SC DEPARTMENT OF EDUCATION

Privacy Program Strategic Plan Executive Summary

Office of Information Security and Privacy
January 24, 2025

The privacy office encourages the implementation of this strategy that has been developed using widely trusted frameworks, standards, and controls to clarify responsibilities, improve program deliveries, and facilitate better communications when conducting regularly programed data protection, risk, and compliance assessment services across the agency and school districts. The Chief Privacy Office has developed the following Privacy Program Strategic Plan:

1. Operational and Program Management for Information Systems

   - SCDE's policies and procedures require that any acquisition of information related products and services, as well as major updates to its system development life cycle, address privacy operational roles and requirements.

   - Implementation steps will include:

     - CPO is designated as the individual responsible for policies relating to data use and privacy.

     - CPO will collaborate with the division [i.e. mission/business process level, tier 2] or their assigned director [i.e., data/information owner] to identify, understand within the context and purpose of the processing, and then assess the appropriate use of personal information within the existing or a planned information system architecture by using the applicable National Institute of Standards and Technology (NIST) Frameworks (e.g., NIST Privacy Framework, NIST SP 800-53r5, 800-39, 800-37r2, etc.) to recommend adopting additional/updated policies.

     - CPO will, if findings determine that the likelihood and severity of a privacy event arising to where the privacy risk and organizational risk intersect (e.g., becomes a problematic data action), provide recommendation to the executive risk officer (e.g., Chief of Staff (COS)), to better enable the enterprise [i.e., organization level, tier 1] risk response decision.

     - CPO will assist the program director/information owners with completing/re-evaluating their business process by using the enterprise privacy impact assessment (PIA) tool (currently RSA Archer GRC Application) to complete their privacy impact assessment, which will also be used to monitor overall organizational readiness based on agency objectives and priorities set at tier 1 and through collaborations at tier 2 to incorporate the implementation.

- CPO is incorporated early enough in the planning phase, or not later than during the agency routing review approval process for any acquisition of information/data related products and services, as well as major updates to its system development data life cycle to ensure privacy by design strategies are considered.

2. Privacy Incident Management

   - SCDE's data governance and data protection policies and procedures require that agency management ensure compliance with privacy incident management requirements.

   - Implementation steps will include:

     - CPO will use the SCDE Data Governance Committee (DGC) structure to govern data protection activities and will chair the Privacy Incident Response Team (PIRT) Advisory Group (PAG). The PAG core members include (i.e., COS, General Counsel, CIO, CPO, CISO, the Division Deputy Superintendent experiencing the incident or potential privacy data breach, and any appropriate ancillary member as necessary). This group will convene based on clearly defined responsibilities, procedures, and activity frequencies.

3. Privacy Risk Management

   - SCDE's risk management policies and procedures require that agency management ensure that PIAs are completed every three years and updated with any substantial changes to the information system or business process to address privacy protection requirements.

   - Implementation steps will include:

     - CPO will chair the DGC Risk Management and Compliance Subcommittee/Group (RMCG), which is also chartered to function as the PAG. The RMCG will review and assess privacy risks related to SCDE IT systems and application requests for proposals (RFPs), procurement requests and data related business contracts, and significant changes to business processes involving data usage. The RMCG will work with SCDE leadership and business owners/program directors to determine acceptable levels of risk to the organization. The RMCG will review incident responses, procedures, and outcomes.

     - CPO will assist the program director/information owners with completing/re-evaluating their business process by using the enterprise privacy impact assessment tool. The CPO will update PIAs when a system change creates new privacy risks (e.g., when functions applied to existing information collection change anonymous information into information in identifiable form).

4. Privacy Awareness and Training

   - SCDE's talent workforce and engaged third party policies and procedures require annual information privacy awareness and training for all employees.

- Specific employees who actively perform student data processing activities will receive routine training to address privacy roles and responsibilities.
- Implementation steps will include:
    - CPO will collaborate with the division or their assigned director to conduct privacy workshops for data stewards and other stakeholders to offer ongoing support in helping offices improve their data protection and privacy awareness levels within their business processing activities. The role-based training will be developed in-house to focus on SCDE privacy related functions/roles.

5. Accountability
    - The CPO will review and report on the progress of this plan on an annual basis to the State Superintendent of Education, prior to the last day of each fiscal year.
    - Implementation steps will include monitoring/reporting regarding:
        - Privacy Maturity Model
        - Incident Response Metrics
        - Privacy Impact Assessments
        - Training and Awareness Metrics
        - Data Subject Access Requests Metrics

Disclaimer:
For questions or clarification regarding this information, please email privacy.office@ed.sc.gov