



IRS SAFEGUARD REVIEW REPORT
NORTH DAKOTA DEPARTMENT OF HUMAN SERVICES
ECONOMIC ASSISTANCE DIVISION
SFN 1948 (3-2019)

County Social Service Office	Date of Review	Date Submitted to State Agency
------------------------------	----------------	--------------------------------

RECORD KEEPING REQUIREMENTS

Agencies authorized to receive Federal Tax Information (FTI) are required to establish a permanent system of standardized records of requests made of disclosure of FTI. IRS Publication 1075 & 448 DHS Administrative Procedures Manual.

Describe Agency's Policy for Disclosure of FTI

RESTRICTED AREA - INSIDE THE BUILDING

Objective - to prevent unauthorized access to FTI. The minimum IRS protection standard requires two barriers to access FTI under normal security (secured or locked perimeter, secured area or containerization). The two barrier rule applies to FTI beginning at the FTI itself and extending outward to individuals without a need-to-know.

Restricted area is an area where entry is limited to authorized personnel (individuals assigned to the area). Restricted areas must be prominently posted and separated from non-restricted areas by physical barriers that control access.

The number of entrances must be kept to a minimum and must have controlled access (i.e. electronic access control, key access, door monitor) to prevent unauthorized entry. The main entrance must be controlled by locating the desk of a responsible employee at the entrance to ensure that only authorized personal with official need may enter.

1. Number of Entrances to the Restricted Area <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> Other
2. Describe How the Main Entrance to the Restricted Area is Controlled
3. Is the restricted area posted? <input type="checkbox"/> Yes <input type="checkbox"/> No
4. Type Issued <input type="checkbox"/> Keys <input type="checkbox"/> Key Card <input type="checkbox"/> Key Pad a) Are records maintained on the issuance of keys/key cards or combination locks? <input type="checkbox"/> Yes <input type="checkbox"/> No b) Are periodic reviews conducted to reconcile records and determine if users still need access? <input type="checkbox"/> Yes <input type="checkbox"/> No
5. Individual Responsible for Issuing and Maintaining the Key, Key Card, and Key Pad Records
6. Do visitors to the restricted area complete a visitor access log that includes the name and organization of the visitor, signature of the visitor, form of identification, date, time of entry and departure, purpose of the visit, and name and organization of the person visited? <input type="checkbox"/> Yes <input type="checkbox"/> No
7. Is the access log closed out at the end of each month and reviewed by management? <input type="checkbox"/> Yes <input type="checkbox"/> No
7a. Name of Individual Responsible for Reviewing and Closing out the Monthly Access Log
8. Does the agency have an Authorized Access List (list of individuals that have a frequent and continuing need to enter a restricted area, but are not assigned to the area)? <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> NA a) Does the list contain the name of individual, agency or department name, name and telephone phone number of agency point of contact (POC), address of agency POC and purpose of access? <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> NA b) Is the list updated annually? <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> NA

9. Does the agency have an Authorized Access List for vendors and non-agency personnel? <input type="checkbox"/> Yes <input type="checkbox"/> No a) Does the list include name of vendor/contractor/non-agency personnel, name and telephone number of agency POC, name and address of vendor POC, address of vendor/contractor and purpose and level of access? <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> NA b) Is the list updated annually? <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> NA
--

Minimum protection standards (MSP) require two barriers between the FTI and someone not authorized or without a need to know (i.e. eligibility worker). A locked computer requiring sign-on with multiple passwords does not meet this requirement.

10. Do security personnel or custodial service workers have access to the restricted area after regular office hours? <input type="checkbox"/> Yes <input type="checkbox"/> No <i>PLEASE NOTE - if so, cleaning and maintenance activities must be performed in the presence of an authorized employee.</i> 10a. If yes, is the cleaning and maintenance activities performed in the presence of an authorized employee? <input type="checkbox"/> Yes <input type="checkbox"/> No
--

CONSTRUCTION/SECURITY OF RESTRICTED AREA

1. Materials Used in the Construction of the Restricted Area <input type="checkbox"/> Masonry <input type="checkbox"/> Brick <input type="checkbox"/> Dry Wall <input type="checkbox"/> Other (specify):	
2. Are doors to the restricted area locked and entrances limited to specifically authorized personnel? <input type="checkbox"/> Yes <input type="checkbox"/> No	
3. Do the doors to the restricted area have non-removable hinge pins? <input type="checkbox"/> Yes <input type="checkbox"/> No a) Are non-removable hinge pins to the doors installed on the inside of the room? <input type="checkbox"/> Yes <input type="checkbox"/> No	
4. Are there security measures in place in case of an unauthorized entry into the restricted area? <input type="checkbox"/> Yes <input type="checkbox"/> No	
5. Types of Alarm Systems Currently in Use (e.g. intrusion alarms, motion detectors, exit alarms)	
6. Individual Responsible for Monitoring the Alarms	
7. Are security cameras used? <input type="checkbox"/> Yes <input type="checkbox"/> No	8. Individual Responsible for Monitoring the Security Feed
9. Does your agency have an Intrusion Detection System designed to detect attempts to enter the facility during closed hours? <input type="checkbox"/> Yes <input type="checkbox"/> No - If yes, describe:	

SECONDARY BARRIER TO PROTECT FTI

1. Agency's Secondary Barrier to Prevent Access to FTI <input type="checkbox"/> Locked Office <input type="checkbox"/> Locked File Room <input type="checkbox"/> Locked File Cabinet <input type="checkbox"/> Locked Desk Drawer <input type="checkbox"/> Other (specify):
2. Secondary Storage Location of Keys
3. Individual(s) Who Have Access to the Keys for Secondary Storage
4. Individual(s) Responsible for Maintaining the Backup Keys for Secondary Storage

HANDLING AND TRANSPORTING FEDERAL TAX INFORMATION (FTI)

The handling of FTI must be such that the documents do not become misplaced or available to unauthorized personnel. Only employees who have a need to know and to whom disclosure may be made should be permitted to access FTI.

1. Are your case files stored electronically? <input type="checkbox"/> Yes <input type="checkbox"/> No	2. Does your agency mail case files containing FTI? <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> NA
3. If your agency mails case files, are the files double-sealed, with the inner envelope marked "confidential" with an indication that only the designated official or delegate is authorized to open it? <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> NA a) Does your agency maintain a record of case files mailed? <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> NA	

4. Does your agency transport case files? <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> NA
4a. If your agency transports case files containing FTI, describe agency procedures.

PHYSICAL SECURITY OF COMPUTERS

1. Are computers and computer operations in a secure area with restricted access? <input type="checkbox"/> Yes <input type="checkbox"/> No
2. Describe Agency's Policy Regarding Computer Security While Clients are in the Office
3. Describe Agency's Policy Regarding Computer Security When an Employee Leaves Their Office
4. Do any employees who have access to FTI, work at an alternate work site (home work site, remote terminals, or other office work sites)? <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> NA
5. Do employees working at an alternate work site use multi-factor authentication to access FTI? <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> NA
6. If any employees work at an alternate work site, do their computers containing FTI have full disk encryption? <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> NA
7. If any employees who have access to FTI work at an alternate work site, do they understand they are prohibited from recording, taking pictures of, or capturing screen shots of any SSA-provided information, including but not limited to, cell phones, tablets, laptops, video cameras, security cameras, family members with access to workstations that can view personal identifiable information (PII)? <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> NA

RESTRICTING ACCESS

1. Agencies are required to restrict access to FTI to only those individuals whose duties or responsibilities require access. Who within your agency has access to FTI?	
2. Is FTI copied? <input type="checkbox"/> Yes <input type="checkbox"/> No	If yes, how is case file labeled?
3. If the case file contains FTI, is the information removed before the file is given to clerical or support staff? <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> NA	
4. When inquiring on a IEVs hit, what notice is sent to the client?	
5. Does the notice include any identifying FTI information? <input type="checkbox"/> Yes <input type="checkbox"/> No	
6. Is FTI transmitted using email? <input type="checkbox"/> Yes <input type="checkbox"/> No	6a) If yes, is the email containing FTI properly labeled (e.g. email subject contains "FTI" to ensure the recipient is aware that the message content contains FTI)? <input type="checkbox"/> Yes <input type="checkbox"/> No
7. Is an audit log used to ensure the proper tracking of all emails containing FTI? <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> NA	

EMPLOYEE SECURITY AWARENESS (EAP SAFEGUARDING INFORMATION - eLEARNING)

1. Do new workers receive employee awareness training? <input type="checkbox"/> Yes <input type="checkbox"/> No
2. Does your agency require workers to complete annual training? <input type="checkbox"/> Yes <input type="checkbox"/> No
3. Are employees aware of disclosure restrictions and the penalties for unauthorized disclosure of FTI? <input type="checkbox"/> Yes <input type="checkbox"/> No

DISPOSAL OF PAPER FTI

1. Method of Disposing of Federal Tax Information (FTI) <input type="checkbox"/> Shred <input type="checkbox"/> Burn <input type="checkbox"/> NA	If burnt, how?
2. Name of Agency Staff or Contractor Responsible for the Destruction of FTI	
3. Location of FTI Case Files Until Destruction has Taken Place	
4. Is the disposal of FTI (case files) supervised? <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> NA	If yes, who supervised the disposal?

DISPOSAL OF ELECTRONIC FTI

1. Does your agency destroy FTI furnished or stored in electronic format? <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> NA	2. If yes, who destroys the FTI?
3. Explain how the FTI is Destroyed	
4. Does your agency review, track, document, and verify media sanitation and disposal actions? <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> NA	

Acknowledgment:

I acknowledge that I have reviewed and completed this IRS Safeguard Review Report as part of the IRS Safeguards Internal Inspections Requirement.

SIGNATURE

Signature	Date
-----------	------

Return to Economic Assistance Division