Albany State University

DegreeWorks Access Request Form

Instructions

1. Requestor/User fills in identification information in Section 1.
2. User reads applicable policies and signs acknowledgement in Section 2.
3. Requestor/User selects appropriate access level/role in Section 4.
4. Supervisor approves system access request in Section 3.
5. The Data Steward(s) sign in Section 5 to authorize the access.
6. The Enterprise System Custodian grants authorized access and provides log-in credentials to the user.

Routing Instructions: On completing Section 5, route form to the ASU HelpDesk. The HelpDesk will route the form to the appropriate Enterprise System Custodian for implementation.

Section 1: User Information

Name:		**Ram ID:**	
Department:		**Job Title:**	
ASU Email:		**Phone:**	
Requestor's Name:	(if requestor is other than the user)	**Requestor's Phone:**	
Reason for access request:			

Section 2: User Policies Acknowledgement

The policies listed below govern user responsibilities regarding system access. These and other Campus Technology policies are available from the ASU Home Page➔ Administration ➔ Campus Technology ➔ Policies and Forms page at http://www.asurams.edu/web/general-campus-technology/policies-procedures. Please read these policies and familiarize yourself with your responsibilities.

1. Acceptable Use Policy
2. Computer Accounts Policy
3. Enterprise Systems Access Policy
4. Password Security Policy

☐ I have read and acknowledged the policies above and agree to abide by all applicable laws and restrictions that govern use of this enterprise system.

User's Signature:		**Date:**	

Section 3: Supervisor Authorization

Supervisor's Signature:		**Date:**	
Supervisor's Name:		**Supervisor's Phone:**	
Supervisor's Title:			
Supervisor's Email:			

Albany State University

DegreeWorks Access Request Form

Section 4: Access Level/Role	
Account Request:	☐ New Account ☐ Modify Account ☐ Remove Account
Role/Access Level (check one):	☐ Advisor ☐ Registrar ☐ Admin [OIIT only]

Section 5: Data Steward(s) Authorization			
For "Advisor" access level:	Dean or Chair of user's area		
Data Steward's Signature:		**Date:**	
For "Registrar" access level:	Asst. VP of Academic Affairs		
Data Steward's Signature:		**Date:**	
For "Admin" access level:	VP of OIIT		
Data Steward's Signature:		**Date:**	

Section 6: Enterprise System Custodian (for OIIT Use Only)			
Account Action:	☐ Account Created ☐ Account Modified ☐ Account Disabled Note: In order to preserve Notes, Plans, and Exceptions created by a user, do not delete ADV or REG accounts. Reset the password to deleted_YYYYMMDD_random – Use the word 'deleted', add the date the user left in YYYYMMDD format, and add some additional random alphanumeric characters. For example, deleted_20110729_73flutes.		
Account Settings:	User Name:		
	Account type: ☐ ADV ☐ REG		
	☐ Training Required ☐ User has completed training		
Custodian's Name:		**Date Completed:**	

Access Levels

- **Student:** All students are granted access to DegreeWorks automatically. Students may view their own audit, save the audit (to PDF), perform What-Ifs, use the GPA calculators, and create plans. This form is not required for students.
- **Advisor:** This allows the user to access student audits; run new audits; create, lock, and set active plans; and add notes. Users with this access level are required to complete an instructor-led training course prior to being given full system access. View the Training Calendar on Sharepoint for course schedules or contact the HelpDesk to request alternate training options.
- **Registrar:** This allows the user all Advisor functions plus the ability to refresh Banner data and add Exceptions. Users with this access level are required to complete an instructor-led training course prior to being given full system access. View the Training Calendar on Sharepoint for course schedules or contact the HelpDesk to request alternate training options.
- **Admin:** This access level is for Enterprise System Custodians and OIIT personnel only. It grants the user all Registrar functions and the ability to Scribe audits, modify SureCode configurations, customize the application look-and-feel, maintain users, run Transit reports, and view application logs. This is a high-level access requiring demonstrated skill and knowledge of the system, its applications, and the policies/procedures governing its operations.