DIVISION OF
PUBLIC SAFETY & SECURITY
UNIVERSITY OF MICHIGAN

Security Camera Technical Standards

Section 1: General Technical Specifications

1. Security camera systems may take the form of standalone Digital Video Recorders (DVR), standalone Network Video Recorders (NVR), or IP cameras connected to a University enterprise video system. No private company or contractor hosted system shall be deployed.
2. DVR and NVR systems shall be secured by credentials. Default passwords shall be changed and recorded with the system manager. Embedded or other operating systems shall be maintained with all available security patches and fixes and firmware; security system applications shall be kept up to date with the latest version as soon as reasonably possible.
3. Access levels shall be used to protect access to system configuration, specific camera groups or partitions, based on the role of the user.
4. Access credentials shall be person specific, using the University issued uniqname whenever possible.
5. Access log capability shall be present and enabled.
6. Access logs shall be maintained for one year
7. Camera hardware shall be protected from access directly or indirectly from outside the configured video system. All camera default passwords, if any, shall be changed and recorded with the manager of the video system.
8. Whenever possible, camera systems shall be integrated or provide an alerting function to indicate an event to direct camera operators to the specific event. This can be provide by the following:
    a. A duress button or intrusion monitoring system connected to the University's MOSCAD alarm system
    b. Access control events from a campus access control system
    c. Areas of rescue assistance phones
    d. On-board camera analytics, such as motion detection

Section 2: Image and Recording Standards

1. Cameras shall be chosen based on suitability for the environment to be installed. While no one set of performance standards will be applicable in all installation scenarios, forensic significant imagery should be obtained by following the following guidelines:

    a. Cameras shall capture a depth of field in combination with recording frame rate to obtain at least 10 frames of a subject moving at walking speed through the target zone.

    b. The resolution of the camera shall capture at least 16 pixels of resolution on a subject's face at the furthest extent of the target area.

    c. The target area lighting level or camera sensitivity shall provide usable imagery with the following guideline:

        i. Light to dark ratio: recommended 6 to 1 as measured on horizontal plane

        ii. A minimum of 70 percent of the camera field of view should be illuminated. The entire target area shall be illuminated.

        iii. A minimum illumination level of 1.5 foot-candles, as measured on a horizontal plane 1 foot off the ground, is recommended for a black-and-white camera with a sensitivity specification of 0.007 foot- candles faceplate illumination. This assumes the camera has a good-quality, F/1.4 fixed focal lens. A color camera or a camera with a zoom lens will require a higher light level in order to get equivalent brightness and contrast.

        iv. If ambient lightning sources are not sufficient for quality images, active illumination technology shall be used (such as infrared illuminators.)

2. Cameras shall never be subject to direct sunlight or other sources of light with the intensity to obstruct the view of the target area.

Section 2: Data Networking Standard

1. Data network requirements include the physical installation as well as data security. All components of a security camera system connected to the University's Backbone data networks or any other networking that connects to a public data network shall contact the University of

Michigan Information and Technology Services (ITS) Networking and Telecommunications group[1] for connectivity requirements, standards and coordination.

2. Security camera network connectivity shall be protected by a combination of network firewalls and/or private vLANs. At no time shall a security camera system be accessible from the Internet.

3. Connections to department data networks shall be coordinated with ITS and the local network administrator. The connected data network shall be able to maintain the network performance necessary for needed bandwidth for recording the intended resolution and frame rate of the system as designed.

4. Installations shall follow the University of Michigan Architecture, Engineering and Construction (AEC) Design Guidelines. In particular, the Technical Sections for Electrical [section 16740] [2] contains applicable standards for cabling.

Section 3: Installation and Maintenance

1. The installation of all camera hardware and any other components shall be installed to allow periodic maintenance and service. Camera equipment shall be maintained in good working order with lenses kept clean and unobstructed.

2. Health monitoring shall be enabled and configured to report any error conditions or other notifications to the manager responsible. Equipment unable to be repaired in a timely manner shall be removed from service. No inoperable equipment shall remain affixed to a structure.

3. Camera systems shall be protected from brief power outages by the use of uninterruptable power supplies (UPS). The power supplies shall be maintained in accordance with the manufacture's recommendations.

4. Camera housings shall be able to be secured from tamper or damage.

5. Cable pathways shall be protected from tamper or damage.

[1] http://www.itcom.itd.umich.edu/backbone/

[2] http://www.umaec.umich.edu/desguide/tech/csi16.html

1. Although security cameras systems are not required to be accessible to the University of Michigan Division of Public Safety and Security's Police Communications Center, installations shall be based on equipment having this capability. The following hardware compatibility list indicates recommended equipment. If the equipment needed is not listed, an ONVIF[3] listed camera is acceptable. (see attached document)

[3] http://www.onvif.org/