Access to Enterprise Data Warehouse by Application Development Project Teams

**Purpose:** This statement establishes guidelines for managing access to Enterprise Data Warehouse (EDW) data by application project team members.

**Applies To:** Employees on application teams whose applications consume EDW data.

**Issued By:** Data Management Committee

**Administered By:** Application teams, UW Tech.

**Problem Statement**

1. According to current policies, applications access EDW data through application specific system accounts. These circumvent EDW data access controls (DAC), providing various levels of direct access up to “read-all” for some applications.

2. Application development project team members access EDW data through the data access control layer in an assigned ASTRA security role. Roles are assigned in accordance with the employee’s job responsibilities. This means that access privileges for applications are broader than the privileges of application development project team members. This leads to inconclusive or skewed results during application development and testing.

   Note: The two ASTRA roles that provide unrestricted access to all EDW data ("Support" and "Audit") are reserved for EDW support personnel and auditors. Application development project team members are typically assigned the role "Analyst".

**Options**

1. Assign application developers an unrestricted ASTRA role, such as “Support” or “Audit”. This means that data access privileges for developers mirror privileges for applications, but it also means that individual’s role assignments may not match job responsibilities according to ASTRA role descriptions.

2. Maintain a separate access control solution for application development project teams.

3. Establish data access control guidelines and policies for system access to EDW data and implement technical solution.

**Recommendations**

1. Long-term: Establish data access control guidelines and policies for system access to EDW data and implement technical solution.

2. Interim: Maintain a separate access control solution for application development project teams.

   *Proposed details Interim solution:
a. Establish **one Nebula 2 group** per application development project, in addition to the application specific system account(s) for the application.
b. These Nebula 2 groups and system accounts provide access to the data directly and do not go through EDW security layer.
c. Membership of the nebula 2 group is restricted to current members of the application development project teams and limited to project duration.
d. Group members connect with their personal log-in information. This guarantees individual identification through individual passwords.
e. The project manager for each application is responsible for auditing and managing membership of these nebula2 groups.

**Concurrence**

The undersigned concur with the proposed change in data access described in this Data Management Guideline.

Data Custodian Signature: William York  
Printed: Djm  
Title:  
Date: 3/1/2010

Chair of DMC Signature: Elizabeth Wilson  
Printed: Libraries  
Title:  
Date: 3/1/10


Questions regarding this document should be emailed to: dmc-support@u.washington.edu