ELECTRONIC ACCESS PROCEDURES

I. PROCEDURES FOR CARD ACCESS SYSTEM

A. Issue of Access Cards

1. Cards are issued by Department of Public Safety Key & Access Services, the ID Card Office, University Housing, or other designated departments.

2. Cards for non-University personnel are issued by Public Safety Key & Access Services, a University faculty or staff must authorize the use of a card by a non-University person.

B. Building Access

Faculty, staff, and students shall be permitted access as required for their work or studies. Departmental administration shall determine who is permitted access to their buildings. Staff from Department of Public Safety, Facilities Management, and Information Technology Services are permitted in almost all areas secured by security management systems.

C. Lost/Stolen Cards

Reporting lost/stolen cards is the responsibility of the card holder. A card holder may not permit any other person to use the card assigned to the card holder. Replacement cards will be issued as described above.

D. Primary Records

The issuing office will maintain the primary records for all cards issued in the security management system software. Records, at a minimum, will include the following information for each card issued:

- Card Number
- Issued to (name and hawkid)
- Mailing Address
- Telephone Number
- Building Access (building, days, hours)
- Date

Automated synchronization with university data shall occur on a regular basis, no less than weekly.

E. Deactivation of Cards

The departmental/collegiate card administrator shall remove access of faculty/staff/students that transfer out of their department or are terminated.

F. Use of electronic access software

1. Access to the security management system software shall be set up as individual user accounts for departmental/collegiate users to access the system. Training is required and is provided by Department of Public Safety Key & Access Services. Accounts are not to be shared except as noted below.

2. Generic user accounts are permitted for a few specific purposes:
    I . Monitoring – a workstation used for monitoring alarms and/or video, without any authority to make changes.
    ii. Hand Geometry enrollment – a workstation at CRWC.
    iii. Programming – certain programming functions need to done with a generic account. These accounts, and the persons permitted to use them, are approved by the Key and Access Services Manager.

G. Restricted Doors

Electronic access doors associated with restricted use spaces, hazardous rooms, or other high-security risks are identified as Restricted.

1. Departments requesting that a door be categorized as Restricted shall send an e-mail describing the request to DPS-access-services@uiowa.edu. Key and Access Services will work to identify individual doors as Restricted and to determine who has access to these rooms.

2. Key & Access Services will work with the Department to program the electronic access system. The door(s) will be identified as “Restricted” and the names of the departmental staff members that provide authorization will be programmed in the system.

3. Record keeping will be done within the AMAG Security Management System.