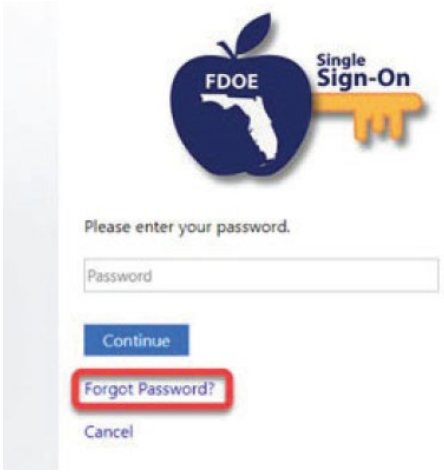
Data Security Best Practices for DOE Systems (Single Sign-On SSO, Provider Portal, QPS)

Account Security:

1. Unique Accounts: Each user of DOE systems (SSO, Provider Portal, QPS) must have their own unique account to protect privacy and security.
2. Strong Passwords:
    - Use strong, complex passwords containing a mix of lowercase and uppercase letters, numbers, and special characters.
    - Passwords should never be shared or written down.
    - If you have forgotten your SSO password, please refer to Password.Recovery.in Provider. Portal.User.Guide for instructions on how to reset.
    - Resetting your password is self_service. Please refer to Password.Recovery in Provider. Portal.User.Guide for instructions on how to reset.



3. Regular Password Updates: Change passwords periodically to maintain security.
4. Multi-Factor Authentication (MFA):
    - Each user of DOE systems (SSO, Provider Portal, QPS) must have their own MFA attached to their unique user ID and password.
    - Choose an MFA method (phone number, email, authenticator app) that you can consistently access.
    - Understand that MFA will be required for each login.

System Usage:

5. Log Out Regularly: Log out of Provider Portal SSO at the end of each session to prevent unauthorized access.
6. Secure Workstations:
    - Lock your workstation or log out whenever it is unattended.

- Enable password-protected screensavers to engage after 10 minutes or less of inactivity.
- When a workstation is left unattended, even for a short time, sensitive information displayed on the screen becomes vulnerable. A password-protected screensaver effectively locks the screen, preventing unauthorized individuals from viewing or accessing that information.

Data Access and Responsibility:

7. Role-Based Access: Staff should only have access to information necessary for their specific job duties.
8. Regular Access Reviews: Regularly review user access to ensure it remains appropriate and aligned with current job duties.
9. Compliance with Policies: Providers are responsible for complying with all state, federal, and local laws, as well as the Florida Department of Education (FDOE) policies regarding information technology use and security. See below links to applicable statutes, codes and regulations.
10. Understanding Security Policies: Users are responsible for reading and understanding FDOE security and privacy policies.
11. Compliance with Contracts: School Readiness (SR) and Voluntary Pre-K (VPK) contracted providers are responsible for complying with the Statewide SR Provider Contract and/or the Statewide VPK Provider Contract. See below links to applicable statutes, codes and regulations.
12. Adherence to FDOE Policies: FDOE security and privacy policies must be always followed when using or connecting to FDOE data resources.

Incident Reporting and Account Management:

13. Staff Terminations: Providers must promptly notify the ECS Help Desk when a staff member with access is terminated.

Applicable Statutes, Codes and Regulations :

Cybersecurity, Section 282.318, Florida Statutes (F.S.)

Education Records, Section 1002.22 F.S.

Records of Children in the VPK Program, Section 1002.72 F.S.

Records of Children in the SR Program, Section 1002.97 F.S.

Assessment and Accountability, Section 1008.39 F.S.

Public Records, Chapter 119, F.S.

Computer Related Crimes, Chapter 815, F.S.

Family Educational Rights and Privacy Act (FERPA)

SFCS, Chapter 60GG-2, Florida Administrative Code (F.A.C.)