UNIVERSITY of DAYTON

Key Control and Electronic Access Control Policy

Effective Date: November 2012

Approval: March 17, 2014; University President

Maintenance of Policy: Vice President of Facilities Management; Department of Public Safety

PURPOSE: To establish standards for the management of facility keys and electronic access control at the University of Dayton.

Employees of every department at the University of Dayton are issued keys in order to access buildings and spaces as required in the performance of their duties. Contractors performing work on University of Dayton property also require keys in order to complete their work. In addition, electronic access control is being installed on perimeter and interior doors of campus facilities, permitting those doors to be accessed by authorized users by presenting their University of Dayton identification card (Flyer Card). The legitimate requirement for access must be balanced with the overarching requirement for security of campus facilities.

Responsibility for university key management is divided between the Department of Public Safety and the Department of Facilities Management. Each department has a vested interest in the review, approval, and fulfillment of key requests, compliance with university keying standards, and custodial tracking of keys from manufacture to disposal.

SCOPE: This policy applies to all University of Dayton employees. This policy also applies to contractors requiring keys in the performance of their contract.

POLICY: This policy establishes consistent standards regarding:

- Building keying standards.
- Key request authority.
- Key request and issuance procedures.
- Key holder responsibilities.
- Lost or stolen key procedures.
- Electronic access control installations.
- Management of access control privileges.

Compliance with these standards will promote effective management of university keys and contribute to improved physical security of campus facilities.

REFERENCE DOCUMENTS:

1. Key Control and Electronic Access Control Procedures
2. Appendix A: Master Key Authorization Letter
3. Appendix B: Sample Key Request
4. Appendix C: Master Keying Matrix and Key Request Authority
5. Appendix D: Key Request Authorization Letter
6. University of Dayton Background Check Policy

POLICY HISTORY:

Approved in original form
November 8, 1993

Approved as amended
November 27, 1995

Approved as amended
June 12, 2000

Approved as amended
November 2012

POLICY (continued):

I. **KEY HOLDER RESPONSIBILITIES**

a. University personnel are responsible for safeguarding all keys issued to them.
b. All keys will be issued through the Facilities Management Key Distribution Office. Keys shall not be transferred or passed from user to user.
c. Personnel will maintain only those keys required in the regular performance of their duties. All excess keys will be turned in to the Key Distribution Office when they are no longer required.
d. University personnel will turn in all keys issued to them to the Key Distribution Office immediately upon termination of employment. In the event of involuntary separation, the employee's supervisor will recover the employee's keys and turn them in to the Key Distribution Office.
    i. The Department of Human Resources will forward reports of persons leaving University employment to the Key Distribution Office. This report will be reconciled and the employee's former supervisor contacted to address keys not returned.
    ii. If a supervisor fails to recover keys from a departing employee, Public Safety will assess the vulnerability of spaces under control of the terminated employee and order rekeying/lock changes as appropriate. The assessment will include consultation with the Key Distribution Office to ensure all impacted spaces are assessed. Any rekeying or lock changes required due to failure to recover keys will be completed at department expense.

II. **KEY REQUEST AUTHORITY**

a. The authority to request a key is relative to the level of access afforded a particular key; thus master keys require a higher level of approval than individual office keys.
b. Key request authority for master keys cannot be delegated and require the specific approval of the authorizing authority.
c. Required approval authority for key requests is listed in APPENDIX C, Master Keying Matrix and Key Request Authority.
d. Vice Presidents and Deans will complete an authorization list of all personnel authorized to complete key requests. The Department of Public Safety will maintain these forms and refer to them when reviewing key requests. A sample authorization list is provided as APPENDIX D.

III. **ELECTRONIC ACCESS CONTROL**

a. Electronic access control is installed in campus buildings to reduce the number of keys issued to community members and enhance security through the centralized management of access privileges and locking of buildings and key interior spaces.
b. Installation, access privileges, and system maintenance are discussed in the Procedures section, paragraph IV.