Policy 3-234: Building Access and Surveillance Systems. Revision 7.

I. Purpose

A. Purpose

This Policy and associated Regulations regulate the installation and maintenance of building access systems and area surveillance systems in buildings and outdoor areas owned or controlled by the University of Utah, and regulate the collection, storage, disposal, access, and use of surveillance data from those systems.

[The Surveillance System Administrator Committee (as defined below) shall during spring 2020 review this Policy and the system registration process it creates, and present to the Academic Senate by October 2020 a report with recommendations, including any recommendations for revision of this Policy and associated Regulations. The report shall be provided to the Board of Trustees. Further, as provided in this Policy, the SSAC shall also thereafter at least annually present a report to the Senate.]

B. Scope

The provisions of this Policy regulating installation and maintenance of building access systems and surveillance systems apply for all buildings or outdoor areas controlled by the University (except for premises leased to and controlled and occupied by non-University entities). These covered areas include all locations where the University of Utah Department of Public Safety has a security presence and responsibility. The provisions of this Policy regulating collection, storage, disposal, access, and use of surveillance data apply to all University departments and contracted entities conducting University activities, regardless of location.

*[**User note:** This Policy and its associated Rules replace the former University Key Policy 3-234, as of 2019. The current version of this Policy is primarily intended to regulate surveillance systems that are of primarily fixed locations. It is anticipated that a revised regulation will subsequently be developed regarding University surveillance systems which are primarily mobile, including cameras mounted on Unmanned Aircraft (i.e., drones, see Utah Code Ann. 72-14-101), and wearable camera devices operated by*

Department of Public Safety personnel (i.e., body cameras). Contact the Department of Public Safety for further information. Also there may be subsequent development of a regulation regarding special-purpose surveillance systems temporarily deployed for short-term events, such as events involving gatherings of large crowds.].

II. Definitions

For the limited purposes of this Policy and any associated Regulations, these words and phrases have the following meanings:

A. Approving Officer – A University officer holding the position of Department Head or higher.

B. Building Access System –Key System (consisting of mechanical locks and keys, including master keys), and other devices, including an Electronic Access System, utilized to control access to a door or an area.

C. Campus Building Access Team– The team within the Facilities Management Department (reporting to the Vice President of Administrative Services) that provides the central administration of the integrated surveillance and access systems for general campus and DPS-designated Public Safety Spaces.

D. Criminal activity— Conduct which is punishable under the criminal laws applicable for the locations and persons involved—including the Utah Criminal Code and applicable federal law for activity occurring in Utah, and the laws of the applicable jurisdiction for activity occurring outside of Utah.

E. DPS – Department of Public Safety – The University of Utah department incorporating campus police and security services.

F. Electronic Access Control System – The hardware and software that control door access.

G. Electronic Access Control Operator – An approved University employee who manages access rights of users through the Electronic Access Control System.

H. Facility Steward – The facilities department or person with primary stewardship responsibility for a particular building or area.

I. General Fund – The University's general operating budget funded through state, tuition, and other sources.

J. Public Safety Space – An indoor or outdoor space that is accessible to the general public and is designated by DPS as a public safety space based on a determination of significant potential risks for criminal activity.

K. SSAC – Surveillance System Administrators Committee– A committee established under authority of this Policy with assigned responsibilities for implementation of this Policy and associated Regulations.

L. Surveillance Data – Any electronic, printed, audible, visible or other form of information captured by a Surveillance System, including any record of user access generated through a Building Access System

M. Surveillance System – A system capable of monitoring and recording the presence or activity of persons in a given physical area of a University building or outdoor area. [This does not include an employee time clock system through which specific employees are required to register their presence at a work-site, for the specific purpose of tracking their work hours; and the data regarding employee presence collected through such a system is not considered Surveillance Data for purposes of this Policy.] The current version of this Policy is intended to regulate systems which are of *primarily fixed locations*, not including systems which are *primarily mobile*.

*[**User note:** it is anticipated that a revised regulation will subsequently be developed regarding University surveillance systems which are primarily mobile, such as body cameras, drones, etc.]*

N. Surveillance System Device –A camera, microphone, video or audio data recording equipment, key card reader, or other type of device which is a component of a Surveillance System.

III. Policy

A. Surveillance System Administrators Committee (SSAC).

The SSAC is hereby established as a University Committee. Its membership and leadership shall be appointed by the President of the University. Members shall include: (i) appropriate representation, as determined by the President, from among the following (or equivalent offices): Campus Building Access Team, the Department of Public Safety, the Office of General Counsel, the offices of the Senior Vice Presidents for Academic Affairs or Health Sciences, Hospitals and Clinics administration, and the office of the Vice President for Student Affairs; (ii) a representative of staff employee interests (selected in consultation with the Staff Council); (iii) a representative of student interests (selected in consultation with the Associated Students of the University of Utah); and (iv) two Tenure-line or Career-line representative(s) of the University faculty recommended to the President by the Senate Personnel and Elections Committee, who shall serve for terms of three-years and may be recommended and reappointed for additional terms without limitation. The President of the Academic Senate, or designee(s), may substitute as needed in the absence of the faculty representatives.

The SSAC shall have the functions described in this Policy and associated Regulations and otherwise assigned by the President. It shall receive administrative support from and regularly report to the Vice President for Administrative Services (or equivalent). At least annually a summary report of the SSAC's recent activities shall be presented for the information of the Academic Senate. In addition, any member of the SSAC may at any time inform the Senate President, who may in turn

inform the Senate Executive Committee, of any significant concern regarding any activities overseen by the SSAC, including a concern of inadequate protection of privacy of individual members of the University community.

B. Registration, approval, installation and operation of building access systems and other surveillance systems.
   1. General provisions.
      a. There are broadly two categories of building access systems and other surveillance systems in use at the University:
         i. main central systems which are operated centrally under auspices of the Campus Building Access Team, typically controlling access to or surveilling designated Public Safety Spaces, transit hubs, and other general usage campus areas, and
         ii. systems which are dispersed among various buildings and facilities in various locations of the campus, with each system being operated under auspices of a particular Facility Steward responsible for the particular building or facility.

         Systems of both categories must only be operated in accord with the fundamental principles underlying this Policy. To ensure enforcement of that requirement for the various dispersed systems, the University establishes and charges the SSAC to oversee a central registry and approval process for such systems.

   2. Central registry and approval of building access systems and other surveillance systems.
      a. The University will maintain a central registry and approval process for building access systems and other surveillance systems, which will be administratively situated within an office reporting to the Vice President for Administrative Services (or equivalent), and will operate under oversight of the SSAC. The SSAC shall develop procedures and criteria for the systems registry and approval process, consistent with this Policy,

including a timetable with deadlines for registration of various types of systems.

b. Each unit of the University operating any building access system or other surveillance system shall by the established deadline submit an application for registration and approval of that system (unless exempted in accord with this Policy and associated Regulations). This includes any system purchased or installed directly by any department, as well as any system provided through third parties. After the established deadline, unless exempted, no unit or person shall operate any pre-existing or any new building access system or other surveillance system at the University, or continue to store or use any surveillance data collected through such a system, unless the system has been registered and approved according to the SSAC-approved procedures.
c. Certain systems, or particular uses for surveillance systems may be exempted from this registration and approval requirement, consistent with the purposes of this Policy, as shall be further described either in a University Rule associated with this Policy, or described in a University Procedure approved by the SSAC.
d. For each registered and approved system, the [Facility Steward] (or equivalent responsible position) shall periodically provide updated information about the operation and monitoring of the system, at a time determined by the SSAC, and the system shall be reviewed for renewal, on a schedule determined by the SSAC (ordinarily no less frequently than every five years). The SSAC has full discretion to require a review of any system at any time, including in response to a concern about improper operation reported by any concerned person. A review shall be based on the then-current approval criteria.
e. After any review, if the SSAC finds that a system is not in substantial compliance with the then-current approval criteria, the SSAC may require that operation of the system be ceased. A decision of the SSAC regarding approval, or cessation of operations of any system, is subject only to an

appeal to the Vice President for Administrative Services (or equivalent officer), whose decision is final.

f. The SSAC shall develop and implement a set of criteria for determining which University employee positions and individual employees shall be authorized to operate surveillance systems or access University surveillance data for University purposes, including criteria for training of employees for such specific responsibilities, and for auditing of compliance, and it shall include in the registry a current list of such authorized personnel.

g. The central registry, and the periodic regular reports of the SSAC, shall be considered public records, reviewable on request of any member of the University community in accord with the Government Records Access Management Act, except to the extent that the Office of General Counsel determines that any particular contents of such records should be redacted in accord with applicable provisions of GRAMA.

C. Principles and criteria for approval and ongoing operation of building access and surveillance systems.

The following principles, restrictions, and other criteria apply for those dispersed systems operated under auspices of a particular [Facility Steward] which are required to be registered and approved through the central registry described in Part III-B above, and the approval process shall ensure compliance with these requirements. Unless otherwise indicated, they also apply for main central building access and surveillance systems which are operated centrally under auspices of the Campus Building Access Team.

1. Principles for operation of building access and other surveillance systems, and collection, storage, disposal, access, and use of surveillance data.
   a. As an institution of higher education, including academic health sciences, with multiple missions, it is a fundamental principle that the University

recognizes and respects rights of privacy of individual persons who enter various areas of the University campus to participate in University activities, including students, faculty members and staff employees, health care patients, and guest visitors entering for lawful purposes. It is also fundamental that the University seeks to ensure for all such persons a campus environment that is safe from criminal activity and other causes of harm to their persons or loss or damage of their personal property. And as a steward of public resources, the University seeks to prevent loss or damage of University controlled property resulting from criminal activity or other causes. The University regulates and operates building access systems and other surveillance systems so as to best serve the combined objectives—balancing personal privacy, security and safety, and resource protection.

b. University personnel are required to operate such systems in compliance with applicable federal, state, and local law and in accord with University Regulations. This Policy and associated University Regulations shall be interpreted to comply with such applicable laws, whether currently existing or subsequently enacted, including federal and state constitutional provisions, the Family Educational Rights and Privacy Act (FERPA) regarding student records, the CLERY Act regarding campus safety and security, the Health Insurance Portability and Accountability Act (HIPAA) regarding health care patient information, and the Utah Governmental Records Access and Management Act (GRAMA) regarding records of the University as a governmental entity.

c. For purposes of exercising control over the collection, storage, disposal, access, and use of surveillance data, for any surveillance data gathered at any University-controlled space, through any surveillance system operated or controlled by the University, the University considers such data to be

the exclusive property of the University of Utah, and not the property of any University employee or contractor.

2. Restrictions on system placement and operation, and data collection, storage, disposal, access, and use.
   a. Surveillance data may only be collected in compliance with this Policy and associated Regulations, and only through a surveillance system that has been registered with and approved by the SSAC (unless exempted). Any collection of surveillance data by any other means is prohibited.
   b. Unless otherwise specifically authorized in advance for a particular compelling purpose by the SSAC and the University General Counsel, and the Vice President for Administrative Services (or equivalent)]:
      i. each surveillance system shall include appropriate signage or by other means shall provide reasonable notice of the system's existence, for persons who are subject to the surveillance while present for lawful purposes.
      ii. no surveillance system shall ever be used to collect video surveillance data from any area which is essentially a private space, including the interior space of any restroom, shower or dressing room, lactation room, or individual office of a faculty or staff member, and in the event surveillance data from an essentially public area contains private information, or information to which a reasonable expectation of privacy may attach, such as library records which identify a library patron, such surveillance data should only be reviewed in consultation with the Office of General Counsel; and
      iii. no surveillance system shall ever be allowed to collect from any location audio surveillance data of discernable human voices;
   c. Permissible and prohibited uses and purposes for surveillance data.
      i. The University may ordinarily access and use surveillance data only for the limited purposes of deterring, detecting, or investigating ***criminal activity***, as a means of providing a campus environment that is safe and secure for students, employees and visitors visiting for lawful

purposes, and protecting University resources and the property of members of the University community from loss or damage.

ii. ii. Further, under the following restrictions, specifically designated University administrative units may be authorized to have limited access and uses of surveillance data for the following limited types of purposes ***not limited to criminal activity*****.** Each authorization of such a type of use and purpose must be approved in advance by the SSAC and the University General Counsel and the Vice President for Administrative Services (or equivalent), and only with a specific determination by the SSAC that authorizing the particular type of use is consistent with the basic principles of this Policy, including appropriate protection of individual privacy, and serves a compelling need for the University. Such an authorization may be made permanently applicable for a defined category of uses by a specified office as described in a University Procedure, or may be time-limited as for a specific incident documented using a form approved by the SSAC. For an administrative investigation of a specific incident, the authorization shall require that access and use of the data be limited only for the purposes of that investigation and only for the time period reasonably necessary. All such authorizations shall be described in the reports of the SSAC presented periodically to the Academic Senate (without revealing confidential information).

    a. An administrative investigation of a potential violation of a non-criminal law or external regulation which is directly applicable to the University or University personnel, if such a violation presents a substantial risk of serious harm to the University or any individual (e.g., federal or state regulations regarding storage of controlled substances, or hazardous materials).
    b. An administrative investigation of a potential violation of a University Regulation involving a type and degree of non-

criminal misconduct which presents a substantial risk of serious harm to the University or an individual (e.g., posting racially derogatory materials in a University work- or learning-space to create a hostile work/ learning environment for University employees or students; or operating or storing a wheeled riding device in a dangerous manner or in a prohibited zone).

c. An administrative investigation by a student-services office regarding a potential disappearance of a campus-resident student, in circumstances in which the student may be at risk of serious harm (e.g., a student housing administrator investigating concerns of a minor student's family about the student's well-being after a long period without contact).
d. A practice of routinely monitoring the presence of University employees or other individuals in specific locations of a facility of the University Hospitals and Clinics, for the limited purposes of protecting patient safety and ensuring compliance with applicable safety regulations.
e. A practice of routinely monitoring the presence of University employees or other individuals in specific locations of a University facility with restricted access, in circumstances in which such monitoring is necessary to comply with directly applicable external laws and regulations or University Regulations such as for protection of sensitive data or regulated technology, or control of special materials (e.g., University Policy 4-004 Information Security; Policy 7-007 Export Control Compliance; Policy 3-300 University Health and Safety.

iii. The University will not access or use surveillance data (from building access systems or other surveillance systems) for the purposes of

a. monitoring an individual student's compliance with course attendance requirements, or
b. monitoring an individual employee's compliance with workplace attendance expectations (except as may be specifically authorized for safety or regulatory compliance purposes in a specific facility under section ii-d or e above).

iv. The University will not use a surveillance system for monitoring the movements or otherwise tracking the location of any individual member of the University community except for the limited purposes authorized under III-C-2-c-i & ii above, or in compliance with a search warrant or any judicially recognized exceptions to warrant requirements.

v. The University will not use facial recognition computer software or equivalent information technology to process video surveillance data to track the presence at a campus location of a particular person for any purpose other than addressing criminal activity which presents a substantial risk of serious harm to the University or an individual (e.g., a credible threat of a terrorist attack by an identifiable individual at a high-population event on campus).

vi. The University may also use certain anonymized surveillance data for limited administrative purposes of identifying typical patterns of use of University facilities, to aid in design and planning of the campus environment (such as designing pedestrian walkways to best accommodate pedestrian traffic flow in observed high traffic areas). Such uses must be approved by the SSAC in advance on a case-by-case basis, and only with appropriate safeguards for privacy of individuals.

vii. Any other uses of surveillance data by the University shall be allowed only for the limited purposes and to the limited extent required by applicable federal, state, or local law, and each such use shall, to the full extent allowed under that applicable law, be promptly reported to the SSAC with an explanation of its purpose and legal justification.

viii. Targeting individuals based on race, ethnicity, disability, gender, nationality, religion, or other protected classifications in collecting and using surveillance data is prohibited.

a. For surveillance systems in areas that are ordinarily used only by particular small groups of University personnel (such as a building section primarily used only by faculty and students of one small academic department), the University encourages that representatives of those regular users of the area be consulted about the initial installation or substantial modification of features of such a surveillance system.

d. The following requirements apply for persons operating surveillance systems or otherwise having regular access to surveillance data.

i. Ordinarily, only University employees qualified in accord with SSAC-approved criteria shall operate surveillance systems or access surveillance data.

1. Electronic Access Control operators must be University employees appointed by Approving Officers (as defined above).
2. Surveillance system operators must be University employees appointed by Approving Officers.
3. Access to surveillance data shall be granted only to University employees so authorized by the SSAC, and only for purposes approved in accord with this Policy.
4. A list of University employee positions and individuals qualified for these responsibilities will be maintained in the SSAC's registry of systems (see Part III-B above).

ii. If approved in advance by the SSAC, a particular surveillance system over which the University has authority may be operated by non-University personnel, in circumstances in which the University contracts with a vendor to provide such system operating services at a specific facility not located on the University's main campus. For example, the SSAC may approve operation of such a system at a distant facility occupied by a University field research station, or a unit of the Hospitals and Clinics. For each such vendor-operated system through which surveillance of members of the University community regularly occurs: (a) the system shall be registered with and approved by the SSAC (unless expressly exempted in accord with Part III-B-2-c of this Policy); (b) the system shall be operated in accord with all relevant provisions of this Policy other than the requirement of operation solely by University personnel (except any provision expressly excluded by the SSAC); and (c) the arrangement with the vendor shall be described in a written contract between the University and the vendor filed with the SSAC.

e. All surveillance data must be stored only on a secure server. The data shall be retained only for the specified retention period for that type of surveillance system (as approved by the SSAC and specified in a University Procedure), and after expiration of that period the data shall be deleted, unless it is marked and saved for an approved purpose. Deletion shall ordinarily occur through an automatic erasure process. The SSAC shall specify a permissible retention period for each type of surveillance data and each type of surveillance system, which the SSAC shall determine based on the surveillance system's location and purpose. The retention periods for centrally operated main systems shall be specified in a University Procedure approved by the SSAC. The retention period for each other (dispersed)

system shall be described in the documentation of the registration and approval of the system by the SSAC.

f. Bookmarking or saving surveillance data beyond the specified retention period may only be performed by an approved system administrator, and may only be done with specific approval from the SSAC, which approval shall be granted only on a case-by-case basis and only for purposes permitted under this Policy.

g. The University will release surveillance data to a non-University agency or person (such as a law-enforcement agency) only to the limited extent the University is required to under the terms of the Utah Government Records Access and Management Act (GRAMA), or other directly applicable state, federal, or local law.

   i. When releasing surveillance data in compliance with GRAMA or other such applicable law, the University will to the full extent permissible under such law protect the privacy of individual members of the University community and visitors visiting for lawful purposes. In particular, the University will protect privacy of students by complying with any applicable requirements of the Family Educational Rights and Privacy Act (FERPA) for any release of surveillance data regarding a student.
   ii. Unless prohibited from doing so by the applicable law, the University will: make reasonable efforts to give notice of the planned release to any individual member of the University community who is an identifiable subject of the surveillance data involved; allow such person an opportunity to comment regarding the planned release; and accommodate any lawful reasonable request for managing the release so as to best protect that individual's privacy. In-particular the University will comply with applicable pre-release notification

requirements of the Family Educational Rights and Privacy Act (FERPA) regarding student records.

h. An individual member of the University community who seeks to access and use surveillance data from the University for purposes of conducting academic research will ordinarily be required to submit a request through the GRAMA process for obtaining University records. The request will be subject to the same restrictions and requirements as a request made by a non-University party. Additionally, any use of such data involving research with human subjects will be subject to University requirements for such research, which may include review by the Institutional Review Board.

i. University personnel who misuse surveillance data or facilitate the misuse of surveillance data by another person are subject to discipline under applicable University Regulations, including provisions of the Student Code, the Faculty Code, or the Corrective Action and Termination Policy for Staff Employees. Such misuse may also be subject to criminal penalties or civil liability under applicable law. The University may audit any surveillance system at any time to detect improper system operation or misuse of data.

3. Other criteria.

The installation and operation of each building access system and each surveillance system must be consistent with design standards approved by the SSAC. Those design standards must include provisions ensuring appropriate security of the surveillance data, which provisions shall be consistent with Policy 4-004: University of Utah Information Security Policy, and University Rules associated with that Policy.

*[**Note:** Parts IV-VII of this Regulation (and all other University Regulations) are Regulations Resource Information – the contents of which are not approved by the Academic Senate or Board of Trustees, and are to be updated from time to time as*

determined appropriate by the cognizant Policy Officer and the Institutional Policy Committee, as per Policy 1-001 and Rule 1-001.]

IV. Rules, Procedures, Guidelines, Forms, and other related resources.

A. Rules
Rule 3-234A: Building Access and Surveillance Systems

B. Procedures *[Reserved]*

C. Guidelines *[Reserved]*

D. Forms *[Reserved]*

E. Other Related Resource Materials *[Reserved]*

V. References

Policy 1-011: Campus Security

Procedure P1-011A: Campus Security

University Rule 4-004F: Physical and Facility Security

VI. Contacts

The designated contact officials for this Policy are:

A. Policy Owners (primary contact persons for questions and advice):

Systems: Executive Director of Facilities Management

Data: Chief of Police, Dale Brophy dale.brophy@dps.utah.edu 801-585-2677.

B. Policy Officers: VP for Administrative Services, John Nixon john.nixon@utah.edu 801-585-0806.

These officials are designated by the University President or delegee, with assistance of the Institutional Policy Committee, to have the following roles and authority, as provided in University Rule 1-001:

> *"A 'Policy Officer' will be assigned by the President for each University Policy, and will typically be someone at the executive level of the University (i.e., the President and his/her Cabinet Officers). The assigned Policy Officer is authorized to allow exceptions to the Policy in appropriate cases... . "*
>
> *"The Policy Officer will identify an "Owner" for each Policy. The Policy Owner is an expert on the Policy topic who may respond to questions about, and provide interpretation of the Policy; and will typically be someone reporting to an executive level position (as defined above), but may be any other person to whom the President or a Vice President has delegated such authority for a specified area of University operations. The Owner has primary responsibility for maintaining the relevant portions of the Regulations Library... [and] bears the responsibility for determining which reference materials are helpful in understanding the meaning and requirements of particular Policies... ." University Rule 1-001-III-B & E.*

VII. History

A. Current version: Revision 7.

Approved by the Academic Senate January 7, 2019.

Approved by the Board of Trustees March 12, 2019.

Legislative History for Revision 7

B. Earlier versions: Beginning with Revision #7, this replaces former Policy 3-234 Key Policy.

Revision 6: Approved by Board of Trustees April 12, 2011, Adding text removed from Policy 4-005 Rev. 4, see Executive Summary. Also reformatted to comply with format standards.

Legislative history for Revision 6: Memorandum February, 11, 2011.

Revision 5: Approved July 8, 1996