Business - Security Audit Checklist

This list should be completed at least once a year. We suggested at the beginning of each new school year. The System Administrators should complete this checklist. As Security Administrator, you have complete access to ASCENDER.

- The LEA/Superintendent will appoint Security Administrators who will be responsible for the Security Administration Application in ASCENDER
- The LEA/Superintendent should have a process in place to tightly control security and determine who will have system access.
- The Security Administrators are responsible for creating, editing, deleting, restoring and maintaining roles and users.
- The Security Administrators will need to make immediate changes to security as needed when personnel enter, leave or change positions.

District Admin:

______ Verify District Session Timers are set according to district policy

______ Verify Login Preferences are set according to district policy

Security Administration

______*Verify Security Administration Users (We recommend one Business Facilitator and one Student Facilitator)

(See page 59-60 of the ASCENDER Business Security Administration document.)

______ Add new roles for next school year if needed.

______ Edit existing roles for next school year as needed.

______ Add new users per Access Request Form

______ Edit existing users per Access Request Form

______ Verify all current users are still employed at the district, if not remove

______ Run Report – List of Users by Permissions

______ Have superintendent verify all permissions for all users are still correct

______ Edit/ Delete existing users as per superintendent

District Admin. - Users

______ Verify District Administrative Users

______ Run report – District Admin>DA00001 - Verify

______ Edit/ Delete existing users as per superintendent

Completed by: ____ Date: ____________________

Superintendent:____ Date: ____________________