Closed Circuit Television Monitoring and Recording Policy

Purpose

The purpose of this directive is to establish guidelines for the Idaho State University Public Safety Department (ISUPS) relative to the use of closed circuit television (CCTV) cameras.

Policy

It shall be the policy of ISUPS to utilize CCTV cameras to monitor and record public areas to ensure the safety and security of the University community. Further, ISUPS shall abide by the Idaho State University Policy for Closed Circuit Television Monitoring and Recording of Public Areas for Safety and Security Purposes.”

Scope

This directive shall affect all sworn and non-sworn employees who use, or supervise the use of the ISUPS CCTV system.

Use of CCTV Equipment

1. The use of CCTV equipment shall be limited to legitimate safety and security purposes, including but not limited to:
   a. Property and Building Protection: building perimeter, entrances and exits, lobbies and corridors, receiving docks, special storage areas, laboratories, cashier locations, ATM/CVC machines, emergency telephones.
   b. Alarm Verification: Intrusion alarms, exit door controls, hold-up alarms.
   c. Video Patrol of Public Areas: Transit stops, parking lots, public street and intersections, shopping areas.
   d. Criminal Investigation: Crimes against persons and property.
   e. Monitoring of Access Control Systems: Monitor and record restricted access transactions at entrances to buildings and other areas.
   f. Monitoring of Pedestrian and Vehicle Traffic Activity

2. The use of CCTV SHALL NOT be utilized for:
   a. Profiling: The practice of targeting individuals based on characteristics of race, gender, ethnicity, sexual orientation, disability or other classifications.

Revised 12/13/2010
b. Targeting of Individuals

c. Peering into Buildings

Public Safety Responsibilities

1. All Public Safety employees shall be guided by the Public Safety Standard operating Procedures relative to the operation of CCTV equipment.

2. The Public Safety Supervisor shall be notified immediately whenever any suspicious, criminal or life-threatening activity is observed, and appropriate police personnel shall be dispatched. In the absence of a Public Safety Supervisor, a patrol supervisor shall be notified by police radio.

3. All observations, notifications, and actions taken shall be documented, in detail, in the Computer Aided Dispatch (CAD) system.

4. Public Safety is the department authorized to oversee and coordinate the use of CCTV monitoring for safety and security purposes at the University. All University areas using CCTV monitoring are responsible for implementing this policy in their respective operations. Public Safety has primary responsibility for disseminating the policy and assisting other unity in implementing the policy and procedures.

5. The Director of Public Safety has the responsibility to authorize all CCTV monitoring for safety and security purposes at the University. All new installations will follow Public Safety operating principles. All existing CCTV monitoring systems will be evaluated for compliance with this policy.

6. Public Safety will monitor new developments in the relevant law and in security industry practices to ensure that CCTV monitoring at the University is consistent with the highest standards and protections.

7. A CCTV monitoring committee, known as the ISU Safety Committee, will be responsible to assure that Public Safety adheres to established policy and procedure in the use of CCTV.

8. The CCTV monitoring committee members will serve as established by the rules of the Safety Committee. An individual may appeal an adverse decision by the CCTV monitoring committee through existing University appeal mechanisms.

9. The CCTV monitoring committee will review camera locations to insure the perimeter of view of fixed location cameras conforms to this policy. The proposed location of permanent CCTV cameras will be provided to the CCTV monitoring committee for review and published in the EXTRA before installation. A list of all University owned or controlled camera locations will be published semi-annually in the EXTRA and made available by Public Safety to anyone requesting the list. The location of temporary cameras to be used for special events will be reviewed by the CCTV monitoring committee for approval and published in the EXTRA before the event if possible.

Revised 12/13/2010
(Note: “temporary cameras” does not include mobile video equipment of hidden surveillance cameras used for criminal investigations.)

Included with the list of CCTV camera locations will be a general description of the technology employed and the capabilities of the cameras.

Students and staff entering certain sensitive locations on campus may have an increased concern for privacy and confidentiality. In order to prevent a possible chilling effect on the use of service at these locations, concerned persons may petition the CCTV monitoring committee to forgo the installation of a proposed camera or for the removal of an existing camera. The CCTV monitoring committee will determine the appropriateness of an installation weighing the concerns of the person(s) making the requests and the safety and security for the entire community.

In recognizing students may also have an enhanced expectation of privacy in the hallways and lounges of residence facilities, CCTV monitoring for safety and security purposes will not be used in residential hallways and lounges unless the Director of Public Safety determines the specific safety/security risk exists.

The CCTV monitoring committee will review complaints regarding camera locations and determine whether the CCTV monitoring policy is being followed. The committee should weigh whether the potential increment in community security outweighs any likely infringement of individual privacy.

10. The CCTV monitoring committee, with the Director of Public Safety, will review all requests received by the Public Safety Department to release recordings obtained through CCTV monitoring. No releases of CCTV recordings will occur without authorization by the Director of Public Safety and the CCTV monitoring committee. Excluded from review by the CCTV monitoring committee are releases of tapes directly related to a criminal investigation, arrest or subpoena. The CCTV monitoring committee may also approve release of CCTV tapes only for legitimate purposes, such as to protect the University and its members from lawsuits or harm. A unanimous vote of the committee is necessary to approve the release of tapes. Any release of tapes will be recorded on a written log.

11. Any member of the CCTV monitoring committee may audit Public Safety’s CCTV monitoring operations, including videotape storage, at any time without prior notice.

12. The Chair of the Safety Committee will report to the Safety Committee at least four (4) times per year describing all requests for camera locations and release of tapes and disposition of those requests.

13. The CCTV monitoring committee will review this policy annually and recommend revisions if needed.

**Tape Management Policy and Procedures**

**Tape Security**

1. Access to video tapes and video recording equipment is limited to:

   a. The University Senior Staff

*Revised 12/13/2010*
b. University CCTV Safety Committee Members

1) A list of current committee members will be posted in the Public Safety Operations Center and will be updated annually.

2) Panel members will be given full cooperation and access to all CCTV monitoring areas and tape storage areas.

3) ISUPS command personnel will be notified immediately whenever a committee member requests to inspect a CCTV monitoring or tape storage area.

4) All committee inspection will be noted on the dispatch radio log.

5) Anyone requesting to view video tapes shall be instructed to contact the ISU Public Safety Director between 9:00 am and 5:00 pm, Monday through Friday.

c. Under no circumstances will alarm monitoring operators or supervisors be permitted access to video tapes or video recording equipment, without the Director’s approval.

d. A Video Tape Control Log shall be maintained by the Public Safety Department and shall be reviewed daily by the Security System Administrator. The Video Tape Control Log will be kept in the Security System Administrator’s office and will not be removed for any reason.

e. Tape Audits and Inventory shall be performed by the Director of Public Safety. Random audits shall be conducted by the CCTV monitoring committee.

Image Storage

1. Each tape will be labeled and identified by Loronix prior to arrival at Public Safety. Public Safety personnel will not alter these tapes.

2. Tapes will remain in the Loronix tape library and only be removed by the Director of Public Safety.

Video clips will not be archived unless approved by the Director of Public Safety.

Changing, Erasing, and Reusing of Tapes

1. Only authorized Public Safety managers may change storage tapes or operate video recording equipment.

2. An entry will be made on the ISUPS Sending and Receiving Sheet reflecting that the appropriate tape(s) were changed, that all tapes have been accounted for, and that the tape storage area is secure.

3. **This task shall NOT be delegated**

*Revised 12/13/2010*
**Review and Dissemination of Information**

1. All personnel will adhere to the Idaho State University Policy for Closed Circuit Television Monitoring and Recording of Public Areas for Safety and Security Purposes.

2. Only authorized management, police and detective personnel are permitted to review or remove tapes.

3. Authorized personnel wishing to view or remove a video tape for any reason must enter all required information in the Video Tape Control Log. All entries must be complete and legible.

4. Video tapes must be returned to storage and secured by the end of each business day, unless they have been subpoenaed or permission is obtained from the Director of Public Safety.

5. Duplication of tapes or printing of images from video tapes is prohibited unless approved by the Director of Public Safety.

6. Conversion of taped images from digital to analog formats is prohibited unless approved by the Director of Public Safety.

**Performance Evaluation**

1. Public Safety dispatch supervisory personnel will periodically and without prior notice have CCTV operators demonstrate their knowledge and understanding of relevant policies, procedures, and technical skills.

2. The Public Safety Department shall be notified of any performance or operational issues or deficiencies.

3. The Public Safety Department shall have primary responsibilities for initiating remedial action.

**Impairment**

1. Under no circumstances shall anyone, except professional factory trained service technicians attempt to service, repair, or tamper with any of the CCTV or video recording equipment.

2. The Public Safety Department shall have primary responsibilities for initiating remedial action.

**System/Equipment Failure**

1. Upon the failure of a CCTV component, CCTV monitoring personnel shall immediately notify the Public Safety Supervisor.

2. If the failure is contained to an individual component, the Public Safety Supervisor shall notify the CCTV manager during their regular business hours. If the failure occurs after hours, the Public Safety Supervisor shall document the equipment failure on the log and request that the Public Safety Department is notified the following business day.

3. If the failure is system wide, the Public Safety Supervisor shall document the failure on the log and immediately notify Public Safety personnel utilizing the Emergency Contact Callout List, located in the binder at the alarm monitoring console inside the dispatch operations center.

*Revised 12/13/2010*
Compliance

Violations of this directive, or portions thereof, may result in disciplinary action.

Officers Assigned to Other Agencies

Officers of this department assigned to or assisting other law enforcement agencies will be guided by this directive.

Application

This directive constitutes departmental policy, and is not intended to enlarge the employer's or employee’s civil or criminal liability in any way. It shall not be construed as the creation of a higher legal standard of safety or care in evidentiary sense with respect to third party claims insofar as the employer's or employee’s legal duty as imposed by law. Violations of policy will only form the basis for departmental administrative sanctions. Violations of law will form the basis for civil and criminal sanctions in a recognized judicial setting.

General Principles

A. Public Safety is committed to enhancing the quality of life of the campus community by integrating the best practices of public policing with state-of-the-art technology. A critical component of a comprehensive security plan using state-of-the-art technology is closed circuit television (CCTV).

B. The purpose of CCTV monitoring of public areas by security personnel is to deter crime and to assist Public Safety in protecting the safety and property of the University community. Any diversion of security technologies and personnel for other purposes (i.e., CCTV monitoring of political or religious activities, or employee and/or student evaluations) would undermine the acceptability of these resources for critical safety goals and is therefore prohibited by this policy.

C. Video monitoring for security purposes will be conducted in a professional, ethical and legal manner. Personnel involved in video monitoring will be appropriately trained and continuously supervised in the responsible use of technology. Violations of procedures for video monitoring referenced in this policy will result in disciplinary action consistent with the rules and regulations governing employees of the University.

D. Information obtained through video monitoring will be used exclusively for security and law enforcement purposes. Information obtained through video monitoring will only be released when authorized by the Director of Public Safety according to the procedures established in this policy.

E. Video monitoring of public areas for security purposes will be conducted in a manner consistent with all existing University policies, including the Non Discrimination Policy, the Sexual Harassment Policy, Open Expression Guidelines and other relevant policies. The code of Practice for video monitoring prohibits monitoring based on the characteristics and classifications contained in the Non-Discrimination Policy (e.g., race, gender, sexual orientation, national origin, disability, etc.)

Revised 12/13/2010
F. Video monitoring of public areas for security purposes at the University is limited to uses that do not violate the reasonable expectation of privacy as defined by law.

G. To maintain an informed University community, ISU Public Safety will periodically disseminate written materials describing the purpose and location of CCTV monitoring and the guidelines for its use. The location of outdoor CCTV cameras monitored by Public Safety will be published in the Student newspaper, EXTRA.

H. Information obtained in violation of this policy may not be used in a disciplinary proceeding against a member of the University faculty, staff or student body.

Procedures

A. All operators and supervisors involved in video monitoring of public areas will perform their duties in accordance with this policy developed by Public Safety.

B. Public Safety management will assure that responsible and proper camera monitoring practices by control operators is continuous.

C. Public Safety will post signs at appropriate locations. Sign will state, “This public area is monitored by security cameras for personal safety and property protection.”

D. Public Safety will limit camera positions and views of residential housing. Any view given to the housing will be no greater than what is available with unaided vision. Furthermore, the view of residential housing facility must not violate the standard of “reasonable expectation of privacy.”

E. Public Safety operations and other monitoring centers will be configured to prevent camera operators from tampering with or duplicating recorded information.

F. Recorded videotapes will be stored for a period not to exceed 30 days and will then be erased, unless retained as part of a criminal investigation or court proceedings (criminal or civil), or other bona fide use as approved by the Director of Public Safety and the CCTV monitoring committee.

G. Video tapes will be stored in a secure location with access by authorized personnel only.

H. Camera control operators will conduct video observation of areas only in plain view of others situated in the public area viewable to the public.

I. Camera control operators will be trained in the technical, legal, and ethical parameters of appropriate camera use.

J. Camera control operators will receive a copy of this policy and provide written acknowledgment that they have read and understood its contents.

K. Camera control operators will receive training in cultural awareness.

Revised 12/13/2010
L. Camera control operators will not monitor individuals based on characteristics of race, gender, ethnicity, sexual orientation, disability, or other classifications protected by the University's Non-Discrimination Policy. Camera control operators will monitor based on suspicious behavior, not individual characteristics.

M. Camera control operators will not spot and continuously view people becoming intimate in public areas.

N. Camera control operators will not view private rooms or areas through windows.

O. Mobile video, portable hidden cameras and recording equipment may be used in investigations. Mobile video equipment will only be used in non-criminal investigations in specific instances as authorized by the Director of Public Safety, the University Attorney or the President of the University.

Examples of Video Monitoring and Recording of Public Areas

Legitimate safety and security purposes include, but are not limited to, the following:

Protection of building and property:
Building perimeters, entrances and exits, lobbies and corridors, receiving docks, special storage areas, laboratories, cashier locations, etc.

Monitoring of access control systems:
Monitor and record restricted access transactions at entrances to buildings and other areas.

Verifications of security alarms:
Intrusion alarms, exit door controls, hold-up alarms, etc.

Video patrol of public areas:
Transit stops, parking lots, public (enclosed and unenclosed) streets, shopping areas, vehicle intersections, etc.

Criminal investigations:
Robbery, burglary, and theft surveillance.

Protection of pedestrians:
Monitor pedestrian and vehicle traffic and vehicles in traffic areas at intersections.

Revised 12/13/2010