Idaho State Department of Education Direction and Policy

Prelude

The Idaho State Department of Education (SDE) is a public trustee to private and confidential data regarding some of the most vulnerable of our public. This is a sacred trust and requires that, we as sentinels of that trust provide the tools, policies, and direction that will safeguard the privacy and possibly even the safety of those children. If for no other reason than this, SDE Technology Services will do what is necessary to inform, educate, and enable the users of the system to safeguard that private data.

We recognize that security is a moving target. That which may have been adequate in the past is no longer sufficient to fulfill this mission. We will not let a stagnant metaphor or apathy determine the level of excellence to which we must ascend. Functionality, security, and traceability are the measures by which our work will be judged, first by ourselves, and then by those we serve.

Direction and Policy

A. We require accountability, traceability and non-repudiation for entered data.
    a. Each user will have their own credentials for accessing data.
    b. Users will not need multiple logins to access different applications.
    c. Users will only be allowed to access data that is necessary for their roles and scope of authority.
    d. Changes to data will be logged with the user's identity and time.
    e. Historical records will be flagged rather than physically deleted from systems.
    f. User passwords not stored in clear text and are either:
        i. Encrypted with secure keys and algorithms
        ii. Hashed using one-way encryption and secure algorithms
    g. We do not create our own "obscure algorithm" security mechanisms, but rely upon proven industry standard security mechanisms.
B. Authorization is delegated to the administrator of nearest responsibility.
    a. User rights assignment will be a function of the immediate administrators of the program and scope.
C. Authentication and user management is delegated to lowest reasonable level.
    a. Use the federated authentication model where possible.
    b. Provide tools for user provisioning and revoking to local administrators.
    c. Provide self-service tools to users where possible.
D. Individual-level data is secured based on user role and scope.
    a. Public identifiers are **never** used as data keys
        i. Social Security Number
        ii. Drivers License Numbers
        iii. EDUID (SDE Person Identifier)

iv. School Employee or Student Identifiers
v. Names or name derivatives
vi. Ethnicity, race, gender, etc.
vii. Physical or electronic locations (address, email, phone numbers)

b. External public identifiers (i.e. Social Security Numbers) and other private data are encrypted or hashed depending upon the reporting requirements associated with them.
c. We segregate data elements into different data scopes with different security attributes to provide role and scope security for individual data.
d. Personal identifiers are not included when data is exported for approved purposes such as research or trend analysis except where required by law or where the identifying data is provided as the means of retrieving the records.

E. Applications are developed using approved methodology and technologies.
   a. Standard libraries for security, user authentication, and data access shall be used and updated to reflect new security, stability, performance, and other requirements.
   b. Quality assurance reviews for functionality, architecture, policy conformance, performance, and security shall be performed prior to deployment.
   c. Applications shall be developed by more than one developer.
   d. Application deployment shall require approval/cooperation of more than one individual.
F. Data integrity shall not be knowingly compromised.
   a. SDE is a custodian of Program, District, and School data.
   b. We provide reasonable and necessary checks and balances to warn users that data may be invalid, but the ultimate validation responsibility lies with the system users.
   c. We monitor our systems for evidence of maliciousness or ineptitude and take appropriate actions.
   d. We perform backups and other data and system maintenance functions as guided by industry best practices.

Implementations

Authorization Infrastructure

SDE has created an object-based authorization library and database in order to allow applications to perform user authorization functions. This library was created with the express needs of managing the thousands of users and tens of thousands of objects (people, classrooms, schools, and districts) and their permutations. We are implementing a distributed management system where both the role (actions to be performed) and the scope (objects to act upon) may be assigned, viewed, reviewed, and verified. This infrastructure has been under development for over a year, and is already being used a few pilot applications. It will be used in all new or replacement applications as they are deployed.

Longitudinal Data Schema

SDE has created a database model with sufficient abstraction to encompass the general needs of all programs within the scope of the Department of Education. This database model consists of a core database containing the common characteristics to all programs and extension databases where

specialized data is stored. Under this model, relationships between various individuals and programs are maintained, and detailed information required by implementations of specific programs is also supported.

Architecture Standardization

SDE has embraced an industry standard toolset and platform for developing our software applications. We have further created and maintain our own project templates and libraries based on this platform so that all applications we develop are similar to each other, not just in appearance, but in architecture. This allows us to leverage experience, training, and industry resources (consultants and training) to maximize the efficacy of our software developers.

Privacy and Encryption Infrastructure

SDE uses industry industry-standard encryption libraries and key strengths in order to secure personally identifiable confidential data. Encryption keys to production data are secured in “key vaults” and not available to individuals for use. Keys are used in conjunction with “salt” values to ensure that the encryption data alone is insufficient to calculate encryption keys. Encrypted data is never decrypted in bulk, but only by individual record. All access to encrypted data is logged by user, action, record, and date/time. These logs are monitored for abuse.

Deployment Infrastructure

SDE uses a redundant and scalable infrastructure for the housing of our production applications and data. This infrastructure provides the necessary redundancy, reliability, and fault tolerance needed to reliably support our customers.

Continuous Process Improvement

SDE has a stated philosophy of “just a little better, every single day”. This pragmatic approach has allowed us to move towards the previously stated directions without requiring our customers to endure catastrophic changes to their processes. We will not require change of our customers simply for the sake of change; however, we do require our customers to change with us as we move towards these attainable and worthy goals.

Feedback

We welcome constructive suggestions and feedback regarding our direction, policy, and tools.