

IRM PROCEDURAL UPDATE

DATE: 07/08/2026

NUMBER: tas-13-0726-0692

SUBJECT: TAS Internal Controls

AFFECTED IRM(s)/SUBSECTION(s): 13.10.2

CHANGE(s):

IRM 13.10.2.2.4.5 added requirement to CC *TAS IDRS Security when sending Form 11377-E to the Head of Office Designee (HOD).

- (1) TAS managers of IDRS users are responsible for day-to-day implementation and administration of IDRS security in their unit/group.
- (2) All TAS managers who have employees with access to IDRS will:
- a. Review and certify profiles of users with sensitive CC combinations in a timely manner. If the USR is responsible for this action, the manager will ensure that the USR takes all required actions.
 - b. Review and certify users only have IDRS CC based upon the user's profile type. See IRM 13.10.2.2.4.1 (6) . If the USR is responsible for this action, the manager will ensure that the USR takes all required actions.
 - c. Ensure the use of RSTRK Definer U (see IRM 10.8.34-11) to restrict employees with a Research or Research – Quality Review Profile Type.
 - d. Ensure that user profiles are locked when an employee is on leave, in non-duty status, or when the employee will not require IDRS access for 15 to 60 consecutive calendar days (in this case the profile shall be locked on the first day). If the USR is responsible for this action, the manager ensures that the USR takes all required actions.
 - e. Take prompt action to amend the employee access profile or remove the employee from IDRS if they no longer need access, when an employee changes managers or assignments, or leaves the IRS.
 - f. Encourage employees to use the CC LOKME to lock their profiles when they will not need system access for between three and 45 days. If the USR is responsible for this action, the manager ensures that the USR takes all required actions.
 - g. Ensure that primary and alternate USRs and IDRS users complete the required initial and annual refresher training.

- h. Timely review and certify weekly and monthly IDRS Security Reports and take appropriate actions to correct security violations or weaknesses. If the USR is responsible for this action, the manager will ensure that the USR takes all required actions.
- i. Ensure that managers/USRs are not in the same IDRS unit as the users they oversee. Manager ensures that USRs have been appointed to cover all IDRS units.
- j. Ensure that IDRS users who meet the criteria for restricted profile types have the appropriate restrictions added to their profiles. In addition, ensure that IDRS users who no longer have restricted roles have the restrictions removed from their profiles. If the USR is responsible for this action, the manager ensures that the USR takes all required actions.
- k. Ensure IDRS users utilize the Password Management Capability. If the USR is responsible for this action, the manager ensures that the USR takes all required actions.
- l. Advise users with 15 or more systemic sign-offs for the month of the need to properly sign off when away from their workstations. See IRM 13.10.2.2.4.1 (3).
- m. Reinforce IDRS security through discussions at group meetings.
- n. Periodically verify the accuracy and completeness of the IDRS Unit and USR Database for their office using the IDRS Unit & USR Database (IUUD).
- o. Upon receipt of Form 11377-E, Taxpayer Data Access, sign and date the form, return the employee copy to the employee, and send the IRS copy in an email to the HOD with a CC to *TAS IDRS Security along with any supporting documents. Within five business days of receipt, the HOD POC must upload the documents to the Taxpayer Data Access Library. See IRM 13.10.2.2.4.1, IDRS Security, for detailed procedures for Form 11377-E.

(3) Managers are responsible for the activities outlined in IRM 10.8.34.3.2, Manager.

IRM 13.10.2.2.4.7 added requirement to ensure IDRS users have the BEARS entitlement PROD USER IDRS Specific Command Codes (IDRS-CC) prior to adding credit transfer command codes (CCs) to their IDRS profile.

(1) The USR is an individual who implements and administers IDRS security at the IDRS unit level. TAS will appoint primary USRs in accordance with IRM 10.8.34.7.2.8, Unit Security Representative (USR).

(2) TAS shall appoint alternate USRs in accordance with IRM 10.8.34.7.2.9, Alternate USR, to assist and/or perform the duties of the primary USR when that individual is not available.

(3) TAS may appoint temporary USRs and alternate USRs for employees on detail assignments not less than 120 days in accordance with IRM 10.8.34.7.2.8 and IRM 10.8.34.7.2.9.

(4) TAS USRs are responsible for:

- a. Reviewing IORS reports for their IDRS unit in accordance with IRM 10.8.34.7.2.11.1, IORS Primary Report Reviewer; IRM 10.8.34.10.3.1.1, IDRS Online Reports Services (IORS); and IRM 10.8.34.10.3.1.2, Review and Certification of Security Reports in IORS.
- b. Ensuring new and returning users in their IDRS units receive an IDRS security awareness briefing prior to accessing IDRS. See IRM 10.8.34.9.1.1.1, IDRS User Security Awareness Training.
- c. Ensuring users in their IDRS units receive periodic (at a minimum annual) IDRS security awareness briefings. See IRM 10.8.34.9.1.1.1.
- d. Ensuring managers of their IDRS units are fully aware of their IDRS security responsibilities as outlined in IRM 10.8.34.7.1.3.
- e. Completing the required initial and annual refresher training. See IRM 10.8.34.9.1.2.5, Unit Security Representative (USR) and Alternate USR Training.
- f. Monitoring the command code usage of employees with sensitive command code combinations in their profiles. See IRM 10.8.34.10.2.1.6.6, Sensitive Command Codes and Sensitive Command Code Combinations.
- g. Restricting IDRS profiles of LTAs approving manual refunds. See IRM 10.8.34.10.2.
- h. Using RSTRK Definer U (see IRM 10.8.34-11) to restrict employees with a Research or Research – Quality Review IDRS Profile Type. See IRM 13.10.2.2.4.1 (6).
- i. Ensuring IDRS users have an active BEARS entitlement for **PROD USER IDRS Specific Command Codes (IDRS-CC)** prior to adding credit transfer command codes ADC24, ADC34, ADC48, ADD24, ADD34, ADD48, DRT24, DRT48, or FRM34 to their IDRS profile.