

UW DATA MANAGEMENT COMMITTEE (DMC)

Security Access and Roles Privilege Matrix for READ-ONLY Access to Enterprise Data Warehouse Data – Version 20

Approved By: DMC Access & Roles Task Force Approved Date: June 11th, 2011
 Modified By: Bill Yock Last Modified : June 11th, 2011

This Role Privilege Matrix describes how data access is administered in the UW’s Enterprise Data Warehouse (EDW). The vertical columns represent the “Business Domains” of data that are available. There are many data tables from each business domain in the EDW that are available to users. Data is loaded into those tables from official source business systems. (i.e. Human Resources - HEPPS, Financial - FAS, Student - SDB, etc.) The horizontal rows of the matrix represent “Roles”, that Data Custodians of the source systems have defined, for specific row and column access to the data tables in each business domain. Refer below to the definitions of the roles, as well as column privilege levels, for details on how access is applied. Refer to the Decision Support web site for details on what data tables and reports are available via the EDW. <http://decisionsupport.washington.edu>

Role Privilege Matrix		Business Domains							
		Human Resources		Financial		Student		Research ¹	
Areas	Roles ²	Rows	Columns	Rows	Columns	Rows	Columns	Rows	Columns
All Units	Administrator/Manager/Fiscal Tech	All	HR Baseline	All	All	None	None	All	All
	Administrative Analyst	All	HR Baseline	All	All	All	ST Baseline	All	All
	Payroll Coordinator	All	HR Expanded	All	All	None	None	All	All
Academic Units	Advisor/Academic Staff	None	None	None	None	All	ST Baseline	None	None
	Principal Investigator	All	HR Baseline	All	All	All	ST Baseline	All	All
	Chancellor/Dean/Dean's Analyst	All	HR Baseline	All	All	All	ST Baseline, ST Aid Low	All	All
Central Offices All Campuses	Academic Analyst	All	HR Baseline	All	All	All	ST Expanded	All	All
	Institutional Analyst	All	HR Baseline	All	All	All	ST Expanded, ST Aid Med	All	All
	Student Aid Analyst	All	HR Baseline	All	All	All	ST Expanded, ST Aid High	All	All
	Student Fiscal Analyst	All	HR Baseline	All	All	All	ST Expanded, ST Fiscal	All	All
	Payroll Analyst	All	HR High	All	All	All	ST Baseline	All	All
	Academic Personnel/HR Analyst	All	HR Full	All	All	All	ST Baseline	All	All
Internal Audit	Auditor	All	All	All	All	All	All	All	All
UW-IT	EDW Administrator	All	All	All	All	All	All	All	All

¹ Research Business Domain – Refers to access to administrative data related to research operations

² Roles - May not relate to a position description or job title.

Note: **Shaded Areas = Role access managed centrally via dmc-support** Non-shaded Areas = Role access managed via delegation to ASTRA unit authorizer

Security Roles and Access Privilege Matrix for READ-ONLY Access to Data - Version 20

ROLE DEFINITIONS

Role/Group Description	Definition
Administrator/Manager/Fiscal Tech	Department administrators and managers, in academic or central departments, responsible for the administration of specific budgets and/or the administration of employees in a specific organization.
Administrative Analyst	Seattle, Tacoma or Bothell administrative staff responsible for providing analysis of data to support UW Administration. For example, analysts in UW Finance and Facilities, UW Information Technology, etc.
Payroll Coordinator	Payroll Coordinators, in academic or central departments, responsible for processing payroll information for specified groups of UW employees.
Advisor/Academic Staff	Student advisors and/or other staff involved in administrative functions related to academic student data only.
Principal Investigator	Principle Investigators assigned to specific grants.
Chancellors/Deans/Dean's Analyst	Chancellors, Deans, or principal Analysts of an academic unit.
Academic Analyst	Analysts that provide academic data analysis to UW central offices.
Institutional Analyst	Seattle, Tacoma or Bothell Institutional Research staff responsible for providing enterprise wide analysis of institutional data. For example, analysts in UW Institutional Studies.
Student Aid Analyst	Analysts that provide student aid data analysis to UW central offices.
Student Fiscal Analyst	Analysts that provide student fiscal data analysis to UW central offices.
Payroll Analyst	Central Department payroll analyst and/or functional staff. For example, work includes federal income tax and employee deduction data access needs.
Academic Personnel/HR Analyst	Central Office HR, Academic HR or EOO analysts and functional staff.
Auditor	Universal access granted by special University privilege. For example, UW Internal Audit staff.
EDW Administrator	UW-IT staff responsible for developing and maintaining the Enterprise Data Warehouse database environment.

Note: **Shaded Areas = Role access managed centrally via dmc-support**

Non-shaded Areas = Role access managed via delegation to ASTRA unit authorizer

Security Roles and Access Privilege Matrix for READ-ONLY Access to Data - Version 20

COLUMN DATA PRIVILEGES

Data Custodians classify data within the Enterprise Data Warehouse according to appropriate security principles and standards. The charts below show for certain categories of data how classifications are applied. The column privilege level headings below are represented in the Role Privilege Matrix above, which indicates the level of access allowed for specific roles. Each Business Domain may have its own set of privilege levels defined. Currently Human Resource and Student domains have specific column privilege levels defined.

X = Privilege for read only access to a category of column data in the EDW

HUMAN RESOURCES		PRIVILEGE LEVELS			
		HR Baseline	HR Expanded	HR High	HR Full
CATEGORY OF COLUMN DATA	All human resources data except for the categories listed below	X	X	X	X
	Employment status		X	X	X
	Social Security number			X	X
	Citizenship			X	X
	Home Address and Phone			X	X
	Deductions			X	X
	Contributions			X	X
	Date of Birth			X	X
	Sex			X	X
	Race/Ethnicity				X
	Disability				X
	Veteran Status				X
	Family Medical Leave Act				X
	Personnel Actions			X	X
	Benefits				X
Medical Conditions				X	

Security Roles and Access Privilege Matrix for READ-ONLY Access to Data - Version 20

STUDENT		PRIVILEGE LEVELS					
		ST Baseline	ST Expanded	ST Fiscal	ST Aid Low	ST Aid Med	ST Aid High
CATEGORY OF COLUMN DATA	All student data except the categories listed below	X	X	X	X	X	X
	Student Charge Data in Fiscal Tables ³	X	X	X	X	X	X
	Social Security Number		X	X		X	X
	Disability		X			X	X
	Non Charge Data in Fiscal Tables ⁴			X			
	Financial Aid Low ⁵				X	X	X
	Financial Aid Med ⁶					X	X
	Financial Aid High ⁷						X

³ Student Fiscal charge related tables contain student expenditures for tuition, fees, housing, food, etc.

⁴ Student Fiscal non-charge related tables contain sensitive student account information

⁵ Financial Aid Low – minimal access – Select financial aid data for financial aid need determination analysis only.

⁶ Financial Aid Medium – broad access – Select financial aid data for enterprise-wide research and reporting only.

⁷ Financial Aid High – complete access – All financial aid data for Office of Student Financial Aid operations staff only.

Security Roles and Access Privilege Matrix for READ-ONLY Access to Data - Version 20**GUIDING PRINCIPLES**

1. This Matrix describes row (i.e. span of control) and column restrictions that should be applied to institutional data in UW applications such as the Enterprise Data Warehouse (EDW). At the current time no row restrictions have been defined for roles with access to EDW data.
2. Role assignments may span across different business domains. For example, the PI role has access to HR, Financial, and Student data. At the current time, the Advisors / Academic Staff role is restricted to data only in the Student business domain.
3. To keep access management simple and timely, Data Custodians are encouraged to assign a user to a single role on the matrix. If an exception to this principle is necessary (i.e. because a user performs more than one job function) it is technically possible to assign a user to more than one role. In this case, the combination of the assigned roles may give the user more, or a higher, level of access privileges.