FACILITIES MANAGEMENT
Section: 530-6 Appendix B
Effective: 06/28/2024
Supersedes: New
Next Review Date: 06/28/2027
Issuance Date: 06/28/2024
Issuing Office: Vice Chancellor - Operations Management and Capital Programs

APPENDIX B – Electronic Access Processes

A. Electronic Access Control Systems (EACS) Requests

1. Departments are responsible for all costs related to interior door access component installation, repair, and replacement in those areas including but not limited to:

    a. Keyless access that has been specified by Department stakeholders during the Capital Planning stage and installed as part of new construction projects.

    b. Keyless access that has been installed after the original building construction.

    c. Replacing standalone keyless entry systems that are not already integrated or capable of integrating with the existing enterprise-wide access control system

    d. State, federal, or university policies and/or regulations require keyless or enhanced access control to a building or area

B. Technology Standard

1. All Electronic Access systems must meet the campus standard as specified within the current design guidelines and specifications, unless exempted in writing by the VC-OMCP or their designee. All Electronic Access installations for interior doors that are initiated after the implementation of this policy shall also meet this campus standard.

2. All Electronic Access hardware that does not interface with or meet the campus standard shall be identified and a feasibility study conducted to evaluate the efficacy of changing the system to one that meets the campus standard. All costs associated with the feasibility study and for any required conversion will be at the expense of the Department.

3. Building additions or modifications that include Electronic Access Control System (EACS) shall be communicated promptly to the Electronic Access Control Program (EACP) Manager. The Manager shall update the Department Access Coordinators (DAC) impacted and update the EACS as necessary. DACs shall notify personnel impacted by any additions or modifications to their areas. Any system updates required to provision access to the new or modified areas shall be completed by the DACs.

C. Electronic Access Responsibilities

1. Administrative Authority (AA) Responsibilities

    a. In conjunction with the facility supervisors, are responsible to designate two individuals within a facility or department area to act as primary and secondary Department Access Coordinators (DAC). Departments may assign additional DACs, depending on their specific requirements.

b. The Administrative Authority may serve as the primary DAC, or delegate other individuals in the building to serve as primary or secondary DACs. The DAC will work with the Designated Security Integrator in maintaining the department's access control and physical security systems program. Failure to designate a back-up DAC could delay processing of access transactions when the primary DAC is unavailable.

c. The name and contact information of the assigned Administrative Authority and their backup and any changes in this capacity must be sent to FM and EACP Manager.

d. Departments are responsible for controlling and scheduling electronic card reader and/or CREDENTIAL access to building entry and perimeter doors and to all areas assigned to, or under, the department's control and responsibility.

e. The department authorizing access for an individual is responsible for removing, returning, or revoking the access as required. This includes any metal keys or electronic access devices issued to allow access to department-controlled areas.

2. Department Access Coordinator (DAC) Responsibilities

a. Obtain authorization from their Divisional Control Point (DCP) or Director to requisition new EACS or initiate modification of existing EACS. All installations and modifications shall comply with university policy and standards and be conducted by or under the oversight of Planning, Capital Program Management or FM.

b. Implement department access control procedures.

c. Managing electronic card reader and/or credential access to building entry and perimeter doors and other card access areas under the department's control

d. Granting or removing card reader authorization for user access to building entrances and other areas under the department's control, including granting and removing access for new employees, departmentally sponsored visitors, retiring employees, terminated employees, and rotating student access as required.

e. Provisioning door schedules for the facility or area under their control.

f. Routinely contacting the Designated Security Integrator to re-authorize individual card-reader access users, based on the level of access and security required (The DAC should authorize the minimal level of access required for an individual to perform their assigned duties or responsibilities).

g. Terminating any means of electronic access to building perimeters or other university areas under their control when the user or employee leaves the department or university.

h. Maintaining accurate records for individuals who have been granted electronic access to building perimeter doors and all other areas under the department's control.

i. Routinely evaluate access control systems and requested modifications for functionality and effectiveness.

j. When EACS or access permissions to buildings or rooms change (departmental space changes, doors are added, rekeyed, or reprogrammed), the DAC shall notify FM and UCPD so that affected users (ITS, Campus Fire Marshal etc.) are notified appropriately.

3. Divisional Control Point (DCP) responsibilities:

a. Document DACs, telephone number, email, department name and building location; and shall send the information to the relevant DCP for compiling into a master list of DACs for the

relevant division.

b. Each DCP shall send their divisional master list of DACs to the EACP designees in FM and UCPD.

c. Departments are responsible for notifying DCPs of all changes to their department delegations.

d. Create and maintain their divisional master lists of DACs up to date and for promptly sending updated lists to the EACS designees in FM and UCPD.

e. Only DACs on the master list are authorized to request EACS actions.

4. Facilities Management (FM) responsibilities:

a. Performing or managing all lock work, EACS readers and door hardware repair for campus managed facilities.

b. Review and fulfill Work Order requests for EACS issues and recovering costs as applicable.

c. Assisting in the on-boarding of new EACS systems and devices during the commissioning of a Capital Project or Renovation at a recharge.

d. Assisting in the training of new DACs to include one-on-one, group, and facility commissioning of Capital Projects or Renovations at a recharge.

e. Ensuring scheduled closures such as holidays are, by default, programmed to automatically secure facilities.

5. EACP Manager responsibilities:

a. Ensure that the electronic access control system server is online and functioning.

b. Validate the redundant, failover system server is functioning and tested quarterly.

c. Request and ensure proper backup and system firewall templates are applied and maintained.

d. Maintain system records, including purging transactions every 12 months to maintain system performance.

e. Coordinate system-related activities between the Integrator, ITS, and DACs as appropriate to ensure successful device installation.

f. Troubleshoot and resolve system-related problems.

g. Actively audit system account management.

h. Document and submit change management requests for proper approval as required for any change that may affect system-wide end users and departments.

i. Schedule and perform system-level housekeeping and audit activities to ensure optimal system operation.

j. Coordinate formal training programs and documentation to on-board new DACs and FM personnel.