network, including Personal Digital Assistants, (Blackberry, iPaq, MindSpring, etc.) must be updated for virus protection and security updates, as applicable, before it may be connected to the network. Contact DISC Customer Support to coordinate updates for this class of equipment.

3. Security Incident Reporting

You must report any suspected breach of security to your immediate supervisor as soon as you discover it. Your supervisor is then required to notify the PC support staff in their Division and/or their Security Council representative. A breach of security might include computer fraud, a computer virus, or unauthorized access to State networks.

Appendix A: Department of Administration Security Council Members

DISC-BAS morey.sullivan@da.state.ks.us	Morey Sullivan	296-3343
DISC-BIS joe.hennes@da.state.ks.us	Joe Hennes	296-3463
DISC-BOCS jerry.merryman@da.state.ks.us	Jerry Merryman, Chair	296-0999
DISC-BOT dave.timpany@da.state.ks.us	Dave Timpany	296-6150
DISC-BDAS tim.griffin@da.state.ks.us	Tim Griffin	296-8565
DISC ITS duncan.friend@da.state.ks.us	Duncan Friend	296-3463
DISC-BOT jim.logan@da.state.ks.us	Jim Logan	296-0292
A&R daryl.daniels@da.state.ks.us	Daryl Daniels	296-2930
DPS jan.cavalieri@da.state.ks.us	Jan Cavalieri	296-4743
Div of Budget jeff.arpin@da.state.ks.us	Jeff Arpin	296-2436
Div of Facilities Mgmt kerry.ranabarger@da.state.ks.us	Kerry Ranabarger	296-1318
D of A Hearings john.mendoza@da.state.ks.us	John Mendoza	296-2485
D of A Legal scott.gates@da.state.ks.us	Scott Gates	296-6000

Appendix B: Security Acknowledgement

Employee Agreement to Comply With
Employee's Guide to Using Technology at Work

The Department of Administration is devoted to information security and employs specialists to maintain security. However, it is the responsibility of users to comply with all information security policies and procedures.

By signature below, the employee hereby acknowledges and agrees to the following:

1. Employee is a Department of Administration employee in possession of Department of Administration information resources;

2. Employee shall protect these information resources from unauthorized activities including disclosure, modification, deletion, and usage.

3. Employee has read and agrees to abide by the "Employees Guide to Using Technology at Work."

4. Employee agrees to discuss with a supervisor any policies or procedures not understood.

5. Employee shall abide by the policies described as a condition of continued employment.

6. Employee understands that any employee found to violate these policies is subject to disciplinary action, including but not limited to, privilege revocation and/or termination of employment.

7. Access to Department of Administration information systems is a privilege, which may be changed or revoked at the discretion of Department of Administration management.

8. Access to Department of Administration information systems automatically terminates upon departure from Department of Administration.

9. Employee shall promptly report violations of these policies to the chair of the Department of Administration Security Council through the Employee's Division Council representative.

10. This document may be amended from time to time. The Department of Administration will notify employees of amendments. Employee will keep abreast of amendments to the "Employees Guide to Using Technology at Work," as made available by hard copy or on-line.

ACKNOWLEDGMENT: EMPLOYEES GUIDE TO USING TECHNOLOGY AT WORK

_____ _____

User's signature Date Witness Date

_____

User's name in block capital letters