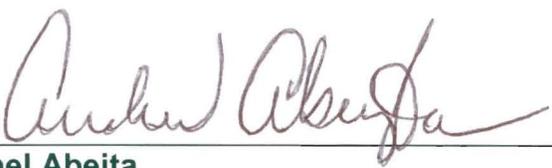


## IARMM TRANSMITTAL SHEET

DOCUMENT IDENTIFICATION NUMBER	SUBJECT	ACTION
Chapter 2, Section 2.3.2	<b>RECORDKEEPING REQUIREMENTS, SAFEGUARDING RECORDS</b>	REPLACE
FOR FURTHER INFORMATION Office of Trust Records 505-816-1607		ISSUANCE DATE 02/22/2010

This release prescribes policy and procedures for safeguarding active and inactive trust and general trust program records for the Office of the Special Trustee for American Indians (OST) and Indian Affairs. Indian Affairs refers to the Office of the Assistant Secretary–Indian Affairs, the Bureau of Indian Affairs (BIA), and the Bureau of Indian Education (BIE).

*for*   
Ethel Abeita  
Director, Office of Trust Records

### FILING INSTRUCTIONS:

**Insert:** On the Trust Portal in the Trust Library under Program Offices, OCIO, Office of Trust Records, Manual

**Effective Date: February 22, 2010**

**Chapter: 2.0 Recordkeeping Requirements**

**Section: 2.3.2 Safeguarding Records**

**Originating Office: Office of Trust Records**

---

### **2.3.2.1 Purpose.**

This chapter establishes policy and procedures for safeguarding active and inactive trust and general trust program records for the Office of the Special Trustee for American Indians (OST) and Indian Affairs. Indian Affairs, as used in this manual, refers to the Office of the Assistant Secretary—Indian Affairs, the Bureau of Indian Affairs (BIA), and Bureau of Indian Education.

### **2.3.2.2 Authorities.**

- A. 5 U.S.C. § 552a, The Privacy Act of 1974.
- B. 25 U.S.C. § 4001, et seq., The American Indian Trust Fund Management Reform Act of 1994, Public Law 103-412.
- C. 44 U.S.C. § 3101 and § 3301, The Federal Records Act, Public Law 81-754.
- D. 44 U.S.C. § 35, The Paperwork Reduction Act of 1995.
- E. 36 CFR, Chapter 12, National Archives and Records Administration.
- F. 43 CFR, Chapter 2, Subpart G, Department of the Interior (DOI) Regulations
- G. 380 DM 3, Files Management (May 9, 1995).

### **2.3.2.3 Policy.**

It is the policy of OST and Indian Affairs to implement procedures for safeguarding active and inactive trust and general trust program records subject to the procedures and guidelines established in 36 CFR, Chapter 12 and to ensure compliance with the Privacy Act and DOI regulations contained in 43 CFR Part 2, Subpart G.

### **2.3.2.4 Responsibility.**

All Indian Affairs and OST programs shall utilize the procedures in this chapter in order to safeguard and protect active and inactive Indian trust and general trust records.

**Effective Date: February 22, 2010**

**Chapter: 2.0 Recordkeeping Requirements**

**Section: 2.3.2 Safeguarding Records**

---

**Originating Office: Office of Trust Records**

---

### **2.3.2.5 Procedures for Safeguarding Records.**

A. Active Indian Fiduciary Trust Records (Active Trust Records). Active Indian fiduciary trust records must be kept in locking file cabinets. Security procedures must be established to ensure and safeguard the confidentiality of information for Indian tribes, Alaska Natives, and individual Indians.

1. Program offices must use locking file cabinets to safeguard active trust records. Prior to ordering file cabinets, ensure that the floor of the building (where the file cabinets are to be located) can support the weight of file cabinets. The program office should take other measures to safeguard trust records such as maintaining the trust records in a room or building with:

- a. Smoke detectors.
- b. Fire alarms.
- c. Water sprinklers.

2. Establish a security control plan for maintaining and accessing active Indian fiduciary trust program records.

a. Label all file cabinets that contain personal, restricted, or sensitive information with a Privacy Act Notice in accordance with IARMM Chapter 1.2.

b. Identify and document the person(s) responsible for maintaining file cabinet keys.

c. All active trust records must be returned and secured in the locking file cabinets at the close of the business day.

d. All locking file cabinets that contain trust records will be locked at the close of each business day.

3. Active trust records should not be removed from trust program offices unless approved by the appropriate supervisor, and documented on the Removal of Active Trust Records Form (IARM Form 2010). Upon return of the trust records, the requester and supervisor will certify, in writing, that the documents have been returned.

Indian Affairs Records Management  
Policy & Procedures Manual

---

**Effective Date: February 22, 2010**

**Chapter: 2.0 Recordkeeping Requirements**

**Section: 2.3.2 Safeguarding Records**

**Originating Office: Office of Trust Records**

---

B. Inactive Indian Fiduciary Trust Records (Inactive Trust Records). The following procedures will be used for inactive Indian fiduciary trust records:

1. Inactive trust records, being prepared for shipment to the American Indian Records Repository (AIRR), do not have to be secured in locking file cabinets at the close of the business day. However, this practice should not exceed 30 working days from the first day of preparation of the records for transfer to AIRR. Inactive files should be sent to AIRR before the 30th day.

2. If inactive trust records need to be maintained beyond their retention period at Indian Affairs and OST offices, a Records Retention Certification Form (IARM Form 2011) must be completed by the program office, and approved by the Office of Trust Records (OTR) Director.

a. Upon approval, all file folders containing records that are retained and are labeled according to the 16 BIA Manual Records Schedule, must be re-labeled in accordance with the applicable current Indian Affairs records schedule. This includes all records that are listed in the certification to the OTR Director. Re-labeling of all file folders must be completed no later than 60 working days of the approved certification by the OTR Director.

b. Inactive records approved beyond their retention by the OTR Director will be classified as active records and should be maintained in accordance with 2.3.2.4.A.

C. Active General Trust Records. The following procedures will be used when securing active general trust records:

1. Store general trust records in file cabinets.

2. Establish a security control plan for maintaining and accessing active general trust records, to include but not limited to the following:

a. Label all file cabinets that contain personal, restricted, or sensitive information with a Privacy Act Notice in accordance with IARMM Chapter 1.2.

b. Identify and document the person(s) responsible for maintaining file cabinet keys.

c. Ensure all active general trust records are returned to file cabinets at the close of each business day.

Indian Affairs Records Management  
Policy & Procedures Manual

---

**Effective Date:** February 22, 2010

**Chapter:** 2.0 Recordkeeping Requirements

**Section:** 2.3.2 Safeguarding Records

**Originating Office:** Office of Trust Records

---

d. Ensure all locking file cabinets that contain personal, restricted, or sensitive information are locked at the close of each business day.

3. Upon approval by the immediate supervisor, records may be removed from the office for meetings, and conducting other business away from the office, when use of the file is necessary.

D. Inactive General Trust Records. If inactive general trust records need to be maintained beyond their retention period at Indian Affairs or OST offices, a Records Retention Certification Form (IARM Form 2011) must be completed by the program office, and approved by the OTR Director.

1. Upon approval, all file folders containing records that are retained and labeled according to the 16 BIA Manual records schedule, must be re-labeled in accordance with the applicable current Indian Affairs records schedule. This includes all records that are listed in the certification submitted to the OTR Director. Re-labeling of all file folders must be completed no later than 60 working days after approval of the certification by the OTR Director.

2. Inactive records approved beyond their retention by the OTR Director will be classified as active records and should be maintained in accordance with 2.3.2.4.C.

E. Safeguarding Records (facility security). Establishing safeguard controls for records will require coordination with federal employees responsible for facility maintenance and security. The following procedures will be implemented in order to assure that Indian Affairs records are secure.

1. Identify the appropriate official at each location who is responsible for facility maintenance and security.

2. Ensure the buildings that store active and inactive trust and general trust records meet minimum security requirements.

a. Request information on the building's security from the Facility Manager who is responsible for ensuring that all building/office lease requirements are in compliance.

b. Document and implement procedures for security controls and external mechanisms to prevent unauthorized access to the building or office. Examples include:

Indian Affairs Records Management  
Policy & Procedures Manual

---

**Effective Date: February 22, 2010**

**Chapter: 2.0 Recordkeeping Requirements**

**Section: 2.3.2 Safeguarding Records**

**Originating Office: Office of Trust Records**

---

i. Periodic patrols by BIA/tribal police or contract security and monitoring by electronic security systems of building(s)/office(s).

ii. Exterior lighting around building(s)/office(s).

iii. Assuring that exterior locking mechanisms on doors have keys and are operational.

iv. Confirming that exterior burglar alarms are operational.

c. Maintain pest prevention by routinely inspecting buildings; control climate conditions; establish food and drink restrictions; perform cleaning regularly; and store food properly. If needed, schedule pest control prevention on a regular basis.

d. Periodically check exterior of building(s)/office(s) to determine the need for maintenance and repair that could result from exposure to the elements.

e. Assuring that smoke alarms and/or water sprinklers are operational and/or available.

F. Records Retention Orders. OST and Indian Affairs shall comply with Records Retention Orders (RRO) issued by the courts. The RROs require that all Indian records, which are relevant to pending litigation, even those considered temporary, must be preserved. Records governed by the RRO cannot be destroyed. This requirement extends to the preservation (including backup files) of Electronically Stored Information (ESI).

1. Every staff member (federal employee, contractor or volunteer) is personally responsible to the court for preservation of these records and relevant information. Staff may be held personally responsible for even the accidental destruction of information within this category. Appropriate disciplinary/adverse action, up to and including termination, may be taken against the staff for destruction (even accidentally), of Indian records or relevant information including ESI.

2. Indian Affairs employees must report all witnessed incidents pertaining to the destruction of Indian records or other information relevant to the RRO to the Regional Records Liaison.

**Effective Date:** February 22, 2010

**Chapter:** 2.0 Recordkeeping Requirements

**Section:** 2.3.2 Safeguarding Records

**Originating Office:** Office of Trust Records

---

3. OST employees must report all witnessed incidents pertaining to the destruction of Indian records or other information relevant to the RRO to the OST Records Retention Order Compliance Coordinator.

**2.3.2.6 Procedures for Performing a Records Risk Management Evaluation.** Risk management is the discipline that ensures an organization does not assume an unacceptable level of risk to records based on the probability and potential impact of each identified threat.

A. Perform a risk analysis using the Risk Management Evaluation Form (IARM Form 2004). This form will assist in identifying the probabilities of risk of loss or damage to records and information:

1. Probable threats from natural, human, or other community disasters;
2. Acts of deliberate destructiveness;
3. Building or equipment failure, malfunction or other catastrophe; or
4. Negligence.

B. Complete a Records and Information Risk Assessment Site Survey Form (IARM Form 2005), by evaluating existing risk to records and information based upon the risk analysis. The risk assessment process involves a review of the physical and environmental security controls.

1. Perform a site survey of the premises to determine potential hazards to records and information due to:
  - a. Geographic location of offices and facilities;
  - b. Physical location of records and information;
  - c. Storage environment, structure, and surroundings; or
  - d. Natural disasters.

C. Perform risk mitigation by taking appropriate action to prevent, or reduce the impact of risks should they occur. These actions may include:

**Effective Date:** February 22, 2010

**Chapter:** 2.0 Recordkeeping Requirements

**Section:** 2.3.2 Safeguarding Records

**Originating Office:** Office of Trust Records

---

1. Identifying a Certified Industrial Hygienist at DOI, Office of Managing Risk and Public Safety, to assist when issues arise with probable risks to human health (e.g. evidence of rodent infestation, excessive mold, viral pandemic). Contact the local BIA safety officer, facility manager, and/or DOI Office of Managing Risk and Public Safety.

2. Ensuring that storage environments are cleaned regularly to remove dirt and debris that attract rodents and insects.

3. Engaging the facility manager in the risk mitigation process to develop cost effective maintenance plans and upgrades to the records storage facilities, as appropriate.

4. Documenting and filing any action taken to mitigate possible vulnerabilities and risks.

D. The Records Recovery Plan is prepared from the completed assessment and analysis in risk mitigation:

1. Devise a recovery plan to address records.
2. Develop scenarios to train staff and to test the plan for effectiveness.
3. Ensure the coordination and assessment of the situation.
4. Determine if external resources are required.
5. Ensure security measures are in place to safeguard records and human health.
6. Keep management informed of activities taken in recovery operations.
7. Review and maintain documentation of recovery operations.

#### **2.3.2.7 Appendices.**

- A. IARM Form 2004, Risk Management Evaluation.
- B. IARM Form 2005, Records and Information Risk Assessment Site Survey.
- C. IARM Form 2010, Removal of Active Trust Records for Official Business.
- D. IARM Form 2011, Records Retention Certification.



## RISK MANAGEMENT EVALUATION

<b>1. Site:</b>					
<b>2. Address:</b>					
<b>3. Completed by:</b>			<b>4. Date Completed:</b>		
<b>5. Probability of Risk:</b>	<b>Possible Risks</b>	<b>Probability High</b>	<b>Probability Low</b>	<b>Effect High</b>	<b>Effect Low</b>
<b>a. TYPE 1: CATASTROPHIC - RARE</b>					
	Earthquake	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Fire:				
	• Wild/Range	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	• Structural	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Flood	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Hurricane	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Tornado	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>b. TYPE 2: SEVERE - SPORADIC</b>					
	Bomb Threat	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Broken Windows	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Broken/Leaky Pipes	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Civil Disturbance/Riot	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Construction on Facility	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Data Security Risk	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Exposed Wires	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Hardware/Software Failure	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Hostage Situation	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Leaky Roof	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Pest Infestation	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Power Failure	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Strong Winds	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Telecommunication Failure	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Viral Pandemic	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Work Place Violence	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>c. TYPE 3: GRADUAL - CONSTANT</b>					
	Cumulative effects of poor environment or neglect	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Deterioration of records (e.g. faded, moldy, water damage)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Inability to locate records	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Theft	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<b>Effect High</b>	<b>Effect Low</b>	<b>6. For a cost effective mitigation plan, focus on preventing the occurrence of, and reducing the impact of, the highest priority risk first. Consider the lower risk categories in the ranking order indicated in the table to the left.</b>		
<b>Probability High</b>	<b>1st Priority</b>	<b>2nd Priority</b>			
<b>Probability Low</b>	<b>3rd Priority</b>	<b>4th Priority</b>			
<b>Example: If there is a <i>high probability</i> of a flood and the event would place records in jeopardy (<i>high effect</i>), then consider the event a 1<sup>st</sup> Priority Risk.</b>					

## INSTRUCTIONS FOR COMPLETING IARM FORM 2004, RISK MANAGEMENT EVALUATION

1. **Site:** Enter the name of the facility where the assessment is being conducted.
2. **Address:** Enter the complete address of the facility (i.e., Office of the Special Trustee for American Indians, 4400 Masthead St. NE, Albuquerque, NM 87109).
3. **Completed by:** Enter the complete name of the person(s) who performed the evaluation.
4. **Date completed:** Enter the date when the evaluation was completed.
5. **Probability of risk.**

**TYPE 1: CATASTROPIC - RARE RISKS.** These types of risks may be rare.

- Column One - Possible Risks:** Check any and all risks that may occur for the site that is being evaluated.  
**Column Two - Probability High:** Check this box if the risk of this event actually occurring is high. Probability of these events may change given the season (i.e., increased risk of wildfire during warmer months).  
**Column Three - Probability Low:** Check this box if the probability of the event actually occurring is low.  
**Column Four - Effect High:** Check this box if this event would place records in serious jeopardy.  
**Column Five - Effect Low:** Check this box if this event would not seriously place records in jeopardy.

**TYPE 2: SEVERE - SPORADIC RISKS.** These types of risks may be sporadic in nature.

- Column One - Possible Risks:** Check any and all risks that may occur for the site being evaluated.  
**Column Two - Probability High:** Check this box if the event actually occurring is high. Probability of these events may change given the season (i.e., increased risk of wildfire during the warmer months).  
**Column Three - Probability Low:** Check this box if the probability of the event actually occurring is low.  
**Column Four - Effect High:** Check this box if this event would place records in serious jeopardy.  
**Column Five - Effect Low:** Check this box if this event would not seriously place records in jeopardy.

**TYPE 3: GRADUAL - CONSTANT RISKS.** These types of risks may need to be monitored on a continuous basis.

- Column One - Possible Risks:** Check any and all risks that may occur for the site being evaluated.  
**Column Two - Probability High:** Check this box if the event actually occurring is high. Probability of these events may change given the season (i.e., increased risk of wildfire during the warmer months).  
**Column Three - Probability Low:** Check this box if the probability of the event actually occurring is low.  
**Column Four - Effect High:** Check this box if this event would place records in serious jeopardy.  
**Column Five - Effect Low:** Check this box if this event would not seriously place records in jeopardy.

6. The probability and effect may be different at any given site and may vary with circumstances or seasonal changes. Priorities for identifying cost effective risk mitigation should focus on preventing the occurrence(s) of and reducing the impact of the risks that have been identified as 1<sup>st</sup> Priority, followed in succession by the 2<sup>nd</sup>, 3<sup>rd</sup> and 4<sup>th</sup> priorities.

**RISK MITIGATION:** To mitigate (lessen) risks to records and information, identify possible existing hazards by using the Risk Management Evaluation Form. Take corrective actions to prevent lengthy downtime or severe damage.



## RISK ASSESSMENT SITE SURVEY

<b>1. ASSESSOR'S INFORMATION:</b>		
a. Contact Name: (Last, First)	b. Phone Number:	c. Date:
<b>2. FACILITY:</b>		
a. Building:	b. Room:	
c. Location of Building:		
d. Type of Building:		
e. Roof Type and Condition:		
f. Approx Room Size:	g. Windows/Doors:	
h. Loft or Mezzanine Storage: <input type="checkbox"/> Yes <input type="checkbox"/> No	i. Locality Risk:	
<b>3. CLIMATE:</b>		
a. High/Low Temperature Range:		
b. Heating: <input type="checkbox"/> Yes <input type="checkbox"/> No	c. Air Conditioning: <input type="checkbox"/> Yes <input type="checkbox"/> No	
d. Humidity Control: <input type="checkbox"/> Yes <input type="checkbox"/> No	e. Temperature/Humidity Monitoring: <input type="checkbox"/> Yes <input type="checkbox"/> No	
<b>4. LIGHTING:</b>		
a. <input type="checkbox"/> Natural <input type="checkbox"/> Fluorescent <input type="checkbox"/> Incandescent <input type="checkbox"/> UV Control		
b. Direct Sunlight: <input type="checkbox"/> Yes <input type="checkbox"/> No      If yes, <input type="checkbox"/> Windows <input type="checkbox"/> Door <input type="checkbox"/> Other _____		
<b>5. SECURITY:</b>		
a. Entry Alarms: <input type="checkbox"/> Doors <input type="checkbox"/> Windows <input type="checkbox"/> Motion Sensors		
b. Fire Alarms: <input type="checkbox"/> Heat <input type="checkbox"/> Smoke		
c. Automatic Extinguishers: Type: _____                              Location: _____		
d. Portable Extinguishers: Type: _____                              Location: _____		
e. Insurance:		
<b>6. VULNERABILITIES:</b>		
a. Fire:	Electrical: Equipment:	b. Heating:
c. Water:	Plumbing: Moisture Accumulation: Building Leaks:	
d. Evidence of Extremes: <input type="checkbox"/> Insects <input type="checkbox"/> Rodents <input type="checkbox"/> Humidity <input type="checkbox"/> Temperature Extremes <input type="checkbox"/> Mold/Mildew		
<b>7. RECORDS/INFORMATION HOUSING:</b>		
1a. Record(s):	b. Media:	
c. Electronic Location:		
d. Electronic Backup:	e. Where:	

f. Enclosure/Container Type:	
g. Housing Type:	
Specialty:	<input type="checkbox"/> Yes <input type="checkbox"/> No
h. Original:	<input type="checkbox"/> Yes <input type="checkbox"/> No
i. Condition:	
j. Problems:	
2a. Records:	b. Media:
c. Electronic Location:	
d. Electronic Backup:	e. Where:
f. Enclosure/Container Type:	
g. Housing Type:	
Specialty:	<input type="checkbox"/> Yes <input type="checkbox"/> No
h. Original:	<input type="checkbox"/> Yes <input type="checkbox"/> No
i. Condition:	
j. Problems:	
<b>8. ELECTRONIC EQUIPMENT:</b>	
a. Type:	b. Info Media:
c. Use:	
d. Brand:	e. Model:
f. Vendor:	g. Serial #:
h. Stand alone: <input type="checkbox"/> Yes <input type="checkbox"/> No	i. Information Backup: <input type="checkbox"/> Yes <input type="checkbox"/> No
j. Backup Method:	k. Location:
l. Problems:	
<b>9. VITAL RECORDS:</b>	
a. Vital records plan in place?	<input type="checkbox"/> Yes <input type="checkbox"/> No
b. Storage site of vital records:	
<b>10. REMARKS:</b>	

**INSTRUCTIONS FOR COMPLETING  
IARM FORM 2005, RECORDS AND INFORMATION RISK ASSESSMENT SITE  
SURVEY**

**1. ASSESSOR'S INFORMATION:**

- a. Contact Name: Enter the site assessor's last and first name.
- b. Phone Number: Enter the site assessor's phone number.
- c. Date: Enter the date when the site assessment was conducted.

**2. FACILITY:**

- a. Building: Enter the name of the building where the assessment is being performed (e.g., Plant 1, John Doe Elementary School).
- b. Room: Enter the room number or a description of the office if applicable (e.g., Accounting office, Room #123).
- c. Location of Building: List the physical address of the building.
- d. Type of Building: List a description of the building that is being assessed (e.g., a 3-story brick building, 1-story wooden frame with metal siding, modular, etc.).
- e. Roof Type and Condition: List the type of roof & its condition (flat roof with gravel, good condition).
- f. Approx Room Size: List the approximate square footage of the room or building (e.g., 300 sq ft, 50,000 sq feet).
- g. Windows/Doors: List location of all windows and doors (e.g., 4 exterior doors, 3 interior doors, 40 windows).
- h. Loft or Mezzanine Storage: Check appropriate box.
- i. Locality Risk: List any risk the building may incur due to its physical location (e.g., flood zone, 5 miles south of nuclear energy plant, etc.).

**3. CLIMATE:**

- a. High/Low Temperature Range: List building's temperature range (e.g., 65° to 95°).
- b. Heating: Check appropriate box.
- c. Air Conditioning: Check appropriate box.
- d. Humidity Control: Check appropriate box.
- e. Temperature/Humidity Monitoring: Check appropriate box.

**4. LIGHTING:**

- a. Natural/Fluorescent/Incandescent/UV Control: Check all that apply.
- b. Direct Sunlight: Check appropriate box(es).

**5. SECURITY:**

- a. Entry Alarms: Check if applicable.
- b. Fire Alarms: Check if applicable.
- c. Automatic Extinguishers: List the type and location (e.g., automatic sprinkler system, 1st floor only).
- d. Portable Extinguishers: List the type and location (e.g., ABC chemical foam, near kitchen).
- e. Insurance: List the type of coverage and also the company that is carrying the policy (e.g., liability, physical property damage with American Liability Insurance).

**6. VULNERABILITIES:**

- a. Fire: List any potential area(s) that may be susceptible to fire (e.g., does not meet current codes, exposed wiring).
- b. Heating: List any heating problems that may exist.
- c. Water: List any problem areas and note the location (e.g., bathrooms, kitchens, leaks, moisture accumulation, etc.).
- d. Evidence of Extremes: Check any and all boxes.

**7. RECORDS/INFORMATION HOUSING:**

- a. Records: List type of records (payroll, trust, general administrative, etc.). You may want to use the information from your Files Maintenance and Disposition Plan.
- b. Media: List the type of media the records are on (e.g., paper, electronic, CD).
- c. Electronic Location: List if this is applicable to the records.
- d. Electronic Backup: List information for the backup records (e.g., what computer, what drive, how often is the backup performed).
- e. Where: List the location of the backup records.
- f. Enclosure/Container Type: List storage unit type (metal filing cabinets).
- g. Housing Type: List the type of housing material of the enclosure (e.g., fireproof, non-fireproof, 4-drawer vertical, 2-drawer lateral, etc.).
- h. Original: List if this is original equipment.
- i. Condition: List the condition of the enclosure(s).
- j. Problems: List any problems with the enclosure(s).

**8. ELECTRONIC EQUIPMENT:**

- a. Type: List the type of equipment (e.g., PC).
- b. Info Media: What type of media are the records stored on (e.g., 3.5" floppy disk, CD, hard drive, etc.).
- c. Use: Describe how the records are used (e.g., payroll, spreadsheets, IIM accounts, contracts, e-mail, etc.).
- d. Brand: List the type of equipment (e.g., Worldwide 4000 Pentium 425).
- e. Model: List the model (e.g., model #WW1050).
- f. Vendor: List the vendor name (e.g., Worldwide).
- g. Serial #: List the serial number.
- h. Stand Alone: Check appropriate box.
- i. Info Backup: Check appropriate box.
- j. Backup Method: List how the backup is stored (e.g., backup through LAN).
- k. Location: List the location of the backup system and tapes (e.g., stored at Backup Storage, Inc.).
- l. Problems: List any problems with the electronic equipment (e.g., no backup in place for hard drive C).

**9. VITAL RECORDS:**

- a. Vital records plan in place? Check appropriate box.
- b. Storage site of vital records. List off-site storage location (physical address, e.g., ABC Storage, 111 Main St., Albuquerque, NM).

**10. REMARKS:** Provide additional comments.



## REMOVAL OF ACTIVE TRUST RECORDS FOR OFFICIAL BUSINESS

### 1. RESPONSIBLE OFFICIAL INFORMATION (Please Print):

a. Date:	b. First Name:	c. MI:	d. Last Name:
e. Trust Program Office:		f. Address:	
g. Telephone:	h. Fax:	i. Cell (Optional):	

### 2. ACTIVE TRUST RECORDS INFORMATION:

a. Schedule or series number:	b. Title and/or subject of file or document:
c. Quantity of documents/files/boxes to be removed:	d. Date(s) trust records will be out of Trust Program Office:

e. Reason for the removal:

f. Certification: I certify that I will exercise all due care to safeguard the identified, active trust records while in my custody.	g. Date:
_____ Signature of Responsible Official	

### 3. APPROVAL:

a. The approving official's signature confirms approval of this document.	b. Date:
_____ Signature of Approving Official                      Title of Approving Official	

### 4. RETURN OF TRUST RECORDS CERTIFICATION/VERIFICATION:

a. Certification: I certify that all active trust records – files or documents have been returned to the official files within the Trust Program Office.	b. Date:
_____ Signature of Responsible Official	

c. Verification: I verify that all active trust records – files or documents have been returned and are accounted for in official files within the Trust Program Office.	d. Date:
_____ Signature of Verifying Official                      Title of Verifying Official	

**INSTRUCTIONS FOR COMPLETING  
IARM FORM 2010  
REMOVAL OF ACTIVE TRUST RECORDS FOR OFFICIAL BUSINESS**

Records Retention Instructions: Retain Removal of Active Trust Records for Official Business Form and copies of all supporting documentation in accordance with GRS 16, Item 7.

**1. RESPONSIBLE OFFICIAL INFORMATION: The requesting official is the responsible official and will complete all items within this section as follows:**

- a. Date: Enter the date request is being made.
- b. First Name: Enter the First Name of the responsible official.
- c. MI: Enter the Middle Initial of the responsible official.
- d. Last Name: Enter the Last Name of the responsible official.
- e. Trust Program Office: Enter the name of the trust program office.
- f. Address: Enter the address of the trust program office.
- g. Telephone: Enter the office telephone number of the responsible official.
- h. Fax: Enter the office facsimile number of the responsible official.
- i. Cell (Optional): Enter the office cell phone number of the responsible official.

**2. ACTIVE TRUST RECORDS INFORMATION: The responsible official will complete all items within this section as follows:**

- a. Schedule or series number: Enter the records schedule and records series number (i.e., GRS 16/7).
- b. Title and/or subject of file or document: Enter the title or subject of the file or document.
- c. Quantity of documents/files/boxes to be removed: Enter the quantity of documents, files, or boxes.
- d. Date(s): Enter the date(s) the trust records will be away from the official file area/location.
- e. Reason for the removal: Enter the reason the trust record(s) are to be removed.
- f. Certification: The responsible official must certify by writing his/her signature.
- g. Date: Enter the date the responsible official signs this document.

**3. APPROVAL: The approving official will sign this document.**

- a. Approving signature: The signature and title of approving official.
- b. Date: The date the approving official signs this document.

**4. RETURN OF TRUST RECORDS CERTIFICATION/VERIFICATION: The responsible and verifying officials will complete this section once records have been returned to the official files as follows:**

- a. Certification: The responsible official must certify by writing his/her signature in this block. The responsible official is certifying that all active trust records (as identified in 2 above) have been returned to the official files.
- b. Date: Enter the date the responsible official signs this document.
- c. Verification: The verifying official must verify by writing his/her signature and title. The verifying official is verifying that all active trust records (as identified in 2 above) have been returned and accounted for in the official files within the Trust Program Office.
- d. Date: Enter the date the verifying official signs this document.



# INSTRUCTIONS FOR COMPLETING IARM FORM 2011, RECORDS RETENTION CERTIFICATION

(Complete one form for each series.)

## 1. RESPONSIBLE OFFICIAL'S INFORMATION:

- a. Date: Today's date.
- b., c. and d. Last name, first name, MI: Complete last name, first name and middle initial.
- e. Title: Enter your position title.
- f. Program office: Enter the program office to include regional office or agency name.
- g. Street address: Enter physical street address.
- h. Office telephone: Enter office telephone number.
- i. Office fax: Enter office fax number.

## 2. RECORDS INFORMATION:

- a. Record schedule or series number: Enter record schedule to include the series number.
- b. Volume (cubic feet): Enter the volume of the records in cubic feet (cubic ft = 1.5 filing cabinet drawer).
- c. Date range: Enter the date range of the records from date open to cut off dates.
- d. Are these trust records? Check applicable box.
- e. Have these records met their retention dates? Check applicable box. If you checked Yes, provide the date these records met their retention date. (Note: Retention date is the date the records have been cut-off and maintained in the office for the specified date indicated in the disposition instructions of the applicable record schedule).
- f. Justification: Justify why these records need to be kept at the program office past their retention date.

## 3. RECORDS HOLDING FACILITY INFORMATION:

- a. Physical location: Enter the physical location of where these records are stored (provide the exact physical street address).
- b. If trust records, are they stored in locking storage equipment? Check applicable box. If not identified as trust records, check N/A for not applicable.
- c. Does the room have the following? Check all conditions that apply.
- d. Are the records stored near overhead water pipes, electrical equipment, excessive heat, and humidity or in locations where rodents have been known to exist? Indicate which conditions are applicable.
- e. Are any of these records at risk through continual use (worn appearance, faded print, brittleness, discoloration of paper torn, marked up, taped, falling apart, water damaged or in last use condition)? Indicate by checking Yes or No if these records are at risk through continual use.
- f. Is there room to store these records in their current location? Check applicable box.
- g. Program manager's certification: Enter the program manager's name. The program manager's signature and date indicate concurrence that the records meet the retention date but are still needed for business operations.

## 4. SUPERINTENDENT CONCURRENCE:

Enter superintendent's name. The superintendent's signature and date of signature indicates concurrence with the program manager's certification.

## 5. REGIONAL OR CENTRAL OFFICE DIRECTOR CONCURRENCE:

Enter regional or central office director's name. The region or central office director's signature and date of signature indicates concurrence with the superintendent or the program manager's certification.