# MANUAL TRANSMITTAL

2.2.1

Department of the Treasury
**Internal Revenue Service**

**OCTOBER 18, 2022**

**EFFECTIVE DATE**

(01-01-2023)

**PURPOSE**

(1) This transmits revised IRM 2.2.1, Partnership Control System, Partnership Control System Chapter Overview.

**MATERIAL CHANGES**

(1) Program Scope and Objectives revised to add more detail.

(2) Background, Authority, Responsibilities, Program Management and Review, and Program Controls added.

(3) Updated to remove Official Use Only (OUO) material and replaced with references to IRM 10.8.1 and IRM 10.8.34.

**EFFECT ON OTHER DOCUMENTS**

IRM 2.2.1, dated December 03, 2019, is superseded.

**AUDIENCE**

This document provides instructions for the general use of the operators accessing the Partnership Control Systems display terminals in the SB/SE, LBI, TE/GE, and Appeals Operation Divisions in the Campuses and Area/Industry Offices.

Nancy Sieger
Chief Information Officer

2.2.1
Partnership Control System Chapter Overview

## Table of Contents

2.2.1.1
(10-18-2022)
**Program Scope and Objectives**

(1) The Partnership Control System (PCS) is used to create, monitor and update information related to Partnership and Investor examinations.

(2) **Purpose**: This IRM provides an overview of the Partnership Control System, including general IDRS security information.

(3) **Audience**: Campus Revenue Agents (RAs), Tax Compliance Officers (TCOs), Tax Examiners (TEs) and Clerks working pass-through entities and/or their investors linked on the PCS.

(4) **Policy Owner**: Chief Information Officer

(5) **Program Owner**: Director, SB/SE Examination

(6) **Primary Stakeholders**: SB/SE, Large Business and Industry (LB&I), and Appeals

(7) **Program Goals**: PCS is a database used to create an electronic linkage between pass-through entities and their underlying partners. Linking in some instances is mandatory. Linkage allows for the proper control of statutes and ensures all relevant partners are processed.

2.2.1.1.1
(01-01-2023)
**Background**

(1) PCS was created to monitor and control pass-through entity investors. Pass-through entities can have many partners and many levels of tiering. Tiering occurs when an investor in a pass-through entity is also a pass-through entity. This complexity can make it difficult to keep track of statutes and monitor all the investors.

2.2.1.1.2
(01-01-2023)
**Authority**

(1) PCS control is a policy that was established in response to the partnership provisions of the Tax Equity and Fiscal Responsibility Act (TEFRA) of 1982. It has been expanded to cover other pass-through entities that fall outside of TEFRA.

2.2.1.1.3
(01-01-2023)
**Responsibilities**

(1) The Director, SB/SE, Headquarters, Examination Field and Campus Policy is responsible for:

- Coordinating and Implementing PCS enhancements; and
- Coordinating resolutions for PCS Systemic problems

(2) The SB/SE Program Manager, Examination Field and Campus Policy, Campus Exam & Field Support is responsible for:

- Ensuring that PCS procedural changes and computer program changes are implemented and coordinated with area office and campus examination personnel; and
- Monitoring and evaluating area office and campus examination PCS quality control procedures

(3) The campus PCS Coordinator is responsible for:

- Identifying and resolving technical problems; and
- Identifying and coordinating the resolution of PCS systemic problems

2.2.1.1.4
(01-01-2023)
**Program Management and Review**

(1) **Program Reports**: PCS generates a variety of reports used to monitor the inventory and related statutes. The data source for the reports is the Partnership Information Control File located in Martinsburg, WV.

(2) **Program Effectiveness**: PCS is used to help identify the effectiveness of the Campus Pass-Through Function program. PCS shows the number of investors linked within a pass-through structure. Failing to link partner returns timely can result in barred statutes or the need to follow burdensome procedures such as manual assessments or untimely notice procedures.

2.2.1.1.5
(01-01-2023)
**Program Controls**

(1) IRS will implement access control measures that will provide protection from unauthorized alteration, loss, unavailability, or disclosure of information.

(2) SACS controls all the IDRS user accesses and permissions.

2.2.1.1.6
(01-01-2020)
**Terms/Definitions/ Acronyms**

(1) List of terms and definitions used throughout this IRM section

| | |
|---|---|
| IDRS | Integrated Data Retrieval System |
| SACS | Security and Communications System |
| USR | Unit Security Representative |
| PTI | Production Training Indicator |
| AIMS | Audit Information Management System |
| TSID | Terminal Security Identifier |

2.2.1.1.7
(01-01-2023)
**Related Resources**

(1) IRM 10.8.1, *Information Technology (IT) Security, Policy, and Guidance*

(2) IRM 10.8.34, *Information Technology (IT) Security, IDRS Security Controls*

2.2.1.2
(01-01-2023)
**Partnership Control System Chapter Overview**

(1) This handbook provides instructions for the general use of the operators accessing the Partnership Control System display terminals in the Campuses and Area/Industry Offices.

(2) These instructions provide explicit procedures for entering or extracting data from the Partnership Control System.

(3) The Partnership Control System uses the Integrated Data Retrieval System's (IDRS) Security System. Detailed instructions for the Security System are contained in IRM 10.8.34, Information Technology (IT) Security, IDRS Security Controls.

2.2.1.3
(01-01-2023)
**IDRS Security System**

(1) The Security and Communications System (SACS) provide security and auditing for IDRS.

(2) The IDRS Security System is designed to provide the protection defined in IRM 10.8.1, Information Technology (IT) Security, Policy, and Guidance, and conforms to the various laws and regulations defined in IRM 10.8.34 IDRS Security Controls, Exhibit 10.8.34-3.

(3) The IDRS Security System provides identification and authorization for every input. • The Employee Security File contains significant data required to recognize each employee authorized to use IDRS. • The Terminal Security File includes terminal identification to recognize each workstation capable of accessing IDRS.

(4) All actions taken on IDRS, both authorized and unauthorized, are recorded in the IDRS audit trail.

(5) The IDRS Security System is designed to provide protection to both the taxpayer and IDRS user.

- The taxpayer must be protected from unauthorized disclosure of information concerning their account as well as unauthorized access, inspection, and changes to it.
- The IDRS user employee must be protected from other personnel using their identification to access or make changes to an account.

2.2.1.3.1
(01-01-2014)
**Protection of Taxpayer Accounts**

(1) Taxpayers must be protected from:

- Unauthorized disclosures of account information.
- Unauthorized changes of account information.
- Unauthorized accesses (UNAX) to account information.

(2) Employees should exercise special precautions to identify the taxpayer or their authorized representative when answering inquiries about a refund, notice, adjustment or delinquent account.

(3) When responding to telephone inquiries and walk-in taxpayers about a tax account, the employee handling the inquiry should obtain:

a. Taxpayer's name, address.
b. Taxpayer Identification Number (SSN or EIN).
c. Document Locator Number (DLN), date or amount on notice or other document received.
d. Date and/or amount of refund, adjustment, payment or return.
e. Type of notice or other communication received.

(4) If a caller is unable to furnish enough information to establish that he/she actually is the taxpayer, the employee should request that the caller find out the information and call back. If the caller states he/she does not have the information and cannot obtain it, the employee should advise the caller to write to the IRS office that generated the taxpayer correspondence.

(5) Employees shall not provide Taxpayer Identification Numbers over the telephone. Exception: Employees performing duties which require them to provide Taxpayer Identification Numbers over the telephone will follow their functional IRM guidelines (e.g. Employees staffing Toll Free Phone Applications).

(6) Walk-in taxpayers should not be given tax return information until they have properly identified themselves.

(7) Information concerning taxpayers will not be provided to third parties without written authorization from the taxpayer. This is true even when the third party requesting information has possession of a copy of the bill or notice in question.

(8) Written authorization from the taxpayer is not restricted to a power of attorney or to any specific form. The authorization must bear the taxpayer's signature. If there is serious doubt whether the signature on the authorization is the taxpayer's, offer to mail the information to the taxpayer's address of record.

2.2.1.3.2
(01-01-2011)
**Protection of the IDRS User**

(1) It is equally important that each employee be protected from other personnel using their identification.

a. Users must properly safeguard their login credentials in order to obtain the benefits of the IDRS security system.
b. Users must adhere to established sign-off procedures described in IRM 10.8.34.6.2.2.3.1.

(2) It is essential that only properly authorized employees have access to IDRS.

a. IDRS access must be requested using the BEARS application. Requests must be approved by the user's manager and their Unit Security Representative (USR). IDRS user accounts can only be created by a home campus IDRS Security Officer or an IDRS Security User Administrator. For IDRS purposes, the home campus is the location where the user's IDRS account is managed based on the user's business organization.
b. Changes to IDRS user accounts must be input by either the user's Unit Security Representative (USR), their home campus IDRS Security Officer, or an IDRS Security User Administrator. These changes must be approved by the user's manager and their Unit Security Representative (USR). IRM 10.8.34 IDRS Security Controls defines which changes can be input by a USR and which can only be input by an IDRS Security Officer or IDRS Security User Administrator. IRM 10.8.34 also describes the procedures that must be followed to request changes to user accounts.
c. User profiles should only contain those IDRS command codes necessary to perform their official duties.

2.2.1.3.3
(01-01-2011)
**Authorized Access**

(1) IDRS users are authorized to access only those accounts required to accomplish their official duties.

(2) IDRS users *must not* access their own or spouse/ex-spouse's account, the account of a friend, relative or any account in which they have a personal financial interest.

(3) IDRS users *must not* access the account of another IRS employee unless it is part of their official duties.

(4) IDRS users *must not* access the account of a celebrity, business, or other prominent individual or entity unless it is part of their official duties.