ASCENDER Security Administration

ASCENDER contains sensitive information as it pertains to all district, employee, student, and vendor records. LEAs are charged with being a responsible custodian of this important information.

Why is ASCENDER Security Important?

- Reduces potential data breaches
- Prevents loss of revenue
- Maintains privacy compliance under FERPA
- Protects sensitive Personally Identifiable Information (PII) – (Including but not limited to SS #, DOB, Banking info, payroll info, etc.) for employees and students; as well as sensitive district and vendor information
- Supports efficient district operations
- Ensures accurate and auditable documents are maintained
- Keeps district reputation intact

Who is Responsible for ASCENDER Security Administration?

- The LEA/Superintendent appoints Security Administrator(s) who will be solely responsible for the Security Administration Application in ASCENDER
- Keep in mind, Security Administrator permission allows FULL ACCESS to ALL aspects of the ASCENDER system providing designated LEA security administrators rights to manage both the necessary roles and permissions for ALL ASCENDER Business and Student users.
- The LEA/Superintendent should have a process in place to tightly control security and determine who will have system access to maintain compliance with the privacy of student records under FERPA. As well as keeping the integrity of sensitive employee, district, and vendor records. Only school officials with a need to access the records should be allowed ASCENDER access.
- We recommend that you review reports regularly to verify who has Security Administrator access as well as review and update staff roles and permissions. You are responsible for keeping your District's data safe and secure.

What is Required of the Designated ASCENDER Security Administrator?

As the District Security Administrator, it is imperative you review and update staff roles and permissions each year. Permissions should be determined individually based on specific roles and their corresponding responsibilities.

- Responsible for creating, editing, and maintaining user roles and permissions
- Make immediate changes to security as needed when personnel enter, leave, or change positions (create new roles, edit an existing role, manage permissions across multiple roles, delete roles)
- Additionally, various reports are available to assist with assessing audit information.

Please contact the Data Services Department for more information or questions concerning ASCENDER Security.