

Electronic Access Requesting - Room Ownership/Requesting Privileges CO-ID-PR7

Responsible Officer: Vice President for Administration and Campus Operations
Sponsoring Department: Mav Express
Revision Date: 13 September 2012
Errors or changes to: aim@uta.edu

CONTENTS

Procedure Objective

Scope

Responsibilities

Procedures

 Section I. General Information

 Section II. Rooms Designated as

 Section III. Rooms Designated as

Forms and Tools/Online Processes

Definitions

Rationale

Related Statutes, Policies, Requirements or Standards

Appendices

Contacts

Website Address for This Procedure

PROCEDURE OBJECTIVE

This procedure clearly defines electronic card access requesting privileges available to the different departments/areas on campus and optimizes campus safety and security through efficient electronic card access management.

SCOPE

All UTA departments/areas requesting electronic card access from Mav Express.

RESPONSIBILITIES

Mav Express

- Maintain proper system structure allowing for the support of this procedure.
- Ensure that all electronic card access privileges granted comply with this procedure.

Departments

- Comply with this procedure.

PROCEDURES

Section I. General Information

- A. **With the exception of Sections II and III below**, all rooms in the Mav Express/CBORD electronic card access system will be owned by the department/entity identified in the CASIM system.
1. Only the CASIM owner will be authorized to request access privileges for these rooms.
 2. Any other departments/entities needing access to these rooms will have to request access via the CASIM owner.
 3. These rooms shall remain accessible to the designated "All Access Groups"

Section II. Rooms Designated as

- A. **Rooms designated as "Classrooms"** under CASIM and officially owned by Classroom Support Services will be open to all provided the Dean or Department Head appoints a staff member as an approved requestor for such space.
1. As an exception to this rule, rooms with videoconference equipment will only be owned by Classroom Support Services. Any department needing access to these technology-enhanced classrooms will have to request access from Classroom Support Services.
 2. Classrooms shall remain accessible to the designated "All Access Groups".
 3. Access privileges to these classrooms will be classified as "temporary" and will be deleted at the end of each semester unless the room requested is in the department's home building(s). Departments can request permanent access to rooms as long as the room is located in their home building(s).
 4. Permanent access may only be granted for patrons classified as employees (faculty and staff).

Section III. Rooms Designated as

- A. **Rooms designated as "Highly Restricted"**

1. Rooms or spaces which have associated legal or regulatory restrictions, such as radioactive materials storage rooms, may receive special treatment and be allowed customized access control privileges **including control over all access groups**. Such requests are evaluated on a case-by-case basis. Departments requesting the "Highly Restricted" designation for a room assigned for their use must submit proper documentation to Campus Card Operations which clearly demonstrates the legal or regulatory requirement which mandates this more restrictive level of access control.
2. Note that despite a "highly restricted" status, access cannot be restricted from the UTA Police Department and the Environmental Health & Safety office.

FORMS AND TOOLS/ONLINE PROCESSES

Access Wizard: Electronic access request are made online via the Access Wizard located at www.uta.edu/access.

NOTE: Only a departmental approved requester can login to the Access Wizard and submit an electronic access request. If you need access privileges, please contact your departmental approved requester.

DEFINITIONS

All Access Groups: All access groups are designated work groups managed by departments such as UTA Police, Environmental Health and Safety, Facilities Management, Campus Card Operations, OIT Networking, and Telecom. Members of these work groups must pass required background checks and their positions must be classified as security sensitive. To properly support the campus infrastructure, these work groups are given access privileges to a large percentage of spaces managed via electronic access. Departments managing these work groups are committed to manage their staff appropriately while maintaining sufficient operational flexibility to perform services. These groups are considered mission-critical and departments and room owners cannot negotiate exclusion of All Access Groups unless the space falls under a defined exception above.

RATIONALE

- Campus electronic access must be managed to offer a reasonable balance between safety/security and convenience.
- Several departments/areas have expressed the need to have control over the rooms falling under their oversight.

RELATED STATUTES, POLICIES, REQUIREMENTS OR STANDARDS

| UT System Administration Policies and Standards | Other Policies and Standards |
|---|--|
| | <i>Electronic Access Review</i> (Procedure 17-1) <i>Automatic Removal of Electronic Door Access Privileges</i> (Procedure 17-7) |

APPENDICES

N/A

CONTACTS

If you have any questions about Procedure 17-8, *Electronic Access Requesting-Room Ownership/Requesting Privileges*, contact the following departments:

| Subject | Office Name | Telephone Number | Email/URL |
|-------------------------|---------------------------------------|------------------|---|
| All topics in Procedure | Mav Express | (817) 272-2645 | access@uta.edu http://www.uta.edu/mavexpress |
| Website access | Administrative Information Management | (817) 272-0222 | aim@uta.edu http://www.uta.edu/aim |

WEBSITE ADDRESS FOR THIS PROCEDURE

<http://www.uta.edu/policy/procedure/17-8>