Harvard Law School Video Security Management Program Overview

GENERAL PRINCIPLES

The purpose of installing video management infrastructure at the Harvard Law School is to enhance the safety and security of the community, reduce institutional risk, and aid in the prevention and investigation of crime at the School or against members of the HLS community. The privacy of the community members is a fundamental principle in the design and implementation of the video management system across campus.

The School maintains a single video management system. Programs and other sub-units within the School are not permitted to install their own video systems for any purpose. The HLS video management system will be operated in view of the University's Video Camera Policy (Policy on Installation and Use of Video Cameras).

PERMITTED LOCATIONS

Important elements such as security, privacy, fields of view, mounting conditions, and aesthetics are considered before particular camera installation is proposed. In general, plausible camera locations are likely to include:

- Building entries, lobbies, outdoor areas, loading docks, technology operations spaces, or other areas of vulnerability.
- Installation of cameras will be a transparent process. In most cases, occupants are informed of camera installations in the building where they work.
- All cameras must be in plain view for the community to easily identify. Covert cameras are not permitted unless authorized for a purpose which is limited in scope, for a specific period of time, and requested by the Harvard University Police Department or the Office of the General Counsel.
- Decoy, fake, or otherwise inoperable cameras are not permitted.
- Insofar as any installed cameras are equipped with the capacity for audio detection, that capacity will be disabled.

Video equipment may not be installed in locations where there is a reasonable expectation of privacy such as:

- dormitory rooms
- the living quarters of other residential facilities
- restrooms and bathing facilities
- locker rooms and other changing facilities
- classrooms
- offices of individuals, with the exception of certain office spaces in which high-risk transactions occur (such as cash management or storage locations for high value/sensitive assets)

AUTHORIZATION, OPERATION, AND ACCESS TO VIDEO

Guidelines for the installation and alteration of video security equipment are specified in Section D of the University's Video Camera Policy. All video camera installations are to be authorized by the HLS Dean for Administration.

The HLS video management system will be operated in accordance with Section E of the University's Video Camera Policy:

- Installations authorized will be coordinated by the Director of Facilities and Operations.
- HLS Information Technology Systems Administrators will be authorized to access the video security system to perform administration, maintenance and updates.
- Cisco Systems will have periodic access to the video security system to properly maintain the system.
- Video servers will be stored in a secure location with limited access.
- All video images will be transmitted via a secure virtual local area network.
- Video images will be stored for thirty (30) days.
- All user access will be logged and managed per University guidelines.

Video camera data maybe accessed for purposes specified in Section F of the University's Video Camera Policy. The Dean, Dean for Administration, HUPD or OGC can review and approve all requests for a search. In the case of an approved search, the Dean of Administration will assign one staff person to access the video security system as specified herein.

In each case where video is accessed, the individual accessing the system shall keep an appropriately detailed record including name, access date, time, purpose, location, data searched, relevant data found, any further use or distribution of the data or relevant information.

Updated August 1, 2016