# Internal Inspections Report

# Field office

## Prepared By:

[Insert Agency]

[Insert Agency Address]

[Insert Field Office Location]

[Insert Field Office Address]

[Insert Date]**INSTRUCTIONS**

The following questions serve as an internal audit checklist regarding the agencies security procedures

relating to Internal Revenue Service documents and federal security implementation controls. The purpose of this questionnaire is to measure the agencies level of compliance with federal disclosure regulations.

When answering the questions in this document, the answers should be entered on the line directly below the question. Formatting and color for the answer has already been set, so modifying this it not advisable. The responses will be colored blue, so it’s easily identifiable. For Example:

1. How is FTI received from the IRS?

FTI is received from the IRS via the secure Tumbleweed client to a Windows XP workstation.

After completion, the form should be printed out and signed by the Disclosure Officer and the Director from the Agency.

The Agency should complete the contact information below for all parties that involved in supplying information.

|  |  |  |
| --- | --- | --- |
| **Name** | **Title** | **E-mail** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

It is advisable for the agency to collect and maintain documented evidence to back to answers to this report in the instance of an audit. Having this evidence on hand will also aid the IRS Safeguards on-site review.**Record Keeping Requirements (Publication 1075 section 3.0) IRC Section 6103(p)(4)(A)**

1. How is FTI accessed? (mail, agency application, other-list)
2. Are products/documents created from the FTI data (letters, reports, etc.)? Describe what products/documents are created.
   1. Is the products/documents tracked? If so, how are these products/documents tracked and stored until destruction?
   2. Are the logs retained? If so, how long are the logs retained?

**Secure Storage (Publication 1075 section 4.0) IRC Section 6103(p)(4)(B)**

1. Please describe how the physical security of the Field Office provides two barriers to prevent unauthorized access to FTI?
2. Are Keypads used?
   1. If yes, is each attempt logged?
   2. Who reviews the access attempt logs? (Name and title)
3. What alarm systems are currently running at Field Office? (e.g. Intrusion Alarms, Motion Detectors, Exit Alarms)
   1. Who monitors these alarms? (Name and title)
4. Are security cameras used at the Field Office?
   1. Who monitors the security feed? (Name and title)
5. Are records maintained on the issuance of keys/key cards?
   1. How are records maintained? (automated file, written log, etc.)
   2. Who is responsible for the issuance of keys/key cards (Name and title)
   3. Are periodic reviews conducted to reconcile records and determine if users still need access?
      1. Date of last review.
6. Is FTI safeguarded in accordance with Pub 1075 when in transit (offsite storage, other offices, etc.)?
   1. Is the FTI sent to an offsite storage facility, protected from access by unauthorized individuals at all times? (If the answer is no, offsite storage facility must be reviewed.)
   2. Are employees allowed to work at an alternate worksite? If so, is the FTI at the alternate work site, safeguarded in accordance with Pub 1075?
   3. Is FTI locked in a storage cabinet?
   4. Where is the key kept?
   5. Who has access to the key?
   6. How many keys are in existence?
   7. Who maintains the backup keys?
7. Are combination locks used?
   1. How often is the combination changed?
   2. Who controls the combinations?
8. Are authorized personnel required to wear an identification badge when serving as a secondary barrier for FTI?
   1. Are ID cards/badges required to be worn by employees at all times?
   2. How are ID cards/badges inventoried or managed?
9. Does the agency follow the requirements for visitor access logs for areas containing FTI? If yes, Are visitor logs closed and reviewed at least monthly?
10. Do visitors/vendors sign a visitor access log?
11. What data elements are captured in the log?
12. Who reviews the visitor access log periodically?
13. Are non-authorized visitors escorted?
14. Who has access to the office after core business hours?
    1. How is security enforced after core business hours?

**Restricting Access (Publication 1075 section 5.0) IRC Section 6103(p)(4(C)**

1. Is access to FTI restricted to only authorized personnel who have a need to know?
2. Is all FTI clearly labeled Federal Tax Information? (paper and electronic)
3. Is FTI commingled with other information? If yes, can FTI within agency records be located and separated easily?
4. Has the agency initiated background investigations for all employees and contractors with access to FTI?
5. Is FTI made available to personnel outside of agency personnel (contractors, other agencies, etc.)?
   1. List personnel/offices and provide a justification.
6. Does the agency have web based applications?
   1. Is FTI accessible through a web site?
7. Are personnel following the agency policy for transmitting FTI via email?
8. Is FTI transmitted via email?
9. If yes, how is the FTI protected? (encryption - describe)

1. Are personnel following the agency policy for transmitting FTI via fax?
   1. Is FTI transmitted via fax machine?
   2. If yes, how is the FTI protected?
   3. Where is the receiving fax machine located? (location in office)
   4. Are all individuals in the receiving location cleared for FTI access?

**Disposing Federal Taxpayer Information (Publication 1075 section 8.0) IRC Section 6103(p)(4)(F)**

1. Is FTI paper waste material generated?
   1. Where is paper waste material placed? (recycle bins, locked containers, waste baskets, other container)
   2. Does the agency destroy paper FTI? If yes, how is the paper waste material destroyed?
   3. Does the agency ensure FTI is not disclosed during disposal processes?
   4. Who performs the destruction of paper waste material? (Agency Staff, Contractor – list)
   5. Is a contractor used to pick up the waste material?
      1. Name of contractor:
      2. Where does the contractor take the waste material for destruction?
      3. Does agency staff accompany material and view destruction?

**Cybersecurity Requirements**

1. Does the agency require multi-factor authentication for remote access?
   1. If yes, please explain how.

I hereby submit this Internal Inspections Report to the headquarters function of this agency as part of the IRS Safeguards Internal Inspections requirement.

***/s/***

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_

Field Office Official Conducting Internal Inspection Date

I acknowledge that I reviewed this Internal Inspections Report as part of the IRS Safeguards Internal Inspections requirement and initiated appropriate corrective actions for any deficiencies identified.

***/s/***

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_

Agency Disclosure Officer Date

***/s/***

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_

Agency Official Date