

REGIONAL OFFICE PREPARATION

BACKGROUND: Access to computer resources should be controlled to protect against unauthorized use, damage, loss, or modifications. Proper access controls assist in the prevention or detection of deliberate or accidental errors caused by improper use or manipulation of data files, unauthorized or incorrect use of computer programs, and/or improper use of computer resources.

Access controls are designed to limit access to documentation, files, and programs. A weakness in or lack of such controls increases the opportunity for unauthorized modification to files and programs, as well as misuse of the computer hardware. Weaknesses in documentation and/or controls over machine use may be compensated by other strong IT controls. However, weaknesses in systems software, program, and data security significantly decrease the integrity of the system. Weaknesses in this area must be considered in the evaluation of application controls. Production programs (source and object code) and job control instructions are kept in a restricted area - using secure authentication methods to gain access. Programmers and other unauthorized personnel need to be expressly prohibited from adding, replacing, or deleting production programs. The updating of the production program storage area should be monitored through the use of a report detailing all updates to the production program storage area, and a review of the programs in the production storage area. Someone should be specifically assigned this monitoring responsibility.

Production data files also need to be kept in restricted areas. Like production programs, programmers and unauthorized users should be expressly prohibited from updating or deleting production data files. Formal procedures should be in place to limit access to confidential data to authorized persons only.

PREPARATION ACTIONS:

Request and review written policies for security over access to automated resources typically address guidelines and responsibilities in the following areas:

- access to program documentation
- access to system software
- access to program and job control instructions
- access to data files
- access to applications
- passwords
- investigation of access violations

Set up data center tour and interviews. Suggested interviewees (can be part of data center tour, if applicable):

- A. Documentation Librarian
- B. System Programming Manager
- C. Applications Programming Manager
- D. Director of Information Systems
- E. Data Base Administrator

Obtain and review copies of the automated logs or journals that record/monitor access to the following:

- program documentation
- systems software
- production programs and job control language
- production data files
- critical application systems
- password tables

Obtain copies of the following system documentation:

- Database schema
- System flowcharts
- Record layouts
- Report formats
- Program flowcharts
- Trans flow diagram
- Control documentation procedures
- Backup procedures
- Disaster Recovery Plan

ON-SITE ACTIONS

1. Observe the storage location of documentation if it is kept in printed form or determine how access to on-line documentation is restricted. Determine if the documentation is adequately secured.

2. Determine if checked out documentation is properly logged and can be located.

3. Determine if the methods used to limit access to systems software to authorized persons are adequate.

4. Determine if checked out documentation is properly logged and if it can be located.

5. Test to see that access to systems software is limited by terminal address.

6. Determine if passwords and utilities that affect program access are adequately controlled. Also determine if controls are adequate to limit access to only those who need it to do their jobs.

7. Determine if programs not in the production library are adequately restricted from processing against data files and if controls are adequate to restrict access to data files to only authorized persons.

8. Determine who has access to confidential data. Verify with the owner of the data that these persons have authorization to access this data.

9. Test to see that access to applications, data, or entry and update of transactions is limited by terminal address and hours of operation.

10. For employees that have requested that their addresses and phone numbers not be disclosed, determine if this information is adequately protected from disclosure.

11. Determine if controls are adequate to restrict access to the database and data base change

utilities.
12. Determine how concurrent access to the same data item is prevented and if it is adequate.
13. Interview users to determine when passwords were last changed.
14. In a department where an employee has recently terminated (if possible), determine if the employee's password has been deleted.
15. Determine how access to password tables is restricted. Determine if access is restricted to only those who really need to access the table.

BACKUPS/PURGING/RECOVERY PROCEDURES
Describe the process used on a periodic basis to purge records from the active file. How often is this done?
Describe the procedures in place to backup the database and application processing capability in case of a disaster or machine malfunction.
Is a 3 year automated history kept on all cases?
Are daily transactions saved to backup in case of machine malfunction?
Do procedures exist so that data can be reconstructed in a reasonable period of time? (grandfather-father-son storage routine)
Is a duplicate set of files, programs, documentation, and systems files stored off-site and restricted from unauthorized access?
Is at least one generation of files maintained in a location other than tape storage area? How often are these updated to reflect most current data/programs?
Describe how disaster recovery arrangements have been performed, planned, and tested by the state.
Have emergency procedures been documented?
Do they include steps to take in the event of a natural disaster?
Are employees familiar with the emergency procedures?
Are heat and smoke detectors installed at the central data center? At the State agency? In the local offices?
Are proper portable fire extinguishers located in strategic and accessible areas? Are they periodically test?
Does an automatic fire suppressing system protect the computer center?
Is the center equipped with temperature and humidity gauges that automatically activate signals if either goes outside the norm? norm?
Is the computer center backed up by an uninterruptible power supply?
Is there backup computer capacity within the computer center?
Is there backup capacity at an off-site location?
Have backup arrangements been documented?

Are backup procedures periodically tested at the backup data center?
SYSTEMS SECURITY-Data Access
Describe the procedures used to store, retrieve, maintain, and control data.
How are schema(s)/subschema documented?
Do DBMS application programs reside in separate libraries from non-DBMS application programs?
Are all changes to the database prevented unless authorized and initiated by persons independent of the data processing function? (Separation of duties)
Are all persons prevented from overriding or bypassing data validation on editing problems?
Is the override function restricted to supervisory personnel in a limited number of circumstances?
Are all system overrides automatically logged by the application so that these actions can be analyzed for appropriateness and correctness?
Are account codes, authorization codes, passwords, etc. controlled to prevent unauthorized usage?
Has a formal change procedure for computer programs been established which requires supervisory authorization before implementation?
Do programmers test modifications against test data as opposed to live?
Does the same programmer make code changes to programs as well as test these changes?
Is access to system utility programs denied to computer operators?
Does the program library do the following: Restrict access to application programs? Control movement of programs from test to production modes? Provide an audit trail of all changes made to programs? Remove obsolete programs on a regular basis from both the source and object libraries? Deny access to program libraries maintained by the system to computer operators?
Are there documented procedures for password assignment, maintenance, and cancellation?
Is the delegation and maintenance of the password system limited to a select number

of people?
Is a mechanism in place to notify those responsible for maintaining the password system of personnel changes?
How frequently are passwords changed?
Are users told not to post user-IDs and passwords in easy-to-see places?
Are all software/data accesses logged? <ul style="list-style-type: none"> • Is the user uniquely identified? • Is the PC uniquely identified? • Is the date/time of access identified? • Are the functions performed identified?
Are access violation reports generated?
Are reports listing authorized users and their access authorities periodically generated and reviewed by management?
Is the responsibility for issuing and storing magnetic tapes, disk packs, or other storage media assigned to a librarian?
Are library procedures documented?
Are sensitive files (such as security classification or privacy act restrictions) properly identified as such and appropriately secured?
Has an overall agency-wide responsibility for conducting periodic risk analyses been formally assigned?
Does the risk analysis measure vulnerability related to fraud or theft or loss of proprietary data and harm to agency activities?
How often are risk analyses conducted? Are these required to be conducted whenever there is a significant change to the physical facility, hardware, or operating system software?
List all available access levels for the system and what can/cannot be done at each level.
Has the agency assigned responsibility for computer security at each office?
When an employee is terminated, is the employee denied access to the data processing department? <ul style="list-style-type: none"> Denied access to any data, program listings, procedure manuals? Are other employees informed of the employee's termination? When is the password deleted from the system?
Are inventory records of all tapes and disks maintained?

Are status records of tapes and disks maintained?
Is Office Automation software (Office 2000, etc.) used? Does it require a separate login to access?
Are users informed and periodically reminded that use of unauthorized software or copying of office software is forbidden?
Is Virus Protection software in place? How often is it updated? Manually or automatically? How is it distributed to user machines?
Does office policy require virus scanning of all foreign disks/files prior to their use on LAN machines?
SECURITY – Physical/Environmental
Is office access controlled by a single entry point, which is monitored by a guard or receptionist?
Do "combination locks", security badges, or other means restrict access to the computer room or spaces where computer equipment is available for use?
Are there security guards during office hours?
Are there security guards after office hours?
Are combination locks or equivalent periodically changed?
Are workstation components secured (bolted or cabled)?
Are personnel trained to challenge improperly identified visitors?
IS LAN servers and administrative terminals located in a secure area accessible only to IT personnel?
Is access to the computer area limited to necessary personnel?
Is the telecommunications closet locked at all times?
Are keys to the file server and telecomm closet controlled to eliminate unauthorized access?
IS LAN operating manuals and documentation properly secured?
Are office computer standards and policies written down?
Do users log or turn off their computers when they will be away for an extended period of time?
Does the system <u>automatically</u> log off a user from a LAN session after a period of

inactivity?
Are workstations, LAN servers and telecomm closets kept clean and free of dirt, dust, and food?
Do surge protectors or line conditioners protect components?
Does an Uninterruptible Power Supply (UPS) protect the LAN?
Are there plastic or protective covers for components?
Are components covered up at night and during emergency evacuation drills?
Do users receive periodic training on emergency evacuation responses and good housekeeping practices?
SYSTEM UTILIZATION
Number of scheduled 8 hour shifts per day:
Number of scheduled days per week:
Average number of jobs per day:
Average number of programs running concurrently:
Does the system provide the capability to electronically transmit data to FNS?
SYSTEM DOCUMENTATION
Does program documentation include:
a) General narrative description of the program?
b) Original specifications plus any modifications?
c) Detailed narrative description of the program?
d) Detailed logic diagram or decision table?
e) Input record formats?
f) Input record descriptions?
g) Output record formats?
h) Output record descriptions?
i) Master file formats?
j) Master file description?
k) List of constants, codes, and tables used?
l) Source program listing?
m) Object program listing?
n) Operating instructions?
o) Description of test data used to test program?
Is access to program documentation restricted to persons who do not operate the equipment?
Are copies of all documentation stored off-site?

Is stored program documentation periodically updated to match that being used?
Are all program changes and their effective dates recorded in run books in a manner that preserves an accurate chronological record of the system?
How often is documentation reviewed to ensure it is current?
Have documented procedures been established covering the operations of the data center?
Are daily equipment operating logs maintained?
Is downtime shown and explained?
Is there an error log or report for each program run?
Are all processes and operator decisions recorded in a daily log?
Is the operator log regularly reviewed for unusual/unauthorized operator actions?
Do these requests describe the proposed changes and reasons for them?
Are changes in the master file authorized in writing by the initiating departments?
Are departments that initiate changes in master file or programs furnished with notices or a register showing changes actually made?
Are changes reviewed to ensure that they were made properly?