

SHARP SECURITY GUIDELINES

Section I. Operator Identification Code Assignment

Agency Responsibilities:

1. The Agency will ensure that only the appropriate employee(s) are allowed access to the SHARP system.
2. The Agency will ensure that only the panels necessary for completion of job duties are requested for each selected employee.
3. The Agency will ensure that each employee requesting access to SHARP completes the appropriate computer based training (CBT) module(s).
4. The Agency agrees to be responsible for the proper management of the SHARP operator identification codes (Operator IDs) and passwords assigned to employees in their agency.
5. The Agency will designate one or more SHARP Security Administrators whose signature(s) will be accepted as agency approval for the requested SHARP access. Electronic mail transmissions received from such designee will be considered an electronic signature. All communication regarding SHARP security will go to the SHARP Security Administrator(s). If a SHARP Security Administrator is not designated, the agency Human Resource Manager will be the default SHARP Security Administrator. The name, work address, work phone, and E-mail address of each SHARP Security Administrator should be provided to:

Kristine Scott
Division of Personnel Services
900 SW Jackson, Room 951-S
Topeka, Kansas 66612-1251
kristine.scott@state.ks.us

- 5a) The Agency SHARP Security Administrator will become familiar with the Introduction to SHARP Computer Based Training module, "Test Activities/Security Signon" chapter and will provide this information to new users and their supervisors.
- 5b) The Agency SHARP Security Administrator will notify the Division of Personnel Services in a timely manner when SHARP Operator IDs are to be removed from the system. Examples of such situations: employee termination from the agency or new duties that do not require access to SHARP.
- 5c) The Agency SHARP Security Administrator will promptly review the quarterly security report provided by the Department of Administration to ensure that all access levels are still appropriate for each employee.

SHARP SECURITY GUIDELINES

Section I. Operator Identification Code Assignment (cont.)

Department of Administration Responsibilities:

1. The Department of Administration will provide central oversight of SHARP Security.
2. The Department of Administration will notify the Agency in a timely manner when noticeable changes will be made to the PeopleSoft software. This may include one or more of the following: Formal meetings, memos, electronic mail messages, SHARPSooter newsletter, or updated training materials.
3. The Department of Administration will develop and provide computer based or web based training modules. Each module shall include a method for testing the trainee's understanding of appropriate data entry methods.
4. The Department of Administration will review the test results of each trainee to determine if further training is needed before SHARP access is granted.
5. The Department of Administration will review the signature on each security request to ensure Agency approval of SHARP access.
6. The Department of Administration will provide a quarterly report to each Agency SHARP Security Administrator listing each employee Operator ID and the corresponding windows, panels and departments that said Operator ID may access.

Section II. Password Protection

Agency Responsibilities:

1. The Agency will ensure that SHARP Operator IDs and passwords are not shared among SHARP users. Each employee shall use only the Operator ID and password specifically assigned to their Employee ID. Any actions performed in the SHARP system will be the responsibility of the person assigned to that Operator ID.
2. The Agency will notify each SHARP user that the password should be changed once every 30 days.
3. The Agency SHARP Security Administrator will review the quarterly report provided by the Department of Administration to ensure that all SHARP users have changed their password in the last 30 days.
4. The Agency SHARP Security Administrator will ensure that SHARP users who do not change their password within a 90-day period are warned that they will lose their user privileges.

SHARP SECURITY GUIDELINES

Section II. Password Protection (cont.)

Department of Administration Responsibilities:

1. The Department of Administration will include the date of last password change for each Operator ID on the quarterly security report.
2. The Department of Administration will attempt to provide notice to the Agency SHARP Security Administrator before an Operator ID is terminated due to inactivity.

Sanctions:

1. If a SHARP user does not change their password within a consecutive 90-day period, their Operator ID will be considered inactive and will be removed from the SHARP system. The Agency SHARP Security Administrator may submit an Agency Security Selection Form to reinstate an inactivated Operator ID.

Attachment 1: Agency Security Selection Form

Attachment 3: Statewide Security Selection Form

Attachment 4: Security Guidelines Flier for Users

Attachment 5: Password Change Reminder Flier for Users

Effective Date: March 17, 2000