Administrative Services: Electronic Access Control - DRAFT

1.0 Purpose and Summary

Electronic access control is essential in providing security, access, and protection to University students, personnel, equipment, buildings, and resources. Universities are popular targets of theft from both internal and external threats. Access to University buildings is a privilege, not a right, and requires clear identification of user access rights, responsibilities, and accountability.

The purpose of this policy is to:

- Regulate access to University property.
- Ensure that any individual, college, department, operating unit, or program within the scope of this policy is aware of their responsibilities.
- To provide clear requirements for the on-going installation and management of electronic access control.
- To balance convenience of use of the electronic access control system with clear security protocols and oversight.
-

1.1 Benefits of Electronic Access Control

- Provides building access for faculty, staff, and students, without the need for metal keys.
- Access to buildings can easily be added or removed electronically.
- Decreases the liability of stolen or lost metal building entrance keys.
- Provides an audit trail that can document activity at each door.
- Perimeter door lock and unlock schedules for buildings can be adjusted as needed.
- Locking and unlocking can be done electronically, reducing staffing loads.
- UPD can be notified if entry doors are forced open or propped open.
- Perimeter doors on a building or group of buildings can be remotely locked in the event of an emergency or threat.

2.0 Scope

This policy and all implemented standards and procedures will apply to all individuals using any device to access University buildings and or resources, including but not limited to:

- Vice Presidents, Deans, Directors, and Department Heads,
- Affiliates, associates, and volunteers,
- Faculty, appointed personnel, staff, and students,
- Third-party vendors, contractors and their agents.

This policy excludes UAA Campus Housing electronic access control.

3.0 Definitions and Acronyms

Campus Security Team: This entity has not been created at the time of the writing of this policy. However, the creation of a Campus Security Team dedicated to the security and monitoring of facilities may be useful to the University in the future.

Door Position Switch: A device that senses if a door is opened or closed and alerts the alarm system or monitoring station that a door is in the open position. Hardware types vary.

Electronic Access Control / Access Control System (ACS): a type of security that manages and controls who or what is allowed entry to a facility. It identifies and grants entrance to individuals based on the validity of their credentials. Secondarily, it can record and track who enters a facility or room and can be tied to other security systems, such as cameras and alarms. A secondary function of monitoring whether a door is open or closed is also typically provided.

IMT: UAA Incident Management Team.

IT: UAA Information Technology Services.

Local alarm: a horn or buzzer that provides local "policing" - via an audible alarm - of a door that is forced or held open too long.

Owner Performance Requirements (OPR's): OPR's define an Owner's project goals, measurable performance criteria, cost considerations, benchmarks, success criteria, and supporting information. OPR's must be developed with significant Owner and/or Owner's representative input and ultimate approval. Effective OPR's incorporate input early from the design or engineering team, operation and maintenance staff, and the end users and are updated throughout the project design.

Personal Identification Number (PIN): a number allocated to an individual and used to validate electronic transactions or procedures.

Proximity card / prox card: a 13.56 MHz "contactless" smart card that can be read without inserting to into a reader device. The term "badge" is used interchangeably.

Security Levels: (examples provided below are for illustrative purposes only, specifics will be determined and further refined by UAA as part of the development of electronic access control system OPR's)

- **Level 1- "Basic Security"**: These areas are typically unlocked during business hours, allowing access by University personnel or the general public. After hours, these areas are secured, and access is via UAA badge and/or use of a PIN. University support units will have access to these areas.

- **Level 2 - "Enhanced Security"**: Areas that are mechanically and electronically locked at all times, including during normal business hours, and that require a UAA badge to gain entry each time (they may also require use of a PIN as a supplemental security measure). University support units will have access to these areas.

- **Level 3 - "High-Risk Security"**: Areas that by federal, state, or local laws or code have restricted access or are restricted by University policies and/or procedures. These areas may require higher security access control devices such as biometric control devices. In some cases, access by University support services may be restricted or limited and may require that support services be escorted by approved personnel or have special training.

UAA: University of Alaska Anchorage. UAA is the "university" in this document and refers to the Anchorage campus only. This document governs only the **Main Anchorage Campus**: the cluster of buildings generally along Providence Dr. and the west side of Elmore Rd., east of Lake Otis Pkwy and south of Northern Lights Blvd

UPD: UAA University Police Department

4.0 Policy

4.1 System and Procurement

I. The electronic access control system should be a single centralized software on a discrete VLAN network, with the exception of the Housing access control system and any future exceptions that are approved through a formal process with written consent by the University Police Department (UPD).

II. All instances of electronic access control and related hardware should comply with UAA's Owner Performance Requirements (not yet developed) for the system and UAA hardware standards. Should new instances require amendments to the Owner Performance Requirements or hardware standards, those amendments should be done formally, with review by UAA Facilities & Campus Services, Information Technology Services (IT), and UPD, with written approval required from UPD.

4.2 Management

I. Management of the electronic access control system should be centralized under either UPD or a Campus Security Team (yet to be formed/defined). A dedicated on-call member should be available for emergencies 24 hours a day, 7 days a week (24/7), with a secondary 24/7 member identified in case of emergencies.

II. Designated representatives from UPD or the Campus Security Team shall be the only individuals who can administer security access levels (who has which rights to access) unless written permission is granted to someone outside those departments by UPD.

III. UPD and IMT shall have designated seats and training on the system for security review and emergency response respectively.

IV. The system and network are to be administered at a technical level by IT.

V. With written approval by UPD, individual UAA departments may have the option for seats on the system with limited access to UPD-approved doors and security level designations.

VI. Departments shall notify UPD immediately of any individuals who constitute a security concern and who should be denied access. Should a department neglect to notify UPD of a known security threat whose access privileges should be eliminated, UPD has the options of:

- Charging the department a security fee,
- Requiring security training for department personnel, and/or
- Revoking any access control seats held by for the department.

VII. A 24/7 maintenance contract with the access control system manufacturer is required to ensure that administrators have the support they need to maintain the system at the optimal security level.

4.3 Access Points

I. The following is a general outline of the hierarchy into which the access control system access points shall be developed. Detailed OPR's are needed to fully differentiate and define access points.

II. Depending on building design and layout, access points will operate in the following manner:

A. Designated perimeter doors will be electrically locked and unlocked according to an electronic schedule, but capable of badge reader entry after hours.

B. Secondary perimeter doors will be electrically locked and unlocked according to electronic schedule but not provided with a badge reader and therefore incapable of entry when locked.

C. Egress only doors will remain locked at all times.

D. All perimeter doors will be equipped with door position switches and have dog down “prop open” devices removed or omitted.

E. After-hours building access will be granted by using a valid UAA badge, thereby creating an audit trail.

F. Electronic access control will be coordinated with physical (hard) key master levels, see 2019 *Key Security Policy* (still in draft form at the writing of this policy).

4.4 Training

I. Written training protocols shall be developed collaboratively by UPD and IT, both for new administrators and for annual refamiliarization training for people already using the system.

II. Any new administrator shall be required to attend initiation training.

III. Annual trainings for the refamiliarization of all administrators, led collaboratively by UPD and IT shall be required.

4.5 Security Audits and Reviews

I. At the end of each semester, a formal security review and electronic audit shall be done of the system that should, at a minimum, include:

   A. The elimination of any individuals who no longer require access to certain spaces or who have left the UAA community.

   B. Updates to security levels to prevent progressive security dissipation or “creep” and to ensure that individuals are granted only the security level that is required and not a higher, more expansive security level.

   C. Piracy prevention (reviewed by UPD, IT, and the software company) to ensure the system is as secure from piracy as possible.

   D. Identification of systems short-comings and maintenance needs and an action plan for addressing them.

   E. Identification of short- and long-term goals for electronic access control, such as improved interface with other UAA software systems.

   F. Identification of security concerns and prioritizations of concerns.

II. Reports

   A. Reports detailing any maintenance, upgrades, or short-comings related to the electronic access control system shall be issued within two weeks after each audit to UPD, IMT, Facilities, and the Administrative Services leadership.

      - **Any critical malfunctions or short-comings that pose a security or major access impediment shall be identified immediately and brought to the attention of UPD and the leadership of Administrative Services.**

4.6 Additional Requirements

I. Door position switches are required at the following locations, some of which may not have existing electronic access control:

   a. Exterior doors,
   b. Doors into spaces of high security concern as determined by UPD or Facilities,
   c. Doors into spaces with expensive equipment as identified by individual departments and confirmed by Facilities and UPD,
   d. Doors into any other areas identified by UPD or Facilities,
   e. All doors with electronic access control in order to alert UPD of any doors left ajar, particularly after hours.

II. At a minimum access control system cards shall be 13.56 MHz contactless, smart type proximity cards. In response to industry trends and technological developments, UAA should consider the secondary option of mobile device access that would work in conjunction with prox card readers.

III. Where access control is installed at doors that do not currently have access control, UAA should consider the long-term cost, maintenance, and security advantages of only installing hardwired electronic lock systems in lieu of Wi-Fi locks.

IV. Door controllers and reader interface modules shall be mounted on the secure side of a door or into telecom rooms. Panels containing door controllers, reader interface modules, and door hardware power supplies shall be provided with tamper switches connected to UPDs monitoring station.