Standard PR.DS: Protection of Federal Tax Information

January 24, 2024

U.S. Department of Education (ED)

Office of the Chief Information Officer (OCIO)

Information Assurance Services (IAS)

Questions about the policies outlined in this document should be directed to Information Assurance Services (IAS) at **IAS_Governance@ed.gov**.

APPROVAL

STEVEN HERNANDEZ

Digitally signed by STEVEN HERNANDEZ
Date: 2024.01.26 17:04:17 -05'00'

Steven Hernandez
Director, IAS/Chief Information Security Officer (CISO)

Revision History

The table below identifies all changes that have been incorporated into this document.

Version	Date	Summary of Changes
1.1	7/31/2020	Initial draft
1.2	8/3/2020	Inclusion of Section on reporting of FTI security breaches
1.3	9/30/2020	Added Safeguards compliance and roles and responsibilities
1.4	10/26/2020	Updated Safeguards compliance and roles and responsibilities to include Management Role, Department Audit Liaison Officer, and FSA Safeguards Team. Additional note added for Incident Response for Federal Tax Information (FTI)
1.5	3/17/2021	Updated document to incorporate feedback received
1.6	5/27/2021	Revised section 1.2 and updated section 2 with Chief Information Security Officer (CISO) and the Senior Agency Official for Privacy (SAOP) responsibilities
1.7	9/8/2021	Updated document to incorporate feedback received
1.8	10/28/2021	Updated document to incorporate feedback received
1.9	1/24/2023	Annual review performed. Updated Section 1.2 and Section 2 m).
1.10	1/24/2024	Annual review performed. Updated Section 2: Standards parts c, d, j, k, l, m, and n.

Table of Contents

1 INTRODUCTION

1.1 Purpose

The purpose of this document is to establish Department of Education (ED) standards for safeguarding the confidentiality of Federal Tax Information (FTI) as required by Internal Revenue Service (IRS) Safeguards Program[1] and IRS Publication 1075, *Tax Information Security and Privacy Guidelines for Federal, State and Local Agencies*[2].

1.2 Scope

The standards established in this document apply to all ED employees, contract personnel, consultants, licensees, and any person or entity accessing ED technology-based information systems which handle, process, or store FTI. Per IRS Publication 1075, FTI consists of:

1. tax data elements, or
2. information derived from a tax return that is received directly from the IRS and in the Department's possession or control.

FTI data is covered by the confidentiality protections of the Internal Revenue Code (IRC) and subject to IRC 6103(p)(4) safeguarding requirements, including IRS oversight.

The key to determining whether a piece of information is considered FTI comes down to the originating source of the information. FTI includes tax return information contained within an individual's tax return, tax data elements that are individualized pieces of tax return information, and not the return itself, received directly from the IRS. FTI also includes any information created by the Department that is derived from federal return or return information received from the IRS.

[1] Safeguards Program | Internal Revenue Service (irs.gov)
[2] https://www.irs.gov/pub/irs-pdf/p1075.pdf

2 STANDARDS

In accordance with Internal Revenue Code (IRC), Section 6103(p)(4)3; and IRS Publication 1075, as a condition of receiving FTI directly from the IRS, pursuant to IRC 6103 or by an IRS-approved exchange agreement, ED must have adequate controls in place to protect the confidentiality of that information and implement safeguards to prevent unauthorized access and use.

a. FTI is categorized as Controlled Unclassified Information/Specified Tax (CUI//SP-TAX)[3] and may contain personally identifiable information (PII). Accordingly, all FTI in the Department's possession must be handled—*at minimum*—in accordance with the confidentiality protections of the IRC and subject to IRC 6103 (p)(4) safeguarding requirements including IRS oversight, per IRS publication 1075 and Department Directive ACSD-OCIO-002, *Controlled Unclassified Information Program*. In addition, all FTI in the Department's possession that includes personally identifiable information must be handled in accordance with all applicable privacy laws, regulations, and policies.

b. FTI may not be masked to change the character of information to circumvent IRC 6103(p)(4) confidentiality requirements. This refers to ED information systems that will handle, store, and manage FTI, and not how FTI or information related to FTI will be disclosed or shared to students, parents, and borrowers.

c. All initial and subsequent requests for FTI and any resulting formal agreements must be approved by the Chief Information Security Officer (CISO) with agreements retained for a minimum of five years.

d. The FSA CISO and FSA Safeguards team are responsible for ensuring that internal inspections are conducted, for submitting required safeguard reports to the IRS, and for any necessary liaison with the IRS.

e. Under the direction of the Department CISO and SAOP, the Office of the Chief Information Officer (OCIO) Audit Liaison Officer is responsible for oversight and management of FTI safeguard reviews, corrective action plans and associated reporting required by IRS Publication 1075.

f. ED information systems that receive, process, store, or transmit FTI must conform to the requirements contained within the IRS Safeguards Program, the current version of IRS Publication 1075 (as amended) and comply with applicable IRS Computer Security Evaluation Matrix (SCSEM) configurations. Wherever there is conflict between the Department's cybersecurity policy and security requirements detailed in IRS Publication 1075, the most restrictive policy must be used.

[3] https://www.archives.gov/cui/registry/category-detail/federal-taxpayer-info?_ga=2.62028652.1553619788.1627933197-1451240049.1627933197

g. Principal Offices requesting or receiving FTI must create and maintain a control overlay that documents IRS Publication 1075 controls and SCSEM configurations which must be implemented in addition to the baseline controls required by the current version of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations*. ED systems that receive, process, store, or transmit FTI must document compliance with the FTI control requirements overlay. Any required controls found to be non-compliant with IRS Publication 1075 or applicable IRS SCSEMs must be tracked and remediated using a Plan of Actions and Milestones (POA&M).

h. Principal Offices must develop, implement, and maintain standard operating procedures to ensure requests for FTI are authorized, controls for ensuring the confidentiality of FTI are ready for immediate implementation upon receipt of FTI, internal inspections are conducted, and reports are provided to the Department CISO and SAOP. The Department CISO and SAOP review internal inspection reports, attest to the validity of the inspection outcome, and deliver the reports to the IRS as required by IRS Publication 1075.

i. Access to FTI is permitted only to individuals who require the FTI to perform their official duties and as authorized under the IRC. Principal Offices must evaluate the need for FTI before the data is requested or disseminated.

j. Principal Offices that intend to disclose FTI to agents or contractors must provide advance notice to the FSA CISO, FSA Safeguards team and SABER PMO, as well as any Principal Office personnel assigned responsibilities for the oversight of programs and personnel with access to FTI.

k. The Department will respond to all known or potential FTI security breaches as breaches of PII with breach response conducted in accordance with ACS Directives ACSD-OCIO-002, *Cybersecurity Policy*, ACSD-OPEPD-002, *Personally Identifiable Information Breach Response Policy and Plan*, FSA SOC Incident Response Standard Operation Procedure (SOP) – Federal Taxpayer Information (FTI) Addendum, and Department standards and procedures that support the implementation of these Directives.

l. The ED Security Operations Center (EDSOC) will coordinate with Principal Office Security Operations Center(s), if required, and will notify the appropriate special agent-in-charge, and the IRS Office of Safeguards all known or potential FTI security breaches as required by IRS Publication 1075.

m. Prior to granting access to FTI or to systems that handle, process or store FTI, Principal Offices must ensure authorized employees and contractors who interact with FTI satisfy IRS Publication 1075 training requirements by completing the Security and Disclosure Awareness Training for FTI and certify their understanding of the Department's cybersecurity and privacy policy and procedures for safeguarding FTI. The most current IRS Publication 1075 training requirements must be satisfied annually as a condition of

maintaining access. For the initial certification, and each annual recertification thereafter, employees and contractors must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of penalty provisions, security requirements, and incident reporting responsibilities. The initial certification and recertifications must be retained by the Department within the Department's authorized learning management systems or other authorized training record repository for at least five (5) years.

n. All access to FTI data and FTI systems is only permitted through the FSA Virtual Desktop Infrastructure (VDI) solution. This user interface is provided by FSA and works to restrict access to authorized users and safeguard all interactions with FTI systems and FTI data.

3 RISK ACCEPTANCE/POLICY EXCEPTIONS

The IRS does not allow agencies to assume risk for FTI data. Deviations from the Department policies, instructions, standards, procedures or memos must be approved and documented through the Department's risk acceptance process. Deviations that include FTI and are governed by IRS Publication 1075 must be submitted through the Department Risk Acceptance Form (RAF), must be approved by the FSA CISO and ED CISO (as delegated) and in coordination with the FSA Safeguards team. Requests must justify the reason for the deviation(s)/exception(s) as well as the compensating security controls implemented to secure the device or information.