
POLICY TRANSMITTAL NO. 09-37

DATE: AUGUST 28, 2009

DATA SERVICES DIVISION

DEPARTMENT OF HUMAN SERVICES
OFFICE OF LEGISLATIVE RELATIONS AND
POLICY

TO: ALL OFFICES

SUBJECT: MANUAL MATERIAL

OKDHS:2-41, Table of Contents; 2-41-4; 2-41-6; 2-41-13; and 2-41-14
through 2-41-15;

EXPLANATION: OKDHS:2-41-4 is revised to improve readability.

OKDHS:2-41-6 is revised to reflect changes in the name and structure
of Data Services Division (DSD) units.

OKDHS:2-41-13 through OKDHS:2-41-14 are revised to reflect name
change of DSD units.

OKDHS:2-41-15 is revised to reflect security emphasis placed with
individual employees in securing electronic devices and information
contained on those devices.

Original signed on 8/25/09

Sarjoo Shah, Director
Data Services Division

Sandra Harrison, Coordinator
Office of Legislative Relations and Policy

WF # 09-K (PMc)

INSTRUCTIONS FOR FILING MANUAL MATERIAL

OAC is the acronym for Oklahoma Administrative Code. If OAC appears before a number on an Appendix or before a Section in text, it means the Appendix or text contains rules or administrative law. Lengthy internal policies and procedures have the same Chapter number as the OAC Chapter to which they pertain following an "OKDHS" number, such as personnel policy at OKDHS:2-1 and personnel rules at OAC 340:2-1. The "340" is the Title number that designates OKDHS as the rulemaking agency; the "2" specifies the Chapter number; and the "1" specifies the Subchapter number.

The chronological order for filing manual material is: (1) OAC 340 by designated Chapter and Subchapter number; (2) if applicable, OKDHS numbered text for the designated Chapter and Subchapter; and (3) all OAC Appendices with the designated Chapter number. For example, the order for filing personnel policy is OAC 340:2-1, OKDHS:2-1, and OAC 340:2 Appendices behind all Chapter 2 manual material. Any questions or assistance with filing manual material will be addressed by contacting Policy Management Unit staff at 405-521-4326.

REMOVE

OKDHS:2-41, Table of Contents

OKDHS:2-41-4

OKDHS:2-41-6

OKDHS:2-41-13

OKDHS:2-41-14

OKDHS:2-41-15

INSERT

OKDHS:2-41, Table of Contents, 1 page, revised 9-1-09

OKDHS:2-41-4, 2 pages, revised 9-1-09

OKDHS:2-41-6, 6 pages, revised 9-1-09

OKDHS:2-41-13, 1 page, revised 9-1-09

OKDHS:2-41-14, 5 pages , revised 9-1-09

OKDHS:2-41-15, 11 pages , revised 9-1-09

SUBCHAPTER 41. DATA SERVICES DIVISION

- OKDHS:2-41-1. Data services
- OKDHS:2-41-2. Legal base and authority **[REVOKED]**
- OKDHS:2-41-3. Mission and goals **[REVOKED]**
- OKDHS:2-41-4. Definitions
- OKDHS:2-41-5. Desired performance standards **[REVOKED]**
- OKDHS:2-41-6. Data Services Division Units
- OKDHS:2-41-7. Systems Design and Development Unit **[REVOKED]**
- OKDHS:2-41-8. Data Center Services Unit **[REVOKED]**
- OKDHS:2-41-9. Data Base Administration **[REVOKED]**
- OKDHS:2-41-10. Customer Support Services Unit (CSSU) **[REVOKED]**
- OKDHS:2-41-11. Network and Local Area Network (LAN) Management (NLM) Unit **[REVOKED]**
- OKDHS:2-41-12. Data processing planning
- OKDHS:2-41-13. Data processing application systems maintenance and development process
- OKDHS:2-41-14. Acquisition of data processing equipment, software, and supplies
- OKDHS:2-41-15. Data security
- OKDHS:2-41-16. Software copyright policy

OKDHS:2-41-4. Definitions

Revised 9-1-09

The following words and terms when used in the Part, shall have the following meaning, unless the context clearly indicates otherwise.

"Application" means a software program designed to enable end users to carry out a specific task or function. Word processors, spreadsheets, graphics programs, and data managers are application examples.

"Automated information systems" means computerized processes which collect, store, calculate, and display or report information about business processes.

"Bus" means a subsystem that transfers data between computer components inside a computer or between computers. In a network, a bus is a transmission path on which signals are dropped off or picked up at every device attached to the line. Only devices addressed by the signals pay attention to them; the others discard the signals.

"Channel Service Unit/Digital Service Unit (CSU/DSU)" means a system that converts electronic computer protocol to digital telephone protocol and vice versa.

"Confidential data" means any piece of data or set of data, the misuse of which violates existing laws or policy, violates client confidentiality or privacy, creates a liability exposure for Oklahoma Department of Human Services (OKDHS), or creates the opportunity for fraud or other illegal activities.

"Controller" means a device that acts as the electrical and logical interface between data terminal equipment and a local area network bus.

"DB2 (Database-2)" means the International Business Machines (IBM) strategic product for general purpose information storage, including database management. It is a reasonably complete implementation of the relational technology. The most strategic component or aspect of DB2 is the interface Structured Query Language (SQL). DB2 is properly viewed as an SQL engine.

"Database architecture" means overall plan and design for OKDHS data structure.

"Data Security" means processes and procedures to ensure data collected and maintained by OKDHS is protected from inadvertent or intentional damage or misuse.

"**Hardware**" means terminals, printers, personal computers, CSU/DSU, controllers, routers, hubs, servers, and central site equipment.

"**Information Management System (IMS)**" means an IBM software product providing an environment for database and transaction processing and database management.

"**ITB**" means invitation to bid.

"**Local Area Network (LAN)**" means a hardware and software environment consisting of a central computer, referred to as a server, that has multiple personal computer workstations, referred to as client(s), and allows or supports telecommunications among the clients.

"**Network**" means a configuration of data processing devices and software connected for information exchange.

"**PC**" means personal computer.

"**Remote access**" means a technology that allows the capability to dial-in or dial-out of a computing capability or network.

"**Router**" means a device that performs a function similar to a local or remote bridge. Routing, however, occurs at Layer 3 of the Open Systems Interconnection (OSI) reference model.

"**Server**" means main controller for a PC hooked to a LAN.

"**Virus**" means an unauthorized data processing application which may alter or destroy computerized data and/or equipment.

"**Wide Area Network (WAN)**" means telecommunications network composed of multiple LANs connected via server, routers, hubs, and phone lines.

"**Workstation**" means the individual OKDHS employee's PC and printer.

OKDHS:2-41-6. Data Services Division Units

Revised 9-1-09

(a) **Enterprise Application Services.** Enterprise Application Services (EAS) is responsible for consultation, design, development, and maintenance for most Oklahoma Department of Human Services (OKDHS) data processing applications and systems. EAS and the appropriate divisions are responsible for approving all OKDHS applications that process on the host and client server environment supported by Data Services Division (DSD). When contracting these services, EAS provides management and staff. The services performed are:

- (1) research;
- (2) consultation;
- (3) maintenance;
- (4) enhancement; and
- (5) new programming.

(b) **Enterprise Support Services.** Enterprise Support Services (ESS) is comprised of five sections:

- (1) Production Services provides technical support for the set up and validation of all production batch and file transfer jobs;
- (2) Operations:
 - (A) oversees all central site equipment such as network, servers, and mainframe;
 - (B) oversees daily production schedules; and
 - (C) conducts systems performance analyses to set benchmarks and thresholds for increased performance;
- (3) Remote Site Services installs all equipment and software in local offices;
- (4) Problem Determination and Resolution:

(A) works to resolve any highly complex problems that arise needing cross unit analysis; and

(B) is operational 24 hours a day, seven days a week, excluding holidays; and

(5) Facilities:

(A) maintains an inventory of all OKDHS data processing hardware and software including:

(i) manufacturer;

(ii) model;

(iii) serial number; and

(iv) warranty end date;

(B) submits the inventory to Office of State Finance (OSF) annually per Section 41.5e of Title 62 of the Oklahoma Statutes (62 O.S. 41.5e); and

(C) secures appropriate maintenance contracts each fiscal year for OKDHS data processing hardware and software.

(c) **Enterprise Technical Services.** Enterprise Technical Services (ETS) is responsible for technical support of information technology (IT) services provided throughout the OKDHS computer network environment. Sections within ETS include: Database Services, Infrastructure Platform and Software Services, Architecture and Design Services, Security Services, and Telecommunications Services. The specialists in ETS work with other DSD units to support the OKDHS environment, and team with other DSD units and OKDHS divisions in partnership on OKDHS projects and processes. Services provided by ETS include:

(1) generation, security, availability, and recoverability of OKDHS host-based Information Management System (IMS), Oracle, Database 2 (DB2), and Structured Query Language (SQL), server database and data stored and maintained in the databases. Host in this context refers to the database servers residing in the OKDHS Data Center at 1110 N.E. 12th Oklahoma City, OK;

(2) support, security, availability, and recoverability of the OKDHS network environment that includes servers residing at the OKDHS Data Center, in remote

field locations, third party software, and the telecommunications equipment and circuits used for connectivity across the network;

(3) support for decentralized data security activities including the decentralized data security representatives;

(4) design, development, maintenance, and security of the InfoNet or Internet applications as related to the access of information or data stored and maintained in any of the host based servers;

(5) support for OKDHS data sharing committees whose activities relate to data sharing at the intra-agency, interagency, interstate, and non-OKDHS levels;

(6) develop and ensure technology implementation plans and designs support the OKDHS enterprise architecture;

(7) develop and document DSD processes and standards in collaboration with other DSD units and sections;

(8) review and evaluate each technology solution and new data processing technology supported by DSD to ensure compliance with OKDHS DSD enterprise strategies;

(9) approve all OKDHS requisitions for all non-standard electronic data processing hardware and software to ensure that the acquisition is compatible with the current data processing environment and consistent with future planning and standards; and

(10) establish technology hardware and software standards for OKDHS.

(d) **Customer Relations and Support.** Customer Relations and Support (CRS):

(1) facilitates the delivery of quality solutions and services provided by DSD through information sharing and feedback ensuring technology supports the business of OKDHS and customers;

(2) measures customer service success;

(3) continuously improves communications within OKDHS;

(4) promotes and markets technology solutions;

- (5) supports all OKDHS IT budgeting and fiscal operations;
- (6) supports traditional business services, such as:
 - (A) general accounting;
 - (B) accounts payable;
 - (C) claims processing;
 - (D) budgeting;
 - (E) purchase authorization system maintenance;
 - (F) requisition and purchase of goods and services;
 - (G) contract administration;
 - (H) inventory and asset management;
 - (I) human resource services; and
 - (J) training;
- (7) completes OKDHS annual Long-Range Electronic Data Processing Plan (Plan) per 62 O.S. 41.5e;
- (8) processes any required updates of the Plan during the fiscal year;
- (9) submits the Plan to OSF each year as a part of the OKDHS overall budget process per OKDHS:2-41-12; and
- (10) maintains an inventory of all OKDHS data processing hardware and software including:
 - (A) manufacturer;
 - (B) model;
 - (C) serial number; and
 - (D) warranty end date.

(e) Research and Strategy. In collaboration with other units within DSD, Research and Strategy:

- (1) performs research in support of the OKDHS DSD Enterprise Architecture;
- (2) develops strategies for the implementation of needed products and services to support OKDHS business requirements, such as strategies for:
 - (A) privacy;
 - (B) security;
 - (C) delivery; and
 - (D) technological solutions;
- (3) develops long-term strategic planning and support;
- (4) performs risk assessment of recommended technology solutions; and
- (5) collaborates with CRS Business Development to establish new marketing and promotional material for DSD.

(f) Business Quality. Business Quality staff is integrally involved with all areas of DSD to coach and ensure that quality practices are followed as a fundamental part of daily practice. Business Quality:

- (1) enforces quality in the products and services offered by DSD; and
- (2) provides business continuity initiatives for OKDHS by:
 - (A) implementing and monitoring the primary components of quality which are:
 - (i) process definition;
 - (ii) requirements management;
 - (iii) project tracking;
 - (iv) change management;

- (v) risk management; and
 - (vi) performance measurements; and
 - (B) instituting business continuity practices into OKDHS systems; and
 - (3) establishes new practices that are well planned, thoroughly defined, and measured ensuring not only compliance, but the continual optimization of processes thereby improving customer service.
- (g) **Project Management Office.** The Project Management Office (PMO):
- (1) delivers professional project management services to OKDHS divisions through the delivery of new and existing information technology projects; and
 - (2) manages the OKDHS portfolio management process including the communication, facilitation, and management of OKDHS Information Technology Governance Board projects.

OKDHS:2-41-13. Data processing application systems maintenance and development process

Revised 9-1-09

Oklahoma Department of Human Services (OKDHS) data processing application systems maintenance and development projects which utilize Data Services Division (DSD) hardware and software are coordinated and approved by DSD. All DSD data processing support is coordinated through the DSD Customer Relations and Support (CRS) coordinator assigned to the requesting office or division.

(1) **Project initiation.** The office or division requiring data processing support along with the CRS coordinator define the basic requirements of the project. The user division initiates web-based form, Portfolio Management Pre-Project Assessment Questionnaire.

(2) **Requirements.** The CRS coordinator works with the requesting division to establish detailed requirements for the service requested. The coordinator assists the requesting division in preparing any necessary federal planning documents, funding requests, or both. If it is determined that part or all of the project is to be out-sourced, the coordinator assists the requesting division in preparing an invitation to bid (ITB) and evaluating bid responses.

(3) **Project plan.** If the project is accomplished utilizing DSD resources, the CRS coordinator:

(A) establishes a project plan;

(B) develops any additional sub-projects;

(C) routes the project plan, work request, and project requirements to the appropriate DSD unit for assignment of resources;

(D) negotiates the project priority; and

(E) monitors the project until completion.

OKDHS:2-41-14. Acquisition of data processing equipment, software, and supplies

Revised 9-1-09

(a) **Division support.** The Data Services Division (DSD) provides support to the other divisions of the Oklahoma Department of Human Services (OKDHS) by assisting in the acquisition, installation, and maintenance of data processing hardware, software, and supplies. The requesting division must complete the web-based Purchase Requisition Form Entry page located on the OKDHS InfoNet for all data processing purchases coordinated and approved by DSD to ensure purchases are compatible with the current data processing environment and consistent with the (Plan) and OKDHS standards.

(b) **Disagreements.** In those instances where the user division disagrees with the DSD recommendation, the issue is referred to the Information Services Division chief information officer (CIO). The CIO tries to resolve the differences by mutual agreement. If the differences are not resolved by the CIO, then the issue is referred to the OKDHS Director for resolution.

(c) **Office automation.** DSD coordinates development of office automation systems and ensures acquisitions and processes allow for interconnectivity of all equipment. OKDHS moves toward a total integrated system encompassing:

- (1) word processing;
- (2) electronic mail;
- (3) host computer center communication;
- (4) personal computing;
- (5) communication;
- (6) video teleconferencing;
- (7) graphics;
- (8) data update, storage, and retrieval; and
- (9) mobile technology.

(d) **Supplies.** DSD:

(1) assists other appropriate divisions and units to ensure state contracts are available to cover needs for technology supplies that cannot be purchased through the standard office supply ordering process;

(2) provides input and assistance to the Department of Central Services for establishment of a statewide personal computer hardware contract; and

(3) secures non-encumbered contracts for other Local Area Networks (LANs) and Wide Area Networks (WANs) related hardware and software needs.

(e) **Maintenance contracts.** DSD establishes OKDHS maintenance contracts for data processing hardware and software including terminals, printers, personal computers, Channel Service Unit (CSU) and Data Service Unit (DSU) controllers, routers, hubs, servers, central site equipment, and all standard purchase software associated with the LAN or WAN and central site data processing.

(f) **Hardware and software inventory.** An inventory of all hardware and software installed statewide is maintained by DSD so that maintenance contracts for all OKDHS hardware and software are secured appropriately each year and to meet the annual state agency reporting requirement per OKDHS:2-41-12. All divisions are expected to forward a copy of receiving report documentation to DSD Enterprise Support Services for all hardware and software acquired. Any move, change, addition, or deletion of hardware or software is promptly reported. The inventory information maintained includes:

(1) purchase authorization number;

(2) manufacturer;

(3) model number;

(4) serial number;

(5) description;

(6) cost;

(7) warranty end date;

(8) location installed; and

(9) technical and network information.

(g) **Hardware.** DSD is responsible for:

(1) approving all purchase or lease of data processing hardware;

(2) having the necessary contracts available to expedite the ordering and provide standardization;

(3) preparing and coordinating bid documents, and reviewing all such documents which are prepared by users;

(4) completing the Purchase Requisition Form Entry Page on the OKDHS InfoNet for data processing hardware and sending it to the requesting user division for purchase authorization number, approval, and processing in those instances where non-DSD funds are used. This web-based document is submitted through normal processing channels to Support Services Division (SSD) Contracts and Purchasing; and

(5) coordinating delivery of hardware.

(h) **Installation.** DSD assists in the:

(1) installation planning and the acquisition of the resources for the installation of electronic data processing hardware and software and the installation of the hardware, software, and cabling necessary to provide LAN or WAN connectivity; and

(2) identification of necessary physical requirements for installation of electronic data processing equipment, such as electrical, air conditioning, and space. Users are responsible for all modifications, such as electrical modifications or changes necessary for the installation of their electronic data processing equipment.

(i) **Maintenance service calls.** All problems with supported LAN or WAN hardware and software are reported through the DSD Call Center. The Call Center logs the problem and places a trouble call with the appropriate DSD unit or contractor to resolve the problem.

(j) **Data processing equipment moves.** When it becomes necessary to relocate an office or data processing equipment within an office, planning and acquisition of the equipment and resources are initiated a minimum of eight weeks in advance of date of the required move, installation, or both.

(1) The OKDHS division or office requiring the move notifies the DSD Customer Relations and Support (CRS) assigned coordinator of the proposed move. The human services center (HSC) routes a move request to the area director and Field Operations Division (FOD) for approval. FOD coordinates the HSC move with DSD and any other affected divisions. This notification includes:

(A) the physical locations the equipment is being moved from and to;

(B) the equipment identification such as type of equipment, serial numbers, bar codes, and finding location of the equipment;

(C) contact person name and phone number; and

(D) network connectivity such as KIDS, and Human Resources Information System (HRIS).

(2) Acquisition of additional equipment or connectivity resources may be required for:

(A) electrical capacity. Electrical capacity is reviewed to determine if additional capacity is required;

(B) cabling. The relocating office must arrange the cabling with the wiring contractor, currently the OKDHS Support Services Division (SSD) Facilities Management Services Construction Unit. At least one month notification is normally required by the contractor prior to the installation date. The DSD CRS assigned coordinator is available to assist with planning;

(C) network devices such as routers, hubs, CSU and DSUs are ordered at least eight weeks prior to the desired installation date by the relocating office with the assistance of DSD;

(D) data lines. At least four weeks prior to the desired installation date, DSD arranges for the appropriate phone company to install the necessary data lines;

(E) work stations. Work stations are ordered at least eight weeks prior to the desired installation date by the relocating office with the assistance of DSD; and

(F) printers. Printers are ordered at least eight weeks prior to the desired installation date by the relocating office with the assistance of DSD.

(3) The relocating office is responsible for arranging for the packing, unpacking, transportation, and installation of all new and existing equipment.

(4) The relocating office must notify SSD Departmental Services Unit Asset Management and Accounting of the bar codes and serial numbers of all equipment which is acquired, moved, or both.

(k) **Software.** Responsibilities of DSD regarding software purchases include:

(1) reviewing and recommending software purchases, leases, or both;

(2) approving all computer software acquisitions prior to purchase;

(3) preparing the web-based document, Purchase Requisition Form Entry Page, to order the software and transmitting the paperwork to the respective division for purchase authorization number, approval, and processing in those instances where non-DSD funds are used;

(4) providing recommendations for training and consulting support on a standard set of software;

(5) providing recommendations for methods of obtaining installation support of all software;

(6) providing maintenance contracts for all supported software, when deemed necessary. DSD is not responsible for maintenance of programs developed and written by users, although it is available to provide technical support as feasible; and

(7) tracking all software licenses ensuring compliance with vendor copyright laws and licensing requirements.

OKDHS:2-41-15. Data securityRevised 9-1-09

(a) **General policy.** All data collected and maintained by Oklahoma Department of Human Services (OKDHS) is owned by and becomes the responsibility of OKDHS. The objective of data security is to ensure the data collected and maintained by OKDHS is protected from inadvertent or intentional damage or misuse. Data is accessible, subject to legal restrictions and the appropriate approval processes as outlined in this regulation, to all entities, both governmental and non-governmental, as needed to accomplish OKDHS objectives. There is no expressed or implied expectation of privacy for users of any OKDHS computer network, computer equipment, or other computer resources. All actions or keystrokes of such users may be monitored at any time.

(1) Data security is the responsibility of all individuals who interact in any way with OKDHS computer systems, computer resources, networks, or data. These individuals have the basic responsibility to protect data and conserve resources they use, or come in contact with, in the course of performing their assigned duties, and they are responsible for utilizing and implementing practices that support and comply with OKDHS data security guidelines.

(2) Data Services Division (DSD) Enterprise Technical Services (ETS) Security Services Section, in conjunction with the OKDHS Information Security Office (ISO), is responsible for drafting, obtaining OKDHS management's approval, disseminating, and updating OKDHS data security guidelines.

(3) DSD, in conjunction with the ISO, has lead responsibility for data security as it relates to data in machine readable form. The ETS Security Services Section assists with monitoring data security practices and interfacing with Electronic Data Processing (EDP) auditors.

(b) **Delegation of data ownership.** For the purposes of interpreting confidentiality restrictions imposed by law, establishing data classification, and approving access to data, ownership of data is delegated by OKDHS to the OKDHS division director, whose division collects and maintains the data.

(c) **Classification.**

(1) All data is classified as either confidential or non-confidential data.

(A) Confidential data is any piece of data or set of data, the misuse of which violates existing laws or policy, violates client confidentiality or privacy, creates a liability exposure for OKDHS, or creates the opportunities for fraud or other illegal activity.

(B) Non-confidential data is any piece of data or set of data which is not confidential.

(2) Guidelines for classification are listed in (A) - (C) of this paragraph.

(A) A data set is classified according to the most sensitive detail it includes.

(B) Information recorded in several formats of media, for example source document, electronic record, or report has the same classification regardless of format or media.

(C) OKDHS complies with Oklahoma's Open Records Act. Certain designated persons who are authorized to release records may request the normal classification category be waived, subject to approval by the owner of the data.

(d) **Assignment of responsibilities.** Data security administration consists of three primary entities which are in turn supported by several functional area entities. The three primary entities are the data owner, the decentralized security representative (DSR), and ETS Security Services. Data processed by the computerized systems must have an identified owner, such as division director, area director, county director, or unit administrator, and the ownership assignment must be documented with ETS Security Services.

(1) The data owner may, at his or her discretion, delegate data security administration responsibilities to a decentralized security representative (DSR). The delegation of a DSR must be in writing and submitted to ETS Security Services using Form 055C002E, Decentralized Access Control Security Agreement. The data owner or his or her delegated DSR is responsible for:

(A) ensuring data is collected and stored in a manner that meets all federal and state laws and OKDHS policy;

(B) classifying data according to legal and OKDHS policy restrictions;

(C) determining and authorizing access and utilization criteria based on the classification; and

- (D) specifying and communicating access and utilization criteria to the ETS Security Services manager.
- (2) The ETS Security Services manager is responsible for:
- (A) processing and filing all requests for access including approvals and denials; and
- (B) administering controls as specified by the owner. These responsibilities include:
- (i) administering access controls to data and resources;
 - (ii) providing procedural safeguards;
 - (iii) providing a method of assigning unique logon identification (ID) numbers and encrypted passwords to ensure user accountability;
 - (iv) furnishing reports of access violations as required;
 - (v) assisting the ISO in providing security awareness education to owners and users;
 - (vi) maintaining information concerning which users have access to what data and resources; and
 - (vii) alleviating disagreements between users and owners concerning access.
- (3) The DSR is appointed by the data owner and coordinates security activities with the ETS Security Services manager. The DSR is responsible for:
- (A) assisting the ETS Security Services manager within the guidelines of OKDHS policy;
- (B) assisting in development of security designs for user requirements which fall within his or her scope;
- (C) testing and exercising the security controls which fall within his or her scope;
- (D) documenting security controls within his or her scope;

(E) administering access controls to data and resources owned by his or her division;

(F) providing procedural safeguards;

(G) supporting the assignment of unique logon IDs and encrypted passwords to ensure user accountability;

(H) reporting violations, abuse of logon IDs, and potential breaches in security to appropriate authorities and providing follow-up activity if needed;

(I) establishing new users and terminating users as appropriate, including notifying DSD Security Services of new, moved, or terminated employees;

(J) complying with all security controls established by the owner of the data and DSD ETS Security Services manager;

(K) training the users of the Local Area Network (LAN) on security control established for the LAN; and

(L) interfacing with and providing information to auditors.

(e) Functional responsibilities.

(1) ETS Security Services Section is the organizational unit within DSD responsible for maintaining the security of OKDHS computerized data and ensuring a valid and secure network environment within the guidelines of OKDHS policy. The ETS Security Services manager is a member of this organizational unit and is in charge of the Data Security Services Section.

(2) The ETS Infrastructure Platform and Software Section maintains the current hardware, operating system(s) and third party software configuration, and administration.

(3) The Telecommunications Services Section maintains the LAN and Wide Area Network (WAN) for OKDHS.

(4) The Database Services Section maintains all database repositories in use at OKDHS.

(5) The Production Services Section of Enterprise Support Services (ESS) is responsible for the scheduled production processing, job set up, job check out, and

output distribution. Production services activities performed by other units within OKDHS are also covered under this standard. Production processing is handled in a secure manner. Production Services is responsible for:

(A) accessing data and resources through the production facilities as developed by the ETS Unit and Enterprise Application Services (EAS) Unit; and

(B) maintaining production libraries.

(6) The Operations Section of ESS is responsible for operation of the computer equipment in the Data Center. The Operations Section is responsible for accessing data and resources through the facilities as developed by the ETS Unit.

(7) EAS develops and maintains OKDHS applications, plans for and designs data processing systems, and advises on design techniques and practices for OKDHS. EAS is responsible for:

(A) ensuring security requirements are addressed in the design and development process;

(B) designing the security requirements for the applications according to the established standards and working with the ETS security architect and ETS Security Services manager to implement these requirements; and

(C) determining if modifications to existing systems will have an impact on security, and if so, notifying the ETS Security Services manager.

(8) Customer Relations and Support (CRS) is responsible for coordination and communication with user divisions and other agencies. CRS serves as a liaison between the OKDHS user community and DSD ETS.

(9) The Telecommunications Services Section is responsible for all OKDHS networks and WANs and supporting network security, in conjunction with the ETS Security Services Section.

(10) Users include employees of OKDHS, vendors, contractors, and other individuals who operate, use, or interface in any way with the OKDHS computer systems, computer resources, or computerized data. The users are responsible for:

(A) complying with all security controls established by appropriate authority;

(B) using the data only for the accomplishment of official duties in the manner approved by the owner;

(C) keeping logon IDs and passwords used to access data and resources confidential including not sharing passwords; and

(D) notifying the ETS Security Services manager of abuse or sharing of logon ID numbers, passwords, or both.

(11) Project Management Office (PMO):

(A) focuses on project managers leading technology teams in the development and implementation of business applications as directed by the Information Technology (IT) Governance Board;

(B) assists the organization in learning to work in an environment where resources and team members are assigned to work on projects that involve multiple units; and

(C) is responsible for:

(i) the portfolio management of all IT projects;

(ii) ensuring security requirements are identified and incorporated in all OKDHS projects; and

(iii) ensuring those security requirements are according to established OKDHS policy and standards by working with the ETS security architect and Security Services manager to implement these requirements.

(f) Remote Access.

(1) In OKDHS computing environment, the remote access capability is prohibited unless expressly approved in writing by the division director or DSR.

(2) Remote access control seeks to ensure unauthorized access to OKDHS data or network capability is not achieved. Approved users of the remote access capability are able to perform approved functions from non-network locations. The remote access capability must have access to or from only one controlled entry point at a server level or higher, not at a user's personal computer (PC) or workstation; thus, a modem or compatible device cannot be used in conjunction with a user's workstation or PC which is connected to OKDHS network.

(g) **Virus protection.** All workstations and servers connected to the OKDHS network have terminate and stay resident (TSR) anti-virus software installed on them. In this environment, virus checking occurs when new media is introduced into the workstation environment. The software automatically eradicates known viruses. Stand alone work stations, work stations not connected to the OKDHS network, may or may not have this anti-virus software installed. Recommendations for virus control are listed in (1) through (3) of this subsection.

(1) Employees do not introduce machine-readable media, such as diskettes, files, and bulletin board downloads into their computing environment at work unless these items are directly related to their work and are scanned for viruses prior to use.

(2) No work related media created by, or received from, sources outside the immediate computing environment are introduced into the workstation environment until it has first been scanned for computer viruses using DSD approved anti-virus software. In a TSR protected environment, this scanning is done automatically. Any media which is taken from the immediate work environment, for example to a class or home, must be scanned before it is reintroduced to the workstation environment. If an employee suspects that non-approved staff may be using the employee's workstation, the employee contacts the DSD Security Services Section.

(3) If an employee thinks that a workstation is infected with a virus, the DSD Help Desk is notified of the problem.

(h) **LAN security.** DSD Security Services Section assists divisions with security issues and requirements for LANs. Any LAN connected through the communications network to any other LAN or mainframe in OKDHS has stringent controls placed upon it. These controls are for the intent of deterring any unauthorized access to OKDHS information. DSD ETS Security Services Unit provides advice and consultation to the division establishing a LAN environment regarding:

- (1) risk analysis;
- (2) security policy;
- (3) disaster recovery;
- (4) information security;
- (5) training of users;

- (6) physical security;
- (7) emergency preparedness; and
- (8) external audit and review.

(i) **Network security.** All networks that have accessibility to OKDHS data are subject to compliance with OKDHS data security guidelines documented in these regulations. Compliance with this provision constitutes a 'trusted relationship' among the respective networks. Under this 'trusted relationship,' the repetitious checking of user ID and passwords to re-authenticate a user's authority and access capabilities are not required. The objective of network security is to ensure the data collected and maintained by OKDHS and OKDHS computing resources are protected from inadvertent or intentional damage or misuse. DSD has lead responsibility for network security for OKDHS. DSD utilizes various methods for ensuring the OKDHS network is secure from unauthorized access. Methods for ensuring the OKDHS network is secure from unauthorized access include, but are not limited to:

- (1) encryption of all OKDHS data that travels over the Internet;
- (2) password protection of any routers that have remote access capabilities into the OKDHS network;
- (3) a front-end system that provides for definition of valid users for dial-up activity to the OKDHS host computer system;
- (4) a single Internet access point to and from the OKDHS network which is protected by firewall; and
- (5) a prohibition of personal equipment connected to any portion of the LAN or WAN. This opens OKDHS to civil liabilities and threatens the safety and security of all network resources.

(j) **Outgoing Internet usage.** Restrictions that apply to the use of the Internet are listed in (1) - (5) of this subsection.

- (1) Only authenticated users, with an active OKDHS user ID and password, are allowed access out through the OKDHS firewall.
- (2) Certain Internet sites and capabilities are blocked, made unavailable, and usage is monitored. There is no expectation of privacy when accessing the Internet. A record of all sites a user accesses is logged and archived.

(3) Aside from scheduled maintenance activities and unscheduled problem resolution activities, access to the Internet is available at all times.

(4) Any workstation on OKDHS network which is used to access the Internet must have OKDHS standard anti-virus software running on it.

(5) Encryption must be used when transmitting OKDHS data over the Internet. Any plans to transmit data must be worked through ETS Security Services.

(k) **Incoming Internet usage.** Processes and controls pertaining to incoming Internet usage requests are established by ETS Security Services on a case by case basis depending on the specific business need and security requirements.

(l) **Mobile devices.** A mobile device is any small computing device which includes, but is not limited to, laptop and tablet computers, personal digital assistants (PDA), and smart-phones. A mobile device is convenient, allowing the user to work from almost any location. The restriction of no personal equipment on the OKDHS network extends to mobile devices. Users in possession of an OKDHS mobile device must:

(A) protect the mobile device from theft and/or unauthorized use. The device may contain sensitive and/or privileged information on both employees and OKDHS clients;

(B) ensure that the device remains encrypted in accordance with OKDHS policy and procedures;

(C) control and protect the device at all times.

(i) A mobile device must not be left unprotected in the passenger compartment of an automobile. If the user has no other option, it is stored in the locked trunk.

(ii) When in public, the user keeps the device off the floor and in the user's possession at all times. If it must be put down, the user places the device between his or her feet or at least against his or her leg so the user is aware of it;

(D) not store client or employee identifiable and personal data on the mobile device. If a user must save data because of a client visit or other official duty, the data must be removed or downloaded to the appropriate location, business application or user's U drive, as soon as possible. Data, both business and personal, is not secure when it remains stored on the hard drive of a mobile device;

(E) keep the mobile devise in the proper bag or carrying case and in the user's possession at all times when traveling.

(i) Mobile devices cannot be checked baggage for air or ground travel.

(ii) When in transit or at airports, users must:

(I) pay special attention to the care and upkeep of the mobile device;

(II) keep aware of the device at all times, especially while going through security;

(III) hold the device until the person in front has cleared the metal detector; and

(IV) keep the device in sight when it emerges on the other side of the screener. If possible, request it be hand-checked.

(iii) When in hotels, store the mobile device safely, such as in a drawer, closet, suitcase, or room safe; and

(F) when a mobile device is lost or stolen, report the loss or theft immediately to:

(i) local authorities;

(ii) his or her immediate supervisor; and

(iii) OKDHS Information Security Office.

(m) **E-mail usage.** The purpose of this subsection is to identify the circumstances under which a user may use the OKDHS electronic mail (e-mail) system, define what OKDHS considers acceptable use and conduct in utilizing e-mail, provide clear communication of OKDHS expectations with respect to what is and what is not acceptable use, and minimize the risk of offensive or inappropriate e-mail.

(A) The OKDHS e-mail system is the property of the state of Oklahoma. Users are authorized to use e-mail consistent with its intended purpose. Because OKDHS users are to devote full time to their assigned duties, personal use of e-mail is limited. Excessive use of e-mail for personal purposes is prohibited.

(B) Solicitation of any type, via e-mail, by a user is prohibited. E-mail must not be used to convey information about commercial ventures, or religious or political causes.

(C) Users must not utilize e-mail to send messages that serve to:

(i) contribute to an intimidating or offensive workplace; or

(ii) threaten, make derogatory statements, or otherwise discuss others' race, national origin, sexual orientation, age, disability, religious or political beliefs, gossip, or otherwise undermine harmonious business relationships.

(D) The author loses control of an e-mail's duplication and distribution by others once the e-mail has been sent.

(E) All messages sent via e-mail are the exclusive property of OKDHS. Messages are monitored, archived, and can be retrieved to be used in court proceedings, disciplinary proceedings, or any other legitimate OKDHS business and may be subject to disclosure under the Open Records Act.

(F) Users have no reasonable expectation of privacy regarding e-mail messages. OKDHS will, with or without prior notice, monitor a user's e-mail. All e-mail is automatically stored on the OKDHS network system. Deleted messages may be restored and read by OKDHS for any reason.

(G) The appropriate division director or DSR must contact ETS Security Services to review a user's e-mail messages.

(H) Users must not utilize OKDHS e-mail to send non-work related e-mails, known as SPAM.

(I) No e-mail or other electronic communications may be sent which attempt to hide the identity of the sender, or represent the sender as someone else or from another company.

(J) It is strictly prohibited to send unsolicited e-mail messages or chain e-mails.