

**Internal Revenue Service Office of Safeguards
Review Prep Questionnaire – (Agency Name)**

Section Three: Data Extracts Received by Agency		
In this section, please select which data extracts (using the drop-down menu) the agency receives and list which divisions have access to the extract. All data extracts are not available to all agencies. If the agency receives an extract not listed below, please attach a separate sheet with the extract name and the divisions that use the FTI.		
Extract	Yes/No	Divisions that use this extract
1099-MISC	No	
Appeals	No	
Business Master File (BMF)	No	
Business Return Transaction File (BRTF)	No	
Corporate Affiliations	No	
CP2000	No	
Examination Operational Automation Database (EOAD)	No	
Exam	No	
Federal Employer Identification Number (FEIN)	No	
Individual Master File (IMF)	No	
Individual Returns Master File (IRMF)	No	
Individual Taxpayer Identification Number (ITIN)	No	
Military Combat Zone (MCZ)	No	
Non-Itemizer	No	
Preparer Tax Identification Number (PTIN)	No	
Taxpayer Address Report (TAR)	No	
Transcript Delivery System (TDS)	No	
Identity Theft Protection Indicator (ITPI)	No	
Levy	No	
SS-8 Notifications	No	
Potentially Dangerous Taxpayer (PDT)	No	
Caution Upon Contact (CAU)	No	
Estate Closing Letter	No	
DIFSLA	No	
BEERs	No	
IRS Taxpayer Address Request – IRC 6103(l)(6)	No	
SSA Wage – IRC 6103(l)(8)	No	

**Internal Revenue Service Office of Safeguards
Review Prep Questionnaire – (Agency Name)**

Section Four: Other Information		
For this section, please answer the questions that apply to the agency. (use the drop-down selections)		
Question	Yes/No/Not Applicable	Explain
1. Does the agency share IT infrastructure, such as hardware or equipment, or FTI data with other state agencies or state organizations?	N/A	
2. Does the agency or state-run consolidated data center own the IT infrastructure used to receive, store, transmit or process FTI? Please provide service level agreement, if applicable.	N/A	
3. Does the agency receive, store, transmit and process FTI in a development, testing or staging environment?	N/A	
4. Does the agency share FTI with nongovernment organizations, such as universities, public interest, research or tribal organizations?	N/A	
5. If “Yes” to Question 4, do they have direct access to systems storing FTI? Describe the level of access allowed. (for example, read only, read and the ability to change/delete data)		
6. Does the agency do any data modeling with FTI, such as forecasting and trend analysis?	N/A	
7. If “Yes” to Question 6, is data modeling done in-house or shared with an external entity, such as a university?		
8. Does the agency share FTI with any contractors? Please list and have contract(s) available for review.	N/A	
9. Describe how your agency maintains IT functions and the services provided (for example, internal IT providing application support with state-run data center providing hardware support).		

**Internal Revenue Service Office of Safeguards
Review Prep Questionnaire – (Agency Name)**

Section Five: Policies and Procedures

If “Yes” for items in this section, please give the policy or procedure date and explain in the column below and attach a copy of the policy with this questionnaire.

	<i>Yes Or No</i>	Policy/Procedure Date and Explanation
<p>1. Does the agency have a current alternative work-site policy? If yes, include information for unattended computers.</p> <p>Per Publication 1075, Section 4.7.3 Other Safeguards:</p> <p>The agency must keep a policy for the security of alternative work sites.</p> <p>The agency will issue rules and procedures to make sure employees don’t leave computers unprotected at any time.</p>		
<p>2. Does the agency have an employee badge policy?</p> <p>Publication 1075, Section 4.2 and Table 3 Minimum Protection Standards:</p> <p>During business hours, if authorized personnel serve as the second barrier between FTI and unauthorized individuals, the authorized personnel must wear picture identification badges or credentials.</p>		

**Internal Revenue Service Office of Safeguards
Review Prep Questionnaire – (Agency Name)**

Section Five: Policies and Procedures

If “Yes” for items in this section, please give the policy or procedure date and explain in the column below and attach a copy of the policy with this questionnaire.

3. Does the agency have a current email policy?

Publication 1075, Section 9.4.3 Email Communications:

Agencies must carry out policies and procedures to make sure FTI is properly protected and secured when transmitted via email.

4. Does the agency have a current fax policy?

Publication 1075, Section 9.4.4 Fax Equipment:

If FTI is prohibited in faxed communications, the agency must write and distribute policy. If FTI is allowed in faxed communications, the agency must only transmit to an authorized recipient.

**Internal Revenue Service Office of Safeguards
Review Prep Questionnaire – (Agency Name)**

Section Five: Policies and Procedures

If “Yes” for items in this section, please give the policy or procedure date and explain in the column below and attach a copy of the policy with this questionnaire.

5. Does the agency have FTI disposal and destruction procedures?

Publication 1075, Section 3.2 Electronic and NonElectronic Logs,

Section 8.3 Destruction and Disposal

Section 8.4 Other Precautions

Section 9.3.10.6 and 9.4.7 Media Sanitization:

Destroy FTI sent to the user and any paper material generated therefrom by burning or shredding. Other methods used must make the FTI unreadable or unusable.

6. Does the agency have an incident response policy?

Publication 1075, Section 9.3.8 Incident Response and Section 10.3

Incident Response Procedures

Agencies must use incident response policies and procedures when responding to an identified unauthorized disclosure or data breach incident.

**Internal Revenue Service Office of Safeguards
Review Prep Questionnaire – (Agency Name)**

Section Five: Policies and Procedures

If “Yes” for items in this section, please give the policy or procedure date and explain in the column below and attach a copy of the policy with this questionnaire.

7. Does the agency have a “piggyback” or “tailgate” policy?

**Publication 1075, Section 4.3.2
Controlling Access to Areas Containing
FTI:**

Agencies shouldn’t allow an individual to “piggyback” or “tailgate” into a restricted location and should document this in agency policy.

**Internal Revenue Service Office of Safeguards
Review Prep Questionnaire – (Agency Name)**

Section Five: Policies and Procedures

If “Yes” for items in this section, please give the policy or procedure date and explain in the column below and attach a copy of the policy with this questionnaire.

8. Does the agency conduct internal inspections and keep records of them? If yes, please give copies of the inspections as well as the inspection schedule.

**Publication 1075, Section 6.4, 6.4.5,
Internal Inspections:**

Agencies must set up a review cycle as follows:

*Local offices receiving FTI: at least every three years

*Headquarters office facilities housing FTI and the agency computer facility: at least every 18 months

*All contractors with access to FTI, including a consolidated data center or off-site storage facility: at least every 18 months

Address key areas including recordkeeping, secure storage, limited access, disposal and computer security.

**Internal Revenue Service Office of Safeguards
Review Prep Questionnaire – (Agency Name)**

Section Five: Policies and Procedures

If “Yes” for items in this section, please give the policy or procedure date and explain in the column below and attach a copy of the policy with this questionnaire.

9. Does the agency keep a plan of action and milestones (POA&M) document?

Publication 1075, Section 6.5 Plan of Action and Milestones:

The agency must carry out a process for making sure they develop and check a POA&M. The POA&M must include corrective actions found during internal inspections and show actions the agency plans to take to resolve these findings.

10. Does the agency have a security policy that covers the following types of training?

- Disclosure awareness
- Security awareness
- Role-based
- Contingency

Publication 1075, Section 6.3 Disclosure Awareness Training

Section 6.2 Training Requirements

Section 9.3.2.2 Security Awareness Training, Section 9.3.2.3 Role-Based Security Training, Section 9.3.6.3 Contingency Training:

Before granting an agency employee or contractor access to FTI, each employee or contractor must certify their understanding of the agency’s security policy and procedures for safeguarding IRS information.

**Internal Revenue Service Office of Safeguards
Review Prep Questionnaire – (Agency Name)**

Section Five: Policies and Procedures

If “Yes” for items in this section, please give the policy or procedure date and explain in the column below and attach a copy of the policy with this questionnaire.

11. Does the agency have a policy for reviewing the Transcript Delivery System (TDS) audit log?

Publication 1075, Section 9.3.1 Access Control

The agency must develop, document and issue policy and procedures to help carry out audit and accountability security controls.

12. Does the agency have a policy for conducting background investigations?

Publication 1075, Section 5.1.1 Background Investigation Minimum Requirements:

The agency must complete a suitability background investigation that’s favorably adjudicated by the agency.

13. Has the agency submitted 45-day notifications for contractors with access to FTI.? Please have the documents available for review.

Publication 1075, Section 7.4, 45-Day Notification Requirements, Exhibit 6, Exhibit 7:

The Office of Safeguards needs advanced notification (45 days) from agencies before they start certain operations or technology capabilities using FTI.