

Louisiana Department of Education Security and Confidentiality Policy

DATA SECURITY PROCEDURES

Data security standards define specific requirements for managing and controlling access to the Louisiana Educational Accountability Data System (LEADS) for the electronic submission of the Nonpublic Schools Annual Report. Security goals will be met by requiring all personnel using Louisiana Department of Education (LDE) computer systems to have a unique user access code, called a User ID, and to be associated with a security profile that will control their access to computer resources. The monitoring and control of access to computer resources will be accomplished using automated security software.

Due to ongoing changes in the data processing environment, situations may occur in which the applicability of these standards may be uncertain. In such cases, it is the user's responsibility to seek the proper interpretation of standards through LDE/Information Technology Services (ITS). In no event, shall undefined or unclear standards be construed to imply an access authorization.

These standards apply to all persons who use or have access to LEADS and other nonpublic data resources.

User Access Authorization:

All requests for User IDs to access LEADS will be evaluated by the Nonpublic Security Coordinator to determine whether to authorize access. All User IDs are assigned by the Nonpublic Security Coordinator according to categories of organizations making the requests.

- User IDs are not to be shared among users.
- Users will be held individually accountable for all system access and any violations recorded under their User ID.
- Users must indicate adherence to this *Security and Confidentiality Policy*

Steps Required For LEADS Access by Nonpublic School Administrators:

If you are a new user or you have a User ID from a previous Student Transcript System (STS) reporting system and your personal information has not changed, you will need to be granted authority to access LEADS.

- ✓ Complete form *NP-002 Site Level Security Request Form* (available on the LDE Nonpublic Schools webpage: <http://www.louisianaschools.net/lde/curr/1573.html>)
 - Indicate the nonpublic school information (Site Code, School Name, and Parish)
 - Indicate the reason for the request (to create a new User ID or to delete an existing User ID that is no longer needed)
 - Enter the full name, phone number and e-mail address of the user

“An Equal Opportunity Employer”

- The user must indicate that they have read and will adhere to the policies as listed in this *Security and Confidentiality Policy*
 - Indicate the name of the user and the Principal or Administrator
- ✓ E-mail the completed form to the Nonpublic Security Coordinator listed on the form.
- ✓ The Nonpublic Security Coordinator assigns the appropriate User ID, password, and security profile, and notifies the User by e-mail.

In general, a request for a new User ID will be completed within five working days. Requests for multiple User ID's or mass changes to existing User ID's may require additional time.

User ID Suspension/Revocation:

User IDs will be revoked in any of the following circumstances:

- After five unsuccessful sign-on attempts.
- After five resource access denials in one terminal session.
- At the scheduled end of consulting or temporary labor engagements.
- Upon notice of termination.
- During the investigation of an actual or suspected security violation, if revocation is requested by management.
- On management request or direction.

User ID Reactivation:

If a User ID has been revoked due to sign-on or resource-access denials, the User ID may be reactivated/resumed only by the ITS Security Coordinator after a review of the circumstances and a discussion with the user.

User ID Termination or Modification:

The Principal or School Administrator must notify the Nonpublic Security Coordinator of changes in status for users (i.e. if a user no longer needs access to LEADS due to termination, or job reassignment). Such updates are critical to the security of the LDOE's databases.

Password Management:

Password Reset System (PRS):

Passwords may be reset using the *Password Reset System (PRS)*, a self-service password reset guide. The first time you log onto PRS you will need a valid User ID and password and you will be required to provide the answers to your personal questions. Enter the PRS URL <https://password.doe.louisiana.gov> in your Internet Browser address bar and press enter.

Initial Passwords:

Initial passwords will be set to expire and to force a new password selection on the user's first sign-on. Initial passwords will be communicated to a new user in confidence by e-mail. Users are required to maintain the confidentiality of their passwords and to change their passwords when they suspect that the privacy of their password may have been compromised.

Forgotten Passwords:

If a user has forgotten their password, they must reset it by using the ***Password Reset System (PRS)***. To access PRS, users must enter the PRS URL <https://password.doe.louisiana.gov> in their Internet Browser address bar and press enter.

Password Change Frequency:

All system passwords will be set to expire every 30 days.

Password Change Mode:

Users will be allowed to select their own password within specific rules and/or masks as established with security system password control options.

Password Rules:

Each password will conform to the following rules and standards:

- Minimum password length is four characters; maximum length is seven characters.
- Users may change their passwords once per day. Additional changes must be requested through the ITS Security Coordinator.
- A user selected password cannot be the same as any of the five previous passwords.