
POLICY TRANSMITTAL NO. 09-07
INFORMATION SECURITY OFFICE

DATE: MAY 5, 2009
DEPARTMENT OF HUMAN SERVICES
OFFICE OF LEGISLATIVE RELATIONS AND
POLICY

TO: ALL OFFICES

SUBJECT: MANUAL MATERIAL

OKDHS:2-45, Table of Contents; 2-45-1 through 2-45-6; and 2-45-10 through 2-45-12.

EXPLANATION: OKDHS:2-45 regulations are revised to define Information Security Office (ISO) functions and responsibilities; and new regulations are issued to provide OKDHS regulations regarding information security responsibilities for key divisions and all employees, continuity of operations, and required information security terms for contracts.

Original signed on 5-5-09

Mark Gower, Information Security Officer
Information Security Office

Sandra Harrison, Coordinator
Office of Legislative Relations and Policy

WF # 09-A (NAP)

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

INSERT

OKDHS:2-45, Table of Contents

OKDHS:2-45, Table of Contents, 1 page only, revised 5-1-09

OKDHS:2-45-1

OKDHS:2-45-1, 1 page only, revised 5-1-09

OKDHS:2-45-2

OKDHS:2-45-3

OKDHS:2-45-4

OKDHS:2-45-5

OKDHS:2-45-6, pages 1-2, issued 5-1-09

OKDHS:2-45-10, pages 1-3, issued 5-1-09

OKDHS:2-45-11, pages 1-4, issued 5-1-09

OKDHS:2-45-12, 1 page only, issued 5-1-09

SUBCHAPTER 45. INFORMATION SECURITY**PART 1. INFORMATION SECURITY OFFICE OPERATIONS**

- OKDHS:2-45-1. Information Security Office purpose and authority
- OKDHS:2-45-2. Definitions **[REVOKED]**
- OKDHS:2-45-3. ISO requirements **[REVOKED]**
- OKDHS:2-45-4. Emergency operating plan **[REVOKED]**
- OKDHS:2-45-5. Business recovery and resumption **[REVOKED]**
- OKDHS:2-45-6. Information Security Office functions

PART 2. OKDHS INFORMATION SECURITY REGULATIONS

- OKDHS:2-45-10. Information security regulations
- OKDHS:2-45-11. Continuity of operations regulations
- OKDHS:2-45-12. Information security terms for contracts

OKDHS:2-45-1. Information Security Office purpose and authority

Revised 5-1-09

(a) **Purpose.** The Information Security Office (ISO) is charged with managing, overseeing, and auditing Oklahoma Department of Human Services (OKDHS) divisions and business units to:

- (1) evaluate, mitigate, and reduce risks to OKDHS data and information systems, in coordination with the OKDHS risk manager, as appropriate. Assessments are conducted in conjunction with the OKDHS risk manager;
- (2) identify, assess, and appropriately manage information security risks to OKDHS business processes, assets, and information systems;
- (3) assist OKDHS divisions and business units to determine and implement controls that appropriately and proactively respond to information security risks;
- (4) develop, implement, and monitor divisional emergency operating plans agencywide; and
- (5) coordinate with OKDHS divisions and business units to manage, respond to, and mitigate identified information security risks.

(b) **Authority.** Authority is granted to ISO by OKDHS executive management and officers to fulfill the requirements of Section 41.5a of Title 62 and Section 683.2(C) of Title 63 of the Oklahoma Statutes.

OKDHS:2-45-6. Information Security Office functions

Issued 5-1-09

(a) Information Security Program administration. The Information Security Office (ISO) develops, implements, manages, oversees, and audits the Information Security Program to protect and ensure the security of Oklahoma Department of Human Services (OKDHS) data and information systems. The Information Security Program is designed to preserve:

(1) confidentiality, to ensure that information is accessible only to those authorized to have access;

(2) integrity, to safeguard the accuracy and completeness of information and processing methods; and

(3) availability, to ensure that authorized users have access to information and associated assets when required.

(b) Information Security Compliance Unit. The ISO Compliance Unit:

(1) identifies federal, statutory, and OKDHS program security requirements;

(2) coordinates external audits; and

(3) tracks OKDHS compliance with security standards and regulations.

(c) Information Security Audit and Investigation Unit. The ISO Audit and Investigation Unit performs:

(1) required information security regulatory audits internally and to OKDHS contractors, business partners, and third parties who do business with OKDHS; and

(2) investigations of security breaches, disclosures, and allegations of data or information system misuse.

(d) Emergency Preparedness and Business Continuity. The ISO administers the programs that assist OKDHS to manage, recover, and respond to emergencies, incidents, and major business disruptions at offices and information centers, to ensure that OKDHS has the capability to fulfill the agency mission and meet obligations. The components of Emergency Preparedness and Business Continuity include:

(1) **Incident Command System.** The ISO Incident Command System (ICS) provides the:

(A) infrastructure to plan, prepare, respond, and manage OKDHS emergencies, disasters, incidents, and events; and

(B) tool for command, control, and coordination of response efforts in order to stabilize the incident, protect life and property, and enable continuation of delivery of OKDHS services.

(2) **Continuity of Operations Plan.** The ISO provides oversight, management, and support for each OKDHS office or facility to develop the Continuity of Operations Plan (COOP), as required by OKDHS:2-45-11, that will assist in the restoration of core services during a localized emergency.

(3) **Business Continuity Plan.** The ISO provides oversight, management, and support for OKDHS divisions to develop and maintain the Business Continuity Plan (BCP) that encompasses the entire divisional recovery process. The recovery planning process provides a Business Impact Analysis for each division to determine the:

(A) critical business functions and services of the division;

(B) required resources to support critical business functions and services; and

(C) requirements for recovery.

(4) **Disaster Recovery Plan.** The ISO provides oversight, management and support to develop and maintain the Disaster Recovery Plan (DRP). The DRP provides the:

(A) technical recovery plan to support OKDHS Business Continuity requirements; and

(B) recovery capabilities and plans for data and information systems and information technology components.

(5) **OKDHS Be Ready Initiative.** The ISO provides education and awareness initiatives through the federal Be Ready Initiative to promote individual and family security and emergency preparedness.

OKDHS:2-45-10. Information security regulations

Issued 5-1-09

(a) Regulations. All Oklahoma Department of Human Services (OKDHS) information must be protected from unauthorized access, use, disclosure, disruption, modification, duplication, diversion, or destruction, whether accidental or intentional, in order to maintain confidentiality, integrity, and availability.

(b) Scope and applicability. OKDHS information security regulations apply to:

(1) all information collected, maintained, or disseminated by OKDHS;

(2) all information systems used by OKDHS, OKDHS contractors and vendors, and any entity on behalf of OKDHS;

(3) all OKDHS divisions, business units, employees, and business partners; and

(4) contractors and third party entities, where applicable, who host, store, access, develop, use, manage, manipulate, or maintain OKDHS data and information systems.

(c) Controls. Information security controls are implemented through a defense-in-depth security structure that is risk-based and business-driven and provides limited access:

(1) to OKDHS information, based on a least-privilege approach and a need-to-know basis; and

(2) by authorized users, based on only information required for the performance of required tasks.

(d) Effective. OKDHS information security regulations remain in effect until officially superseded or cancelled by the Information Security Office (ISO). No OKDHS division may create a policy that supersedes information security regulations or the Information Security Program requirements.

(e) Information security responsibilities.

(1) Information Security Office. The ISO has overall responsibility and authority for the development and implementation of the OKDHS Information Security

Program, including information security regulations, standards, guidelines, and procedures. ISO responsibilities include:

(A) administer audit and oversight authority to ensure compliance with information security regulations and procedural requirements;

(B) ensure that information security management processes are integrated with the OKDHS strategic and operational planning process; and

(C) ensure that ISO, in coordination with OKDHS executive officers, monitors and annually reports on the effectiveness of the Information Security Program.

(2) **Data Services Division.** Data Services Division (DSD) is responsible for technical implementation and technical administration of the Information Security Program, to comply with OKDHS information security regulations. DSD responsibilities include:

(A) develop and implement additional divisional regulations, standards, guidelines, and procedures, with input from ISO, OKDHS executive officers, and business and system owners;

(B) provide security and awareness training to all DSD staff, and specialized training to staff with significant security or system responsibilities; and

(C) designate staff to directly liaison with ISO to develop and maintain DSD information security regulations, standards, guidelines, procedures, and control techniques.

(3) **Finance Division.** Finance Division is responsible for compliance with the Information Security Program as it pertains to Finance systems and the Finance Data Center. Finance Division responsibilities include:

(A) develop and implement additional divisional regulations, standards, guidelines, and procedures, with input from ISO, OKDHS executive officers, and business and system owners;

(B) provide security and awareness training to all Finance Division staff, and specialized training to staff with significant security or system responsibilities; and

(C) designate staff to directly liaison with ISO to develop and maintain Finance Division information security regulations, standards, guidelines, procedures, and control techniques.

(4) **Information Technology Governance Board.** Information Technology (IT) Governance Board responsibilities include:

(A) designate staff to directly liaison with ISO;

(B) promote the Information Security Program regulations and initiatives; and

(C) actively participate, through the IT Governance Board liaison, in strategic, initiative, and project-based information security planning.

(5) **OKDHS divisions.** All OKDHS divisions are responsible for compliance with the Information Security Program to protect data and information systems over which they have control. Division responsibilities include:

(A) develop and implement additional divisional regulations, standards, guidelines, and procedures, with input from ISO, OKDHS executive officers, and business and system owners;

(B) provide security and awareness training to all divisional staff, and specialized training to divisional staff with significant security or system responsibilities; and

(C) designate staff to directly liaison with ISO to develop and maintain divisional information security regulations, standards, guidelines, procedures, and control techniques.

(6) **OKDHS employees.** OKDHS employees are responsible for compliance with the Information Security Program to ensure the protection of OKDHS data and information systems.

(f) **Sanctions.** Failure to comply with provisions of OKDHS:2-45 may result in disciplinary action, per OKDHS:2-1-7, and could result in civil or criminal penalties.

OKDHS:2-45-11. Continuity of operations regulations

Issued 5-1-09

(a) **Regulations.** Each Oklahoma Department of Human Services (OKDHS) office or facility must develop an emergency operating plan that is followed in the event of tornado, fire, bomb threat, hostage situation, or other emergency.

(b) **Scope and applicability.** The emergency operating plan is:

(1) developed by each office or facility to accommodate the needs of the office or facility;

(2) formatted according to the document template and structure provided by the Information Security Office (ISO);

(3) submitted to ISO for approval;

(4) posted at the office or facility, with a copy maintained by ISO;

(5) made available upon request;

(6) updated and submitted annually to ISO for review; and

(7) discussed with local staff by local management a minimum of twice each calendar year to ensure awareness of the plan and plan activities.

(c) **Definitions.** The following words and terms, when used in this Subchapter, shall have the following meaning, unless the context clearly indicates otherwise:

(1) "**Emergency operating plan**" means the written plan and procedures established to protect staff and visitors of an office or facility in the event of a natural or man-made disaster or emergency.

(2) "**Response**" means providing services to reduce casualties and damage and speed recovery during and after an emergency. Response activities include:

(A) warning;

(B) evacuation;

(C) rescue; and

(D) business recovery and resumption.

(d) **Effective.** OKDHS continuity of operations regulations remain in effect until officially superseded or cancelled by the ISO. No OKDHS division may create a policy that supersedes continuity of operations regulations or the Information Security Program requirements.

(e) **Emergency operating plan.** The ISO requirements for the emergency operating plan submitted by each office or facility include the items in (1) through (7).

(1) Emergency notification and contact list, including:

(A) primary and alternate contacts and phone numbers for responsible staff;

(B) local emergency contacts and phone numbers;

(C) OKDHS Incident Command System phone number, 1-800-789-0752; and

(D) OKDHS direct management contact information, including Office of Communications and area and division management.

(2) Emergency incident procedures for separate evacuation and sheltering in-place plans, including:

(A) posted evacuation routes;

(B) procedures for and locations of assembly areas;

(C) responsibilities for floor and staff monitors;

(D) procedures for accounting for staff;

(E) procedures to determine all clear; and

(F) designation of an alternate site(s) for operations, which requires local planning for use of another facility in the event the primary facility is damaged.

(3) Bomb threat procedures, including:

(A) checklist for the person receiving the call, in accordance with instructions provided on Form 23RS121E, Bomb Threat Aid;

(B) response and reporting procedures, in accordance with paragraph (1) of this Section; and

(C) evacuation procedures, in accordance with paragraph (2) of this Section, with the addition of procedures listed in (i) through (iii) of this subparagraph. Staff must:

(i) visually inspect their work areas and report any unfamiliar or suspicious objects;

(ii) not move or touch any suspicious item or object; and

(iii) leave the area when directed.

(4) Vulnerable clients list, including:

(A) contact information for vulnerable client;

(B) physical address of vulnerable client; and

(C) methods to contact the vulnerable client.

(5) Vital records list, including:

(A) type and location of paper vital records that are onsite;

(B) copies of vital records for backups; and

(C) system and method for re-creating vital records from other documents.

(6) Warning system. The warning system used by the office or facility to notify staff and visitors of procedures for outside evacuation, sheltering in-place, and all clear is:

(A) described in the emergency operating plan; and

(B) tested according to ISO requirements. Any deficiency in the warning system is corrected immediately upon discovery.

(7) Special assistance procedures, including:

(A) list of staff and clients who require special assistance during an evacuation; and

(B) designation of OKDHS staff to direct special assistance procedures for persons not familiar with the evacuation process.

(f) **Business recovery and resumption.** The ISO provides assistance at the time of an emergency to develop business recovery and resumption action plans with short-term and long-term scopes.

(1) The local office provides the needed resources to develop and implement business recovery and resumption action plans. Planning sessions are led by ISO or designee.

(2) The local office maintains and submits to ISO required logs, journals, and history of the incident, according to the schedules provided by ISO.

(3) The ISO or designee, within established time frames, conducts a review of the incident and reports the action plans, results, and impacts to the chief information officer and chief administrative officer.

(4) When deviation from the action plan is required, the local office consults ISO for approval.

(g) **Sanctions.** Failure to comply with provisions of OKDHS:2-45 may result in disciplinary action, per OKDHS:2-1-7, and could result in civil or criminal penalties.

OKDHS:2-45-12. Information security terms for contracts

Issued 5-1-09

(a) **Regulations.** All contracts and agreements entered into or on behalf of the Oklahoma Department of Human Services (OKDHS), where the relationship involves another private or public entity who hosts, stores, accesses, develops, uses, manages, manipulates, or maintains data and information systems owned by or on behalf of OKDHS, must include information security terms to protect the confidentiality, integrity, and availability of OKDHS information or information systems. The OKDHS Support Services Division Contracts and Purchasing Unit ensures appropriate language is included in all contacts and agreements.

(b) **Scope and applicability.** The information security requirements of this Section apply to all OKDHS divisions, business units, and business partners who, on behalf of OKDHS, enter into contracts and agreements with contractors and third party entities, where applicable, who host, store, access, develop, use, manage, manipulate, or maintain OKDHS data and information systems.

(c) **Effective.** Regulations regarding information security terms for contracts remain in effect until officially superseded or cancelled by the ISO. No OKDHS division may create a policy that supersedes these regulations or the Information Security Program requirements.

(d) **Sanctions.** Failure to comply with provisions of OKDHS:2-45 may result in disciplinary action, per OKDHS:2-1-7, and could result in civil or criminal penalties.