80-18 Surveillance Systems

80-18-1 Purpose • 80-18-2 Policy • 80-18-3 Access • 80-18-4 Administration • 80-18-5 Definitions • 80-18-6 Responsibilities • 80-18-7 Exceptions • 80-18-8 Penalties • 80-18-9 Public Notice

1. **Purpose**. The purpose of this policy and subsequent procedures is to regulate surveillance system installation, monitoring, recording and reviewing on property owned, operated and/or controlled by the Eastern New Mexico University System (the System). Surveillance systems can be a valuable tool to deter criminal activity, enhance loss prevention, provide evidence for criminal investigations, assist with emergency management and facilitate first responder calls for service. The System is committed to enhancing the quality of life of our communities by integrating best practices of campus safety. A critical component of a comprehensive public safety program in a collegiate environment is the use of surveillance technology.

2. **Policy**. The policies established in furtherance of the above-mentioned purposes are as follows:

   A. Information obtained via surveillance systems will be exclusively used for policy enforcement, loss prevention, security, emergency management and law enforcement purposes. The system may use surveillance footage to investigate an alleged violation of policy or an unlawful act and to support disciplinary hearings.

   B. Information obtained by surveillance systems will only be released in accordance with the provisions of the New Mexico Inspection of Public Records Act, law enforcement discovery requirements, to comply with court orders or to facilitate the System's needs which are outlined in 80-18-2.A. of this policy, provided that any information obtained by surveillance systems that constitutes an educational record under the Federal Educational Rights and Privacy Act (FERPA) shall only be released in accordance therewith.

   C. The use of surveillance systems will be restricted to areas where there is no reasonable expectation of privacy as defined by state and federal law. Campuses that utilize surveillance systems shall be conspicuously posted with signs which would give a reasonable person notice that they may be video recorded while on campus.

   D. Departments within the System who are not outlined in 80-18-2. A. of this policy are prohibited from purchasing, installing or maintaining their own surveillance systems.

   E. Authorized vendors are prohibited from providing unauthorized access to surveillance systems and viewing software to employees or external sources**.**

   F. The monitoring, recording and reviewing of surveillance systems will be conducted in a manner consistent with existing System policies such as those related to non-discrimination, harassment and sexual harassment as well as all applicable state and federal laws.

   G. Images and any related data collected by ENMU surveillance systems are the property of the System.

   H. Third party audio recordings are prohibited within the System unless the area monitored by the third-party audio recording has conspicuous sign postings that would give a reasonable person notice that she or he is being audio recorded within a particular area.

I. Surveillance systems shall be adequately maintained and configured in such a manner that servers or other hardware designed to store images or video footage have a minimum of thirty (30) days of available storage.

J. The System will preserve surveillance content used or requested in any civil, criminal or administrative investigation in accordance with the provisions of Functional Retention and Disposition Schedules outlined in 1.21.2 of the New Mexico Administrative Code.

K. Law enforcement personnel employed by the System entrusted with the collection, handling, preservation and storage of criminal evidence shall do so in accordance with departmental policy and best practices, as well as state and federal law.

L. The use of fake or dummy cameras on property owned, operated or controlled by the System is prohibited.

M. Unauthorized interception, duplication, transmission or use of surveillance content for purposes other than their intended purpose by unauthorized personnel is strictly prohibited.

3. Access. All access shall be administered in accordance with the following:

A. Authorized personnel of ENMU department of Public Safety, police department, security department or their departmental equivalent at any branch community college campus will be the only personnel authorized to have access to surveillance software.

B. Authorized Information Technology Services (ITS) personnel responsible for the maintenance or adjustments of surveillance systems may access aspects of a surveillance systems as part of the official performance of these specific duties.

C. Authorized vendors responsible for installation, maintenance or adjustment of surveillance systems may access aspects of surveillance systems as part of the official performance of these specific duties.

D. To the extent permitted by law, students, faculty or staff involved in an investigation of an alleged violation of System policy may have access to a copy of related footage as part of their investigation or adjudication of the matter, if applicable.

E. Access to surveillance content will be strictly controlled. Access will only be granted under limited circumstances and at the discretion of the Public Safety Administrator on each campus.

F. Surveillance systems will not be used as a mechanism to regularly evaluate employee performance absent a formal investigation. Any and all requests of footage related an employee for an employment issue will be made from the applicable director of Human Resources and forwarded to the Public Safety Administrator for processing.

G. Surveillance information or data that constitutes an educational record shall be handled consistent with FERPA.

4. Administration. This policy and subsequent procedures shall be administered by the chief of Police for the ENMU Department of Public Safety at the ENMU-Portales campus with oversight by the System chief financial officer (CFO).

Procedures

5. Definitions.

A. "Surveillance System" is any digital camera or closed-circuit television (CCTV) system whether fixed or mobile capable of capturing images and video that can be compressed, stored or sent over communication networks. This includes any and all related components, equipment, hardware or software.

B. "Surveillance Software" is any programs and other operating information used by a computer or portable device to view images, video and/or audio collected by a surveillance system.

C. "Surveillance Hardware" is any physical, tangible parts, equipment or components of the surveillance system.

D. "Public Safety Administrator" for the purpose of this policy is the chief of Police, chief of Security, director of Public Safety, director of Security or their positional equivalent at each campus within the System. It will be the responsibility of the branch community college president to appoint an individual for this role in the event that a branch community college campus does not have a positional equivalent.

6. Responsibilities. The following roles and responsibilities shall be established:

A. The Public Safety Administrator is responsible for ensuring compliance with this policy. This person is also responsible for responding to requests to access surveillance footage for investigative purposes and establishing restricted user permissions in surveillance software.

B. The Public Safety Administrator is also responsible for coordinating maintenance agreements with internal departments and/or external vendors to make sure surveillance, alarm and/or access control systems are functional and performing at an optimal level based upon available financial resources.

C. The CFO or any branch community college president may approve placement of surveillance systems in specific areas to address safety and security concerns based upon recommendations of the Emergency Planning Committee or Public Safety Administrator.

7. Exemptions. Academic departments or athletics who may use CCTV monitoring and recording as a way to evaluate performance, academic integrity or practical application exercises consistent with state and federal laws are exempted from this policy only to the extent this policy prohibits the purchase, installation, maintenance, or use of CCTV monitoring and recording, provided that the purchase, installation, maintenance, or use of such technology by a particular academic department or athletics shall be limited to these specific purposes. Such departments include, but are not limited to:

A. Athletics
B. Speech and Hearing Clinic
C. Health Sciences Center

8. Penalties. The mission of the System is one founded upon public trust. Protecting confidentiality to the extent permitted by law and System policy is also very important. Individuals who violate this policy may face System disciplinary action up to and including expulsion or termination. Individuals who violate this policy may also face civil and criminal penalties.

9. Public Notice. The ENMU System may use surveillance systems to enhance the safety and security of persons and property. This policy does not imply or guarantee the continual monitoring of surveillance systems in real time or on every public area owned, operated or controlled by the System.

Approved by the Board of Regents May, 10, 2019