

PROCEDURE MANUAL

	PROCEDURE 223.011		
	Page 1 of 5		
	Last Revision Date:	04/13/2026	
	Effective Date:	03/07/2022	
Last Review Date:		04/13/2026	
Section:	Technology	Subject:	Enterprise Application Enterprise Application Access Management

PURPOSE

The purpose of this procedure is to define how Arizona Western College (AWC) manages access to enterprise applications (ERP systems) to ensure the confidentiality, integrity, and availability of institutional data and systems.

SCOPE

This procedure applies to all users of AWC technology assets including employees, students, volunteers, and contractors. Access management controls are designed to minimize potential exposure to AWC resulting from unauthorized use of resources and to preserve and protect the confidentiality, integrity and availability of AWC's networks, systems and applications.

PROCEDURE

1. **Definitions**

1.1 Ellucian Colleague – the college utilizes Ellucian's Colleague Cloud Hosted platform for their ERP solution.

1.2 Colleague Access is the ability for college employees or authorized consultants to use Enterprise Application, the primary administrative information system of the college, to carry out the business of the college.

1.3 Data Steward is a person designated by College Leadership to manage ERP security definitions and software update testing for their business areas. Appointments are based on their overall business process knowledge, Colleague module and knowledge, data security and integrity responsibilities. See Appendix A for positions responsible for Data Stewardship.

1.4 Pre-Approved Role is a security definition pre-determined and approved by the appropriate Data Stewards, based on a specific job function or position. As such, additional approval is not required for individuals meeting the requirements of the pre-approved role.

2. **Authority**
 - 2.1 Colleague UI Access is controlled through the application of security classes. Access definitions are created by Data Stewards and maintained by ITSS Enterprise Applications Team; security assignments are based on pre-approved roles or individual access requests approved by Data Stewards and administered by Enterprise Applications. User supervisors may request access through the use of the form for initial or subsequent Colleague access. Access will be managed as appropriate to the individual's role within the College, per the procedure defined below.

3. **Granting Enterprise Application Enterprise Application Access**
 - 3.1 Requests for access to the college's ERP system will be submitted by an employee's supervisor, using the Colleague Production Access Request. Access is granted based on pre-approved roles or defined classes, and not by individual mnemonics (screens).
 - 3.2 Access to pre-approved roles, when defined, will be reviewed to ensure that the individual's position meets the standards defined for the role.
 - 3.3 Where there is not a defined pre-approved role, Data Stewards are responsible for reviewing the access requested, suggesting or describing modifications to the request, and approving the access.
 - 3.4 Once all required approvals have been obtained or validated, the ITSS Enterprise Applications Team will apply the confirmed access and inform the requesting supervisor, cc: the employee for whom access has been granted.

4. **Modifying Access**
 - 4.1 All requests to modify existing access granted to an employee will be submitted using the Colleague Production Access Request form, indicating the required access to be changed (added, removed).
 - 4.2 Changes to access may be initiated by the employee's supervisor, based on changes in job duties, or by Data Stewards, based on new procedures or enhancements implemented.
 - 4.3 All modifications (additions, deletions) to access initiated by Data Stewards will require the permission of the supervisor of the individual whose access will be changed, to keep supervisors informed of the changes in responsibilities of their employees.
 - 4.4 Approval for the addition of access will follow the same requirements as outlined above for granting access.
 - 4.5 In the event of sudden or unexpected loss of a staff member due to illness/injury or termination, emergency temporary access to ERP functions may be granted to another user upon receipt of a request from the supervisor and Vice President overseeing the department.
 - i Such a request should ensure that separation of duties is maintained for the user to ensure adequate controls within business processes.

5. **Terminating Access**

5.1 ERP access will be terminated based upon notification from Human Resources that an individual is no longer an employee of or authorized consultant working for the college.

5.2 ERP access may also be terminated by ITSS through notices received from Human Resources of a transfer to a position whose responsibilities require different access within the ERP. In such cases, the supervisor of the position to which the employee transferred will be responsible for requesting appropriate access for that employee.

i Supervisors of the vacated position should ensure that access to data and processes is promptly removed, for data security reasons. Former incumbents should not retain access once they have left the position.

5.3 ERP access may also be terminated for inappropriate use of the system and/or the data to which an individual has access, as determined by Human Resources and the Chief Information Officer.

5.4

6. **Inactive Colleague Accounts**

6.1 Inactive accounts, defined as a UI account not demonstrating use in the ERP for ninety (90) days, may be prevented from accessing the application. Reactivation of the employees' access will require a new request to be submitted by the employee's supervisor.

7. **Access Review**

7.1 Colleague user access must be reviewed at least annually for changes in job functions that would necessitate a change in access. The Director of Enterprise Applications will make current access lists available to Data Stewards and supervisors for review and confirmation of access needed.

Appendix A: Data Steward Areas of Representation

Security access to the ERP / Colleague modules listed below will be maintained by the position noted or designee, as approved by college leadership. Modules not listed will be managed by the Director of Enterprise Applications until an otherwise appropriate Data Steward is appointed to manage the processes and access.

Module (within Colleague)	Data Steward Responsible (Title subject to college updates)
AC – Academic Records (ST)	Registrar
AE – Activities and Events (Core)	Director of Enterprise Applications
AM – Recruitment Admissions (ST)	Registrar
AP – Accounts Payable (CF)	Assistant Controller
AR – Accounts Receivable (ST)	Accounts Receivable Supervisor
BU – Budget Management (CF)	Assistant Controller
CC – Communications Management (Core)	Director of Enterprise Applications
CFS – Enterprise Application Financials Setup (CF)	Director of Enterprise Applications
CO – Campus Organizations (Core)	Director of Enterprise Applications
CR – Cash Receipts (ST)	Accounts Receivable Supervisor
CS – Core Setup/Utilities (Core)	Director of Enterprise Applications
CU – Curriculum Management (ST)	Director of Curriculum, Assessment & Scheduling
DA – Degree Audit (ST)	Director of Curriculum, Assessment & Scheduling
DM – Demographics (Core)	Director of Institutional Effectiveness and Research
EA – Employment Actions (HR)	Benefits Manager
EC – Ecommerce (Core)	Director of Enterprise Applications
ELF – Electronic File Transfer (Core)	Director of Enterprise Applications
ER – Employee Labor Relations (HR)	Benefits Manager
FA – Financial Aid (ST)	Director of Financial Aid
FI – Faculty Information (ST)	Director of Institutional Effectiveness and Research
FP – Facilities Profile (Core)	Director of Curriculum, Assessment & Scheduling
FRP – Federal Reporting (ST)	Director of Institutional Effectiveness and Research
FRX – Financial Reporting Export (CF)	Director of Enterprise Applications
FX – Fixed Assets (CF)	Assistant Controller
HD – HR Data Marts (HR)	Benefits Manager
IN – Inventory (CF)	Assistant Controller
OR – Organization Info (Core)	Director of Enterprise Applications
Module (Enterprise Application Application) [Continued]	Data Steward Responsible [Continued]
PA – Projects Accounting (CF)	Assistant Controller
PC – Position Budgeting (HR)	Benefits Manager
PE – Personnel (HR)	Benefits Manager
PH – Process Handler (Core)	Director of Enterprise Applications
PR – Payroll (HR)	Payroll Manager
PU – Purchasing (CF)	Director of Purchasing
R25 – Resource 25 Interface (ST)	Director of Curriculum, Assessment & Scheduling
RL – Residence Life (ST)	Director of Residence Life
S25 – Schedule 25 Interface (ST)	Director of Curriculum, Assessment & Scheduling
SC – Scheduling (Core)	Director of Curriculum, Assessment & Scheduling
SDU – Student Database Utilities (ST)	Director of Enterprise Applications

SL – Surveys (Core)	Director of Enterprise Applications
SRH – State Reporting (HR)	Payroll Manager
SSS – Student Support Setup (ST)	Director of Enterprise Applications
SV – Staff/Volunteer Info (Core)	Director of Enterprise Applications
WB – Web Admin Support (ST)	Director of Enterprise Applications
UT – Utilities Application (All Modules)	Director of Enterprise Applications
XAWC – AWC Custom Reports	Director of Enterprise Applications

HISTORY

IT Reviewer Name	Update Date	AWC Reviewer	Approval Date
Tyler Vodehnal	1/24/2023	Dr. Corr	5-22-2023
Scott Estes, Caleigh Flores, Tyler Vodehnal	11/20/2023		
Tyler Vodehnal	04-01-2024	Ashley Herrington	04-01-2024
Scott Estes, Tyler Vodehnal, Mercedes Soto	02-04-2025	Ashley Herrington	4/14/2025
Scott Estes, Tyler Vodehnal	02/04/2025	Dr. Reetika Dhawan	4/13/2026