Section-02 Information Services	OP-020703	Page: 1	Effective Date: 12/29/2021
Auditing Computerized Applications	ACA Standards: None		
Scott Crow, Director Oklahoma Department of Corrections		Signature on File	

Auditing Computerized Applications

I. Auditing Procedures

All computerized applications supported by the Office of Management and Enterprise Services (OMES) Information Services Division (ISD) will be audited periodically to ensure user and management needs are being met and operating procedures are being followed. The chief administrator of Physical Security will ensure audits are performed in accordance with this procedure. Audits that require the OMES ISD involvement will be requested via a Cherwell ticket.

A. Guidelines for Audits

Audits of computerized applications supported by IT will ensure that:

1. The application is functioning correctly as designed;
2. The application is adequately meeting user and management needs;
3. All source code, programs, and documentation are current;
4. All necessary procedures relating to security, backups, contingency plans, and cross-training are being followed;
5. The computer equipment has sufficient capacity for continued normal operations;
6. The application is being used correctly and all applicable operational procedures are being followed;
7. Licensed software is validated, ensuring illegal software is not in use;
8. Software conforms to state and agency standards; and
9. Removal of any unauthorized software.

B. Internal Audits

Information Technology application audits will ensure that:

1. All libraries, directories, source code, and documentation are current;

2. The Help Desk is maintaining a problem log for application complaints;

3. A specific individual is responsible for program support and upgrades for each application;

4. Cross-training of user staff is conducted in accordance with OP-100101 entitled “Training and Staff Development;”

5. Security measures are being taken to protect the source library, directories, application code, and data;

6. Backup/recovery measures are taken to protect the source library, directories, application code, and data; and

7. Information security is maintained in accordance with state and agency standards.

C. External Audits

Field application audits will ensure that:

1. All software and related policies and procedures, administrative memorandums and manuals are current;

2. A problem log is being maintained;

3. Backups/recovery routines are being followed by determining the frequency and storage of backups;

4. Adequate disaster/contingency plans have been developed;

5. Verify that cross-training has occurred to ensure support in the event of leave, employee turnover, etc., and to avoid dependence on key personnel;

6. Information security is maintained in accordance with state and agency standards; and

7. Field staff are using the system correctly and in accordance with published instructions and user documentation.

II. References

Policy Statement P-020700 entitled "Oklahoma Department of Corrections Data System Management"

OP-100101 entitled “Training and Staff Development”

State of Oklahoma Information Security Policy, Procedures, and Guidelines Security Policy, Procedures, and Guidelines Revised December 2017

III. Action

All senior staff is responsible for compliance with this procedure.

The chief administrator of Physical Security is responsible for the annual review and revisions.

Any exceptions to this procedure will require prior written approval from the agency director.

This procedure is effective as indicated.

Replaced: OP-020703 entitled "Auditing Computerized Applications" dated December 10, 2020

Distribution: Policy and Operations Manual
Agency Website