Rule R3-234A: Building Access and Surveillance Systems

Revision 0. Effective date: March 12, 2019.

I. Purpose and Scope 1

II. Definitions 2

III. Rule 2

A. Administrative responsibility and funding for Building Access and Surveillance Systems. 2

B. Registration and Approval of Surveillance Systems. 3

C. Key Systems. 4

IV. Policies/ Rules, Procedures, Guidelines, Forms and other Related Resources 5

V. References 5

VI. Contacts 6

VII. History 6

I. Purpose and Scope

A. Purpose.

This Rule implements University Policy 3-234 Building Access and Surveillance Systems. The purposes of this Rule are to regulate the installation and operation of building access systems (including building key systems and electronic access and associated management interfaces), regulate the installation and operation of surveillance systems, and regulate the collection, storage, and use of surveillance

data collected through system surveillance systems for University buildings and outdoor areas.

B. Scope.

This Rule regulates building access systems and surveillance systems with a primarily fixed location at a University building or outdoor area.

II. Definitions

The definitions provided in Policy 3-234 apply for this rule.

III. Rule

A. Administrative responsibility and funding for Building Access and Surveillance Systems.

1. Administrative responsibility for systems.

a. Departments operating surveillance systems registered with and approved by the Surveillance Systems Administrators Committee (SSAC) are responsible for the installation, management, maintenance, and use of surveillance software (which ordinarily will be carried out by the department's designated Information Technology staff). And see Policy 3-234-III-B-2-b, prohibiting the operation of any system which has not been registered and approved, unless exempted.

b. Each surveillance system monitoring activity in an area which has been designated by the DPS as a Public Safety Space will ordinarily be centrally managed, by the Campus Building Access Team.

2. Funding of Systems.

a. Initial acquisition and installation costs and renovations of both building access systems and surveillance systems are funded through various sources apart from ongoing operations and maintenance.

b. After initial installation, the designated [Facility Steward] for a building ordinarily manages the operation and maintenance, and routine

replacement of building access systems and surveillance systems for that building, funded through per-device fees and other fund allocations within the purview of the [Facility Steward].

c. The Campus Building Access Team reviews actual costs and projections annually for the operations and maintenance of Electronic Access Control and Surveillance Systems and proposes fee adjustments. The Vice President for Administrative Services approves such adjustments.

d. Devices providing electronic access or surveillance for areas designated as Public Safety Spaces, and other areas ordinarily used by the general public, are funded from the General Fund. Other devices are funded by the department using those devices. Departments are responsible for damage and costs resulting from unauthorized installations.

B. Registration and Approval of Surveillance Systems.

1. The following exemptions from the otherwise applicable surveillance system registration requirements of Policy 3-234-III- are hereby granted.

a. Clinical Patient Care.

i. Monitoring patients under medical care by authorized medical professionals.

b. Human Subject Research.

i. Research authorized by the Institutional Review Board for Human Subject Research.

c. Teaching and Learning.

i. Recording for instructional purposes as part of an approved University of Utah course, under supervision of the course instructor.

d. Video Conferencing.

i. Meetings conducted through electronic devices where all parties are aware of being recorded.

e. Personal Communication Devices (i.e., smart phones) and others, as specified by the SSAC.

C. Key Systems.

1. A key system consists of mechanical locks and keys, including master keys.
2. Each building key system for a University facility must meet campus design standards and be approved by the applicable Facility Steward.
3. Initial key systems, including keys for the initial set of authorized users, are ordinarily provided in conjunction with the construction or renovation project, with costs for the keys included in the project costs.
4. Replacements for lost keys are provided by the Campus Building Access Team, with replacement costs billed to the requesting department. Replacements for broken or faulty keys which are returned are replaced at no cost to the requesting department.
5. If a University-owned or -occupied facility has been identified as a “security risk” such that changing locks becomes necessary, then the building occupant responsible for the risk is liable for the resulting costs. The SSAC, along with input from Risk Management and Property Accounting, will determine whether a facility is such a security risk. Considerations in this determination may include, but are not limited to:
   a. number or type of keys unaccounted for or lost;
   b. theft or vandalism risk;
   c. life safety concerns;
   d. sensitive, technical, proprietary, or high-value equipment.
6. Departments are required to account for keys annually, or as requested by the Campus Building Access Team or the Department of Public Safety.
7. Departments are responsible for returning keys when access is no longer required.

8. All key users (persons to whom any key is issued) must be approved by an Approving Officer (as defined in Policy 3-234) or their designee.
9. Prior to authorizing keys, an Approving Officer or designee must have completed the University-authorized access security training within the past two years.
10. Master keys are issued to individuals only upon receiving the appropriate authorization. The level of required authorization is based on the type of master key, as follows:
    a. Master keys covering multiple buildings and/or electronic access override keys, Surveillance System Administrators Committee (SSAC)
    b. Building master for multi-department building, cognizant vice president for each department.
    c. Building master for single department building and/or department master within multi-department building, Approving Officer
    d. Other keys (building entrances, department sub-master, offices etc.), Approving Office or authorized representative.

Sections IV- VII are for user information and are not subject to the approval of the Academic Senate or the Board of Trustees. The Institutional Policy Committee, the Policy Owner, or the Policy Officer may update these sections at any time.

IV. Policies/ Rules, Procedures, Guidelines, Forms and other Related Resources

A. Policies/ Rules.
    1. Policy 3-234: Building Access and Surveillance Systems

B. Procedures, Guidelines, and Forms. [*reserved*]

C. Other Related Resources. [*reserved*]

V. References

A. [*reserved*]

VI. Contacts

The designated contact officials for this regulation are:

A. Policy Owner(s) (primary contact person for questions and advice):

1. Systems: Executive Director of Facilities Management
2. Data: Chief of Police

B. Policy Officer(s): Vice President for Administrative Services

See Rule 1-001 for information about the roles and authority of policy owners and policy officers.

VII. History

Revision History.

A. Current version. Revision 0.

1. Approved by the Academic Senate on January 7, 2019, and the Board of Trustees on March 12, 2019 with effective date of March 12, 2019.
2. Legislative History
3. Editorial Revisions

B. Previous versions.

C. Renumbering

1. Not applicable.