



**Academic Event
Scheduling System
(AESS)/Series25 Access
Request Form**

For UCit Use Only

Username

Department

Access Level

Password

This form is used to authorize AESS/Series25 System security privileges for persons using the online AESS/Series25 System. New persons may be added and existing user's accounts may be eliminated or have changes made to their current privileges.

Direct any questions about the completing this form to the R25 Security team at 556-9065 or via email at r25Security@uc.edu. Mail completed form to R25 Security Access, ML #0149.

Notification of AESS/Series25 System account information will be mailed to new users after appropriate authorization has been received.

User Information - Information supplied on this form is strictly confidential. Please provide complete information.

This request is to (select any that apply):

Add New User ____ Transfer ____ Name Change ____ Terminate Access ____

This request is for a (select one):

UC Employee ____ Corporate ____ Contractor ____ Temp ____ Student ____

Transfer from (Dept) _____ to (Dept) _____

If this is a name change, previous name _____

If this is a contractor, temp, or student, expiration date ____/____/____

First Name: _____ Middle Initial: ____ Last Name: _____

University ID: _____ - _____ - _____ Username (6+2): _____ Birthdate (MMDD): _____

Business Phone: (_____) _____ - _____ x _____

Department: _____

Job Title: _____

Mail Location: _____ Building/Room: _____

E-Mail Address _____

AUTHORIZATION:

Department Information: *Departmental authorization is required to process this request. This section identifies the AESS/Series25 System Coordinator for your department.*

Authorizing Department: _____

AESS/Series25 System Coordinator: _____

Coordinator's E-mail: _____ Phone: (_____) _____ - _____

Note: It is your responsibility to request the deletion of this account when the account holder is no longer an active member of the university community. Accounts are not to pass from employee to employee. New accounts must be requested for new employees.

Authorized Signature: _____ Date: ____/____/____

The User Agreement – Signature of the account user is required before the request can be processed.

Core Systems Access Rules

- Access to any UC Core System will only be granted with appropriate requests and approvals.
- An Access Request Form is required to reinstate a deleted account.
- Passwords will only be reset for an account that belongs to the user requesting the password reset.
- No one may use an account that belongs to another person.
- Each person with an account for a Core System may have one and only one username and one and only one userid for that system.
- Each person accessing a Core System must have a unique account belonging only to that person.
- All contractors, temps and student workers must provide an expiration date for their core system account. If no date is provided, an expiration date of 6 months will be placed on the account. Expiration dates may be extended by having the authorized person for a department submit an e-mail to Systems and Operations Security indicating the new expiration date.

In accordance with University Rule 3361:10-17-04: Conduct and Ethics: Use of University Resources:

Members of the Faculty, Administration, Student Body, Volunteer Workers, and Staff are responsible for the appropriate use of University resources. Use of University resources in a manner inconsistent with this rule is a violation subject to disciplinary action.

(B) University Property, Facilities, and Services:

(3) All University computers shall be used solely for authorized academic, instructional, research, administrative or contract purposes. Any unauthorized use of computer resources and/or facilities shall constitute a violation of University policy and will subject the violator to University disciplinary action.

Further, all users of the university's information-technological resources must adhere to the Policy for Responsible Use of Information Technology at the University of Cincinnati.

Signature: _____ Date: ____/____/____

The user of the account shall be responsible for all activities of the account. This account is not transferable to any other individual, nor should the password be given to anyone else.