Data Administration Agreement - Encryption of Student ID in the Office of Planning and Budgeting Database

Purpose

To document an agreed upon approach towards safeguarding personally identifiable student information in the Office of Planning and Budgeting (OPB) database. This does not deal with the need to de-identify student information to meet the requirements of record retention schedules at the University of Washington which will be addressed in a separate document.

Overview

The OPB maintains an Institutional Data Repository of data which includes student attributes. It receives sensitive academic and financial aid data from the source systems in order to perform longitudinal analysis. Data Custodians from the OPB, Registrars Office, Student Financial Aid Office and the Office of Information Management (OIM) recently met to discuss concerns regarding record retention and privacy. As a result of that meeting it was agreed that the OPB would create new controls which encrypt the student identity attribute and the Office of Information Management would review those controls and report on their effectiveness. The next section highlights the observations and recommendations resulting from the OIM evaluation.

Observations and Recommendations

1. The encryption of the student identifier provides another level of obfuscation that makes it harder (but not impossible) for general end users of the OPB database to link back to records in the source system. (An end user could deduce a specific identity based on gender, DOB, and other parameters if the population of students was small and the end user had identity information from other sources.)

2. The encryption method being used by OPB uses standard Oracle database functions that are industry standard and “strong”. They are applied by the OPB Database Administrator (DBA).

3. A cipher key (a mnemonic created by the DBA) is used inside the function to perform the encryption.

4. The function, in which the cipher key is contained, is itself encrypted using standard Oracle database procedures. The DBA, as the only user having Oracle system administrator privileges, can decrypt the Oracle function and reveal the cipher key. Only the DBA of the Oracle database, has the ability to call the encryption/decryption functions.

5. The Director of Institutional Studies has indicated that there are temporary ad hoc business processes in which there is a requirement to decrypt and determine the specific student identifier in its native form. These requirements exist when the data from the OPB database needs to be joined on data from the UWSDB and EDW where data values are not encrypted. In these instances the DBA will either:
   a. Provide a view of the joined data but not display the encrypted data values, or

Document Location: https://www.washington.edu/provost/oim/dmc
Questions regarding this document should be emailed to: dmc-support@u.washington.edu
b. Provide a view of the decrypted values for the smallest known set of instances required.

6. Read rights to these views will be restricted to the specified end users for a limited time period necessary to meet needs. OPB agrees to destroy the views as soon as possible once the business need is completed.

7. A decryption process will need to be performed when OIM is ready to migrate the Oracle database to the Enterprise Data Warehouse (EDW). It is assumed that the EDW will apply similar or additional measures that will provide stronger controls.

8. No review of other system security measures was performed by OIM. Only the encryption and un-encryption processes were reviewed. It is recommended that UW Internal Audit provide additional review of best practices.

**Concurrence**

The undersigned concur with observations and recommendations in this data administration agreement document. They understand the implied risks and endorse the use of student data in the OPB database when the practices outlined in the agreement are performed.

Signature
University Registrar
(Data Custodian)  

Signature
Director, Financial Aid Office
(Data Custodian)

Signature
Director, Office Institutional Studies
(Data Custodian)

Signature
Associate Vice Provost, Information Management
(Data Trustee)