



# MANUAL TRANSMITTAL

Department of the Treasury  
Internal Revenue Service

2.7.1

MAY 20, 2013

## EFFECTIVE DATE

(05-20-2013)

## PURPOSE

- (1) This transmits revised IRM 2.7.1, *Information Technology (IT) Operations, Inter-center*.

## MATERIAL CHANGES

- (1) IRM 2.7.1.1 - Removed references to Service Level Agreements (SLA) and to Channel Extension.
- (2) IRM 2.7.1.3 - Indicated the shifting of duties regarding TSID configurations to EOps SOSD IDRS Security throughout this subsection.
- (3) IRM 2.7.1.3.1 - Clarified that ECC-MEM is a DR site.
- (4) IRM 2.7.1.3.2 - Removed chart of IRSCs and corresponding ECCs.
- (5) IRM 2.7.1.3.4 - Clarified steps for initiating configuration change requests and for routing configuration change request forms; removed various paragraphs and the two figures dealing with ticket procedures.
- (6) IRM 2.7.1.3.5 - Clarified steps for initiating configuration change requests and for routing configuration change request forms; removed various paragraphs dealing with ticket procedures.
- (7) IRM 2.7.1.3.6 - Removed ticket procedures and updated mailbox name to which requests are to be sent.
- (8) IRM 2.7.1.3.7 - Removed FAX as an option.
- (9) IRM 2.7.1.3.8 - Updated list of NESiGates.
- (10) IRM 2.7.1.7.2 (formerly IRM 2.7.1.8.2) - Replaced reference to obsolete IRM 25.10.3 with IRM 10.8.34. in second paragraph.
- (11) Replaced references to ITAMS with KISAM throughout.
- (12) Organizational name changes made throughout.
- (13) Editorial corrections and changes made throughout.
- (14) Removed obsolete subsections.
- (15) Removed several exhibits.

## EFFECT ON OTHER DOCUMENTS

IRM 2.7.1, dated January 1, 2011, is superseded.

## **AUDIENCE**

These guidelines are for Information Technology (IT) staff that perform operational functions in IRS campuses, National Headquarters, User and Network Services, and Enterprise Computing Centers.

Terence V. Milholland  
Chief Technology Officer

Inter-center

## Table of Contents

[illegible]

	#
	#
	#
	#
	#
	#
	#
	#
	#
	#
	#
	#
	#
	#
	#
	#
	#
2.7.1.6 Computer Room Environment	
2.7.1.6.1 Housekeeping	
	#
	#
2.7.1.6.4 System Maintenance	
	#
	#
	#
	#
	#
	#
	#
	#
	#
	#
	#
	#
2.7.1.7 Physical and Cybersecurity of Information Technology Operations	
	#
	#
2.7.1.7.3 Security Awareness	
	#

---

2.7.1.7.5 Privacy/Disclosure Considerations in Computer Applications

#  
#  
#  
#  
#  
#

2.7.1.8 Computer Room Security

#  
#

2.7.1.8.3 Emergency Procedures

#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#

Exhibits

#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#



#  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
#  
#  
  
#  
#  
  
#  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#

#  
#  
#  
#  
#  
#  
  
#  
#  
  
#  
#  
#  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#



#####

#  
#  
#  
#  
  
#  
#  
#  
#  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
#  
#  
  
#  
#  
  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
  
#  
#  
#

#####

#  
#  
#  
#  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
#  
#  
  
#  
#  
#

#####  
#####  
#####  
#####  
#####  
#####

[illegible]

#  
#  
#  
  
#  
#  
#  
  
#  
#  
  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#

#  
#  
#  
#  
  
#  
#  
  
#  
  
  
#  
#  
#  
#  
#  
#  
#  
#  
  
#  
  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
  
#  
#  
  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#



#####

# #  
# #  
# #  
# #  
# #  
# #  
# #  
# #  
# #  
# #  
# #  
# #  
# #  
# #  
# #

# #  
# #  
# #  
# #  
# #

# #  
# #  
# #  
# #  
# #  
# #  
# #  
# #  
# #  
# #

# #  
# #  
# #

# #  
# #  
# #  
# #  
# #  
# #  
# #

[illegible]

#  
#  
#

##  
##  
##  
##  
##

#  
#  
#

#####

#  
#  
#  
#

#  
#  
#  
#  
#

#  
#  
#  
#

#  
#  
#  
#  
#  
#  
#

#

#

[illegible]

#  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
#  
#  
#  
#

#  
#  
#  
#  
#  
#  
#  
#  
#  
#

2.7.1.6  
(01-01-2011)  
**Computer Room  
Environment**

- (1) The environment of the computer room is important for the proper operations of the computer equipment. This includes housekeeping, temperature, humidity and electrical power.

2.7.1.6.1  
(01-01-2011)  
**Housekeeping**

- (1) In an IT environment, good housekeeping practices can be vital to successful operations. Primarily, the computer room is a complex of sophisticated, delicate electronic gear and magnetic media. It is critical to maintain good housekeeping in the areas around the Laser Print Systems.
- (2) The minimum good housekeeping practices that must be maintained are as follows:
  - a. Refrain from eating, drinking, or smoking in the computer room.
  - b. Keep no plants requiring water.
  - c. Refrain from blocking computer air vents with books, printouts or other materials.
  - d. Dispose of carbon paper from printouts or other materials, promptly and properly.
  - e. Retain unmounted tapes in protective straps on the set-up carts or in tape drive pockets/slots until needed.
  - f. Return media promptly to carts when dismounted.
  - g. Refrain from storing boxes, etc., under the computer room floor.

#  
#  
#  
#  
#  
#  
#  
#  
#  
#

#  
#  
#  
#  
  
#  
#  
#  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#

2.7.1.6.4  
(01-01-2011)  
**System Maintenance**

- (1) This section provides management practices and considerations that will be observed to ensure effective maintenance of equipment in all IRS computer facilities. Although the Service uses a complex array of equipment from a variety of vendors, some of which is leased and some purchased, it is fundamental that reliable equipment operation be ensured. Therefore, computer facility management must devote special attention to scheduled and unscheduled maintenance to ensure uninterrupted processing. Continued review of maintenance requirements and history can avoid unnecessary data processing equipment costs.
- (2) The common maintenance classifications and definitions to use are:
  - a. Preventive Maintenance (PM) — maintenance performed by the vendor on a scheduled basis to keep the equipment in proper operating condition.
  - b. Unscheduled Maintenance (UM) — maintenance performed by the vendor when equipment failure has occurred. It is performed as required and on an unscheduled basis.



#  
#  
#  
#  
#  
#  
  
#  
#  
  
#  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
#

---

2.7.1.6.5.1

2.7.1.6.5.2

#  
#  
#  
#  
  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
  
#  
#  
#

2.7.1.6.6.1

#  
#  
#  
#  
  
#  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
#  
#  
#

2.7.1.6.6.2

#  
#  
#  
#

[illegible]

2.7.1.6.7.1

#### 2.7.1.6.7.2

2.7.1.7  
(01-01-2011)

**Physical and  
Cybersecurity of  
Information Technology  
Operations**

- (1) This section provides minimum guidelines to be observed by all IT Services personnel in carrying out their responsibilities for computer room and library security. It makes appropriate reference to other IRMs that contain information required by IT personnel in providing computer room security.

#  
#

#  
#  
#  
#  
#  
#

#  
#  
#  
#

#  
#  
#  
#  
#  
#

#  
#  
#  
#  
#

2.7.1.7.3  
(01-01-2011)

**Security Awareness**

- (1) Computer room and library managers and employees must maintain a high level of security awareness and compliance in the computer room and library. New, recalled, and contract employees must be given a thorough security briefing before they begin their active duties. Security related topics should be discussed by computer managers when they have meetings with their employees.

#  
#  
#  
#  
#  
#

#####

2.7.1.7.5  
(01-01-2011)  
**Privacy/Disclosure  
Considerations in  
Computer Applications**

- (1) In the creation and implementation of any project or program, privacy and disclosure considerations are extremely significant. Whenever there is the slightest chance that a system of records (as defined by the Privacy Act of 1974) is being created, the appropriate Disclosure Manager should be consulted. It is the user's responsibility to ascertain and certify whether or not the project will result in the creation of a system of records. (See IRM 37.2.1, *Privacy Act of 1974; Freedom of Information Act - Privacy Act Of 1974* for Privacy Act publication and reporting requirements and an in-depth discussion of "systems of records.")
- (2) The Communications and Government Liaison Division will ensure the necessary Disclosure Manager review has occurred prior to the creation or implementation of any new project or program.
- (3) The term "systems of records" is defined in the Privacy Act as "any group of records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number or symbol assigned to the individual." A record can include as little as one descriptive item about an individual. For example, a file containing only the names but headed by a label (e.g., Blood Donors) which conveys some information about the people named would constitute a "systems of records."

##  
##  
##  
##

#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
#  
  
#  
#  
  
  
  
  
  
  
  
  
  
#  
#  
#  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
#  
  
  
  
  
  
  
  
  
  
#  
#  
#  
#  
#  
#  
#  
#  
  
#  
#

#####

2.7.1.8  
(01-01-2011)  
**Computer Room  
Security**

#####



#  
#  
#  
#  
#  
#  
#  
#

2.7.1.8.3  
(01-01-2011)  
**Emergency Procedures**

- (1) Local management must establish effective emergency procedures for responses to intrusion alarms, smoke detection alarms, building evacuation alarms, and use of emergency power-down buttons. Post these procedures in highly visible locations in the computer room and computer library. Local management must have a working knowledge of their Occupant Emergency Plan.

#  
#  
#  
##  
#  
#  
#  
#  
#  
##  
#  
#  
#  
##  
#  
#  
#  
#  
#  
##  
#  
##  
#  
#  
#  
#

[illegible]

[illegible]

##  
##  
##  
##  
##  
##  
##  
  
##  
##  
##  
##  
##  
##  
##  
  
##  
##  
##  
##  
##  
##  
##  
  
##  
##  
##  
##  
##  
##  
##  
  
##  
##  
##  
##  
##  
##  
##  
  
##  
##  
##  
##  
##  
##  
##

#####

#  
#  
#  
#  
#  
#  
#  
#

#  
#

#  
#

#

#  
#

#  
##  
#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#



## Exhibit 2.7.1-2 (Cont. 1) (01-01-2011)

		#
		#
		#
		#
		#
		#
		#
		#
		#
		#
		#
		#
		#
		#
		#
		#
		#
		#
		#
		#
		#

[illegible]





#  
#  
  
#  
#  
  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#

[illegible]

page 40 2.7 Information Technology (IT) Operations

#  
#  
#

#

#

#

#

#

#

#

#

#

#

#

††

#

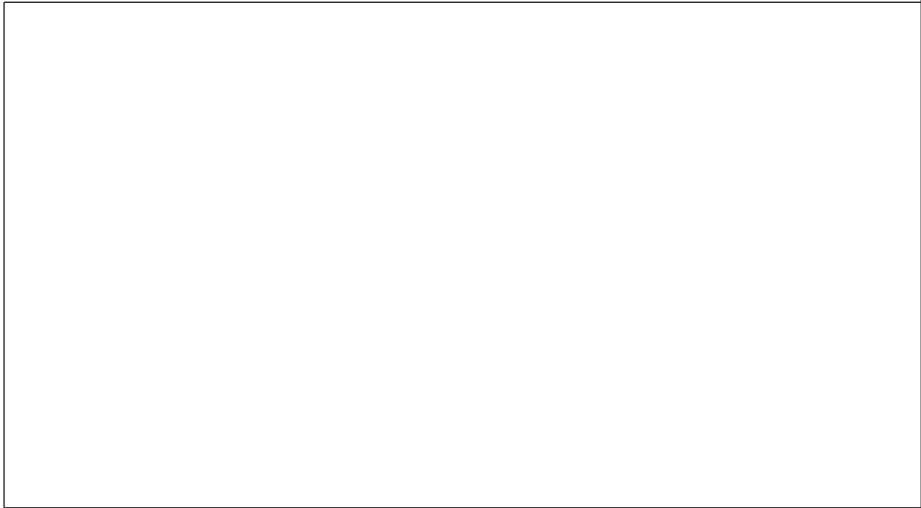
#

##

#

π

..



#####



#

[illegible]

