

## ELECTRONIC ACCESS POLICY

### **I. PURPOSE**

This statement of University policy is intended to provide appropriate security for campus facilities in order to protect life, property, patient confidentiality, and research integrity. The associated procedures provide for the administration and control of electronic access and access cards.

### **II. GENERAL ACCESS CARD POLICIES**

#### ***A. Ownership of Access Cards***

The University of Iowa is the owner of access cards and access fobs (hereafter referred to generically as cards). Cards are obtained from Department of Public Safety Key & Access Services, the ID Card Office, University Housing, or other designated departments.

Cards shall be assigned to an individual and the name and contact information for the individual shall be stored in the security management software. Issuance of generic cards shall require the approval of the Department of Public Safety.

#### ***B. Administration of the Card System***

The AMAG Security Management Systems are administered by Department of Public Safety Key & Access Services with responsibility for department areas/buildings distributed to the departments/colleges. A separate card system is administered by UIHC Safety and Security. The University Parking and Transportation Dept administer card systems for parking lot access. The responsibilities of administration include:

1. Maintenance of accurate controls and records to provide accountabilities for all cards issued.
2. Activating cards to allow access (upon receipt of appropriate written authorization).
3. Deactivating cards upon receipt of notification of loss, theft, termination or change in status.
4. Establishing user accounts for departmental/collegiate software administration.

#### ***C. Responsibilities of Department of Public Safety Key & Access Services***

Department of Public Safety Key & Access Services is responsible for maintaining the locks, door devices, hardware, software, and field controllers of the electronic security management system in General Education Fund buildings. Non-GEF buildings will hire FM for the maintenance of these systems or will have trained and qualified staff to perform this work. Department of Public Safety Key & Access Services will administer the system, establish procedures, program system-wide settings, provide user training, and work with the Department of Public Safety in effectively administering the systems.

#### ***D. Responsibilities of Registrar's Office***

The Registrar's Office is responsible for maintaining accurate student registration records so that card access can be properly granted or denied based on student status.

#### ***E. Responsibilities of Human Resources***

The Human Resources Department is responsible for maintaining accurate employee data so that card access can be properly granted or denied based on employee status.

#### ***F. Responsibilities of Housing Management***

University Housing will determine residence hall access for residence and facility maintenance needs. Changes in authorization for access to residence halls will be handled by Housing and they will maintain procedures which govern card access to student residences. They will also maintain accurate housing contract records so that access can be properly granted or denied based on housing status.

#### ***G. Department/Collegiate Responsibility***

Designated and trained departmental/collegiate employees may use the security management software to authorize faculty, staff, and student access to buildings with card access capability.

#### ***H. Individual Responsibility***

Faculty, staff, and students that need access to a building with electronic security management system will be issued a card or their ID card will be enabled to grant access. Individuals associated with the University must have an official relationship to be granted a card. Each person is permitted one access card or one card per system if the cards are not multi-functional. Reporting lost/stolen cards is the responsibility of the card holder. There will be a charge for replacement cards.

Card holders shall not share their access cards or let unauthorized persons into locked buildings or rooms using their access card.