**University Procedure 3-234A**

**Registration and Approval of Building Access Systems and Surveillance Systems**

To implement University Policy 3-234 and University Rule 3-234A, as enacted [January 2019].

Approved by the Surveillance System Administrators Committee (SSAC), date\_\_\_\_

[*EXAMPLE ONLY FOR DISCUSSION PURPOSES--- DRAFT 2018-12-28*]

1. **Overall timetable for initial registration and approval, and periodic renewal reviews, of the various systems.**

**Phase 1. All systems are to be *initially inventoried* by \_\_\_\_\_[date]**. Inventorying occurs by system operators providing to the SSAC a brief general description using the SSAC approved form. Being merely included in this inventory does not constitute SSAC approval of any system as meeting the criteria under Policy 3-234 for continuing operation.

**Phase 2. Groups of systems begin approval process, on staggered deadlines.** The SSAC organizes the previously inventoried list of systems into appropriate groupings, develops a series of staggered deadlines, assigns a time period for the operators of the systems in each group to submit an application for approval, and notifies the operators of their timelines. Organizing the systems into groups with staggered timelines allows the SSAC to do its review work at a reasonable pace, rather than having the entire list of systems arriving for review in one brief period. The SSAC may also find that these groupings will be useful for setting staggered timelines for required renewals of registration & approvals in subsequent years. E.g., systems in one group might be scheduled to undergo a renewal review two years from the original, another group in the third year, etc, so that the renewal work for the SSAC will be staggered and paced, rather than having the reviews of every system occur at the same time. Some flexibility on this scheduling is best left to the SSAC to adapt as it learns from experience in the first years of operating the registry.

**Phase 3. Systems, by groups, on established dates, are considered for approval by the SSAC, and approved if criteria are met. For noncompliant systems, efforts are made to correct deficiencies, and if compliance is ultimately not attained those systems are shut down.** System operators complete and submit their approval applications according to the staggered schedule (using SSAC approved form). The SSAC reviews applications, and for those systems which meet the established criteria, they are placed on the approved registry and permitted to continue operating (until their scheduled renewal review). For any system which has an incomplete application, or otherwise fails to meet criteria, the SSAC withholds approval, and attempts to work with system operators to correct deficiencies. If satisfaction of approval criteria can eventually be demonstrated, SSAC will register the system as approved and schedule it for the appropriate renewal period. If the SSAC determines that any system will not brought into compliance with the approval criteria within a reasonable time, the SSAC will deny approval, categorize it accordingly on the registry, and require that operation of the system be ceased.

**Phase 4. Renewal reviews are scheduled and conducted.** All systems after initial approval and listing on the registry are required to go through a summary renewal review process no less frequently than every [five] years. On the staggered schedule set by the SSAC, and using an SSAC-approved renewal application form using then-current approval criteria, each system’s operator applies for renewal. The SSAC reviews, approves renewal of compliant systems, and works with operators to correct deficiencies of non-compliant systems (or requires shut-down of systems which are not made compliant within reasonable time).

The SSAC may also choose to do spot checks of compliance of any systems, at any time, including at the time of scheduled renewal. And any member of the University community concerned about improper operation of any system or misuse of surveillance data may at any time recommend to SSAC that it review a particular system. SSAC has the authority and discretion to review any system at any time, including auditing the automated records of access to stored data, and the authority to require any non-compliant system to be brought into compliance or to cease operation— subject only to appeal to the Vice President for Administrative Services, whose decision is final, as per Policy 3-234.

 [Note that by provisions in Policy 3-234, a full report on the implementation of the revised Policy and the registration & approval process will be presented to the Academic Senate by {October 2020}. And on an ongoing basis beginning 2019 there are to be annual summary reports to the Senate on the activities of the SSAC.]

1. **Checklist of criteria for approval of surveillance systems at time of initial approval, and on renewal for continuing operation.**

 \_\_\_\_ Compliant with all applicable federal, state, and local laws (including FERPA, Clery, HIPAA and GRAMA).

 Compliant with Policy 3-234 requirements, including:

 \_\_\_\_ system meets SSAC-approved system design standards

 \_\_\_\_ adequate signage or other appropriate means of notifying surveilled persons of the existing of the surveillance (e.g., signs indicating presence of cameras. Balancing sufficient number and visibility of signs, without undue expense for the University).

\_\_\_\_ qualifications of system operators/persons with routine access to data

\_\_\_\_ security of data storage servers and otherwise secure handling of data

\_\_\_\_ data retention period & assured deletion of aged-out data appropriate for the particular type of system (see standard periods in this Procedure below)

\_\_\_\_ restrictions on bookmarking or saving data beyond ordinary retention period

\_\_\_\_ restrictions on collecting audio data, data from essentially private spaces (e.g. individual faculty offices), & private information from otherwise essentially public areas

\_\_\_\_ history of and continuing commitment to allowing only proper uses of collected data (crime detection & deterrence, safety & security, [[or other SSAC approved limited administrative purpose]]).

 ----- other specific criterion approved by the SSAC, consistent with principles of Policy 3-234. Describe & explain\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

\_\_\_\_ Overall, consistency with Policy 3-234 underlying principles of protecting privacy of individuals to fullest extent possible while providing safe & secure campus environment.

1. **Retention periods for stored surveillance data, based on the type of surveillance system and use of such date.**

The following are the maximum periods that stored surveillance data may ordinarily be retained. Any exception of saving data longer than this period must be approved in advance by the SSAC, either through approval of the system plan at time of registration, or approval for a specific instance case-by-case.

Type of system Ordinary maximum retention period

 [EXAMPLE--TBD ] [EXAMPLE --TBD ]