Division of Information Technologies
Technology Services Section

Standard Operating Procedure #8808

Title: System Security and Use
(Formerly: Misuse of the Data Processing System)

Originator(s): Technology Services **Reviewed:** March 21, 2005

Date: October 1, 1984

Revised: March 21, 2005

8808.1 GENERAL

The purpose of this SOP is to implement the Executive Order dated July, 1978, and the former Division of Automated Data Processing (DADP) Policy Statement regarding access to public records through the use of computer technology. Additionally, it is intended to prescribe the policies and procedures for governing the way that DoIT uses the software "Top Secret" for fulfilling DoIT/CSS responsibility as custodian of our user's computing resources.

A copy of the Executive Order and DADP Policy Statement are attached to this SOP as Exhibits A and B.

Implementation of this SOP is a shared responsibility between DoIT/CSS and it's users. The applicable policies and procedures are outlined below.

8808.2 POLICY

1. It is the policy of this agency that the Executive Order dated July 1, 1978, and the former Division of ADP Policy Statement regarding access of public records through the use of computer technology be strictly adhered to. Some excerpts are quoted below.

2. It is the public policy of this State that all public records shall be open for inspection by any person at reasonable times, except as provided in Part 2 of Article 72 of Title 24, C.R.S. 1973 as amended, or as otherwise specifically provided by law.

3. The release of any information to the public, supplied through automated processes, shall not take place unless the following events have transpired:

a. Written requisition delineating the desired information records, or data must be received by the official custodian.

b. The official custodian must determine if the requested information, record, or data constitutes public record and its disclosure is within the law.

4. The DoIT, acting as a service bureau, has a fiduciary obligation to provide its customers with assurance that all data resulting from the activities of an agency using DoIT's computing and networking facilities equipment is considered private data of that agency. Use and dissemination of this data by computer center personnel is absolutely prohibited without proper authority being given. The appropriate Executive Director or the official custodian must provide written authority to the computer facility director prior to any data within the facility director's jurisdiction being released in any manner to any individual, government agency, or private concern. It is the facility director's responsibility to adopt adequate safeguards to protect data stored within the facility.

5. The DoIT has a business need, based on customer expectations, to take reasonable steps to ensure that unauthorized access to DoIT's owned resources does not compromise the integrity or function of the services provided by the DoIT.

6. The DoIT's policy is that each DoIT staff member have access to only those resources necessary and appropriate to that staff member's job duties. The data processing systems shall be used only for official State business. Use of the data processing system for non-business activities is not allowed. This includes personal business (i.e., letters, games, etc.), access of the system software without proper consent, abusive language (i.e., messages), and abuse of the operating system including hardware.

7. The TOP SECRET software product is the product selected as the vehicle to carry out the DoIT/CSS responsibility with respect to securing resources and controlling access on one system. Owners of data and program resources will control the extent of security required and those persons who have access and the extent of the access or to resources which transcend the individual technical support group assignments.

8808.3 PROCEDURES and METHODS

1. Accessor IDs (ACID) will be assigned by the Service Center for all DoIT/CSS employees; and, at their request, for those agencies for which DoIT/CSS acts as their TOP SECRET agent. For those agencies that have an appointed agency security administrator (ASA), that administrator will assign ACIDs for

that agency's employees.

2. Securing of customer-owned resources(data, programs) will be performed by the owning agency administrator.

3. A Statement of Compliance will be required for each ACID assigned by the DoIT/CSS Service Center. When an ACID is assigned, the Service Center or ASA will assure that a statement is signed and placed on file. ASAs will maintain the files of statements pertaining to their agencies, and the Service Center will obtain signatures and maintain the files of statements for DoIT/CSS employees and agencies for which they act as agent.

4. ACIDs will be purged when they are unused for six months. A list will be developed on the first of the month indicating those ACIDs that have not been used for six months and have been deleted. The list will be available on-line for ASAs' review.

5. When an ACID is suspended, a password elapsed or forgotten, or other problem, action to correct the situation will be taken by ASAs for those agencies having one appointed, and by the Service Center for DoIT/CSS employees and agencies for which DoiT/CSS acts as agent. Only in emergency situations will action be taken by the Service Center for agencies with appointed ASAs and only when the ASA or designated backup is not available and agency approval is granted. The Service Center will require the caller to state their two personal safe 'words' or phrases. (we no longer require specific personal information) We will <u>not</u> reset ID's unless the customer can identify these two items. This implies the items exist in the first place. When taking action for DoIT/CSS employees or agencies for which DoIT/CSS acts as agent the safe 'words' will be verified against the Statement of Compliance.

6. Just as each employee having an ACID is required to sign a Statement of Compliance, each ASA is required to sign an additional statement acknowledging the duties and responsibility of the position. Copies of the ASA statement and Statement of Compliance are attached to this SOP as EXHIBIT C and D.

7. Every effort will be made to assure that each ACID has a person identified with it. In cases where this is not reasonable or possible, an office manager or other manager will sign a Statement of Compliance for the ACID and assume the responsibility for actions taken under this ACID.

8. All software products are controlled by groups of technical support staff. Each group is responsible for a set of software products. The members of each group, and the software products for which the group is responsible is determined and maintained by the Technology Services Manager.

a. Each group is associated with a TSS profile, which grants full access to the resources used exclusively by the software products for which each group is responsible.

b. A second TSS profile is used to contain authorizations, which are common to the technical support area as a whole. This profile allows read-access to resources, which are associated with multiple software products, or to resources, which transcend the individual technical support group assignments.

c. A third TSS profile is used to contain resource authorizations for customer-owned resources. This profile is common to all technical support staff members and thereby facilitates the distribution of duties, which require access to customer-owned resources. Non-temporary resource authorizations made to a specific technical support staff member's User-Id will be moved to this common profile. The owning customer retains the ability to continue or remove the authorization from this common profile.

8808.4 EMERGENCY EXCEPTION HANDLING

1. A provision to override any resource access specification is required. The ability to override resource access specifications is provided to allow the performance of job duties, which require access to otherwise inaccessible resources when access cannot be obtained through normal procedures. This provision is used only when absolutely necessary for continued operation of software vital to the computer center's operation.

2. The use of this provision is monitored by the DoIT central security administrator and security officer. Inappropriate use of this provision by technical support staff is grounds for disciplinary action up to and including termination and/or legal remedies as provided for by local, state, and federal law.

8808.5 RESPONSIBILITIES

DoIT/CSS SECURITY ADMINISTRATOR

a. Administration of the security system.

b. Assist in the investigation and resolution of attempted violations, as requested.

c. Assuring that signed Security Administrator Authorization forms and signed Statements of Compliance from all appropriate employees are

obtained.

d. Assure appropriate approvals for any non-owner access to data.

e. Point of contact within DoIT/CSS for security matters.

AGENCY SECURITY ADMINISTRATORS

a. Enforcing security requirements is within the agency.

b. Securing agency data and assigning access authorizations.

c. Obtaining and maintaining files of annual Statements of Compliance from all agency employees having ACIDs at DoIT/CSS.

d. Point of contact within the agency on security issues.

e. Research and resolution of violations.

1. DoIT TECHNICAL MANAGERS AND SUPERVISORS

a. DoIT managers and supervisors must immediately notify the DoIT/CSS Security Administrator in writing when any subordinates in their reporting structure changes duties or responsibilities resulting in computer security permission changes. The manager or supervisor will review the employee's current access privileges with the DoIT managers and supervisors and must immediately notify the DoIT/CSS Security Administrator to document and make any access changes necessitated by the change in duties or responsibilities. The DoIT/CSS Security Administrator will then prepare a report for management documenting the changes or noting that no changes were necessary.

8808.6 PROCESSING ATTEMPTED SECURITY VIOLATIONS

When a breach of security is detected which involves repeated non-authorized attempt at or access to data, the following actions will be taken:

1. The ACID is revoked. It can only be reinstated by the DoIT/CSS Security Administration Staff.

2. The administrator responsible for the violating ACID will be asked to provide an explanation for the attempted access and those persons who have access and the extent of the access.

2. If the explanation is satisfactory to the ASA responsible for the resource, the violating ACID will be reinstated and the incident closed.

4. If the explanation is unsatisfactory to the ASA responsible for the resource, the following actions will be taken.

    a. A memo is sent to the Executive Director of the department in which the User is employed detailing the incident and requesting an explanation.

    b. A memo is sent to the Executive Director of the department responsible for the secured resource indicating that an attempt was made to gain access and indicating that the ACID has been revoked and will not be reinstated without a satisfactory explanation, which will be shared with them.

    c. When the explanation is received from the offending department's Executive Director, it will be the joint decision of the CIO of DoIT/CSS and affected Executive Director whether to reinstate the ACID. Consideration will be given to the opinion of the department responsible for the secured resource.

    d. If no explanation is provided or an unsatisfactory explanation is given, the incident may be referred to the Attorney General for actions they deem necessary.

    e. Upon final determination, memos will be sent to the interested parties indicating actions taken.

8808.7 PERIODIC REVIEW OF MAINFRAME ACID

1. Regardless of other intervening changes identified in this SOP, ACIDs must be reviewed at least yearly following the methodology as included below.

2. DoIT Mainframe Top Secret ACIDs will be reviewed after any of the following changes take place to DoIT personnel:

    a. Job Duties Change
    b. Team Membership Changes
    c. Job Position Changes

3. A DoIT Personnel Administrator and the involved employee’s manager must verify the job descriptions and assure that job duties necessitate any computer security permissions granted.

4. The following methodology will be employed during the verification process of ACIDs after any of the above changes have taken place:

a. List the ACID and all of its profiles to print.
b. Comparison of the ACID to other team member ACIDs to verify any obvious differences (as a litmus test).
c. Discuss additional permits or revocations of resources to be applied to the ACID with direct supervisor. Focus on team job responsibilities as well as individual job responsibilities.
d. Be mindful of the shared duties that backup personnel must assume.

APPROVED:

_____
Guy Mellor
Deputy Director

COLORADO DEPARTMENT OF PERSONNEL AND ADMINISTRATION
DIVISION OF INFORMATION TECHNOLOGIES
STATEMENT OF COMPLIANCE FOR
COMPUTER USAGE AND DATA SECURITY

It is the policy of the Department of Personnel and Administration's (DPA), Division of Information Technologies (DoIT), that the Executive Order dated July 1, 1978 and the former Division of ADP Policy Statement regarding access of public records through the use of computer technology be strictly followed. An excerpt from these documents can be found below. Please review the paragraphs and indicate your understanding and acceptance by signature. If anything is unclear, or you wish to review the complete documents, please contact your security administrator or the DPA/DoIT Service Center.

It is the public policy of this State that all public records shall be open for inspection by any person at reasonable times, except as provided in Part 2 of Article 72 of Title 24, C.R.S. amended, or as otherwise specifically provided by law.

The release of any information to the public, supplied through automated processes, shall not take place unless the following events have transpired:

- Written requisition delineating the desired information, records, or data must be received by the official custodian.
- The official custodian must determine if the requested information, record, or data constitutes public record and its disclosure is within the law.
- All data resulting from the activities of an agency using DPA/DoIT (formerly CITS/CSS) equipment is considered private data of that agency. Use and dissemination of this data by computer center personnel is absolutely prohibited without proper authority being given. The appropriate Executive Director or the official custodian must provide written authority to the computer facility's manager prior to any data within the facility manager's jurisdiction being released in any manner to any individual, government agency, or private concern. It is the facility manager's responsibility to adopt adequate safeguards to protect data stored within the facility.

The data processing system shall be used only for official State business. Use of the data processing system for non-business activities is not allowed. This includes personal business (i.e. letters, games, etc.), access of the system software without proper consent, abusive language (i.e. messages), and abuse of the operating system including hardware.

- Accessing, or attempts to access data files or programs, which you are not authorized to use, is a security violation. Therefore, do not "browse" or otherwise use files or programs that aren't yours or that you do not have the owner's permission to use.
- Do not sabotage data or programs.
- Do not illegally copy or use illegal software on State computers whether it was originally purchased by the State or is your own personal purchase. All users must comply with the licensing provisions of all software including paying for "shareware" types of software beyond their trial dates.

_____ _____

Name (Please print)

_____ _____

Signature Date

Exhibit C

COLORADO INFORMATION TECHNOLOGY SERVICES
COMPUTING SERVICES SECTION

AGENCY SECURITY ADMINISTATOR'S ADDITIONAL STATEMENT OF COMPLIANCE

The designated Agency Security Administrator (ASA) is an integral part of the security system at the Colorado Information Technology Services, Computing Services Section (DOIT/CSS). The ASA is vested with significant powers and responsibilities. In addition to having signed a DOIT/CSS Statement of Compliance, an ASA is required to sign this Statement of Compliance for Agency Security Administrator. Carefully read the responsibilities defined below. Indicate your understanding and acceptance of these additional requirements with your signature.

RESPONSIBILITIES

- Enforcing security requirements within the agency.
- Securing agency data and assigning access authorizations.
- Obtaining and retaining, on file, Statements of Compliance from all agency employees having access IDs to DOIT/CSS.
- Point of contact within the agency on security matters.
- Participation in research and resolution of violations.

I have read, understand and accept these responsibilities.

Name (Please print)	User ID
Agency	
Signature	Date

Exhibit D