CCS Administrative Procedure
6.00.01-F Security Cameras – Approved Use & Design Standards

Implementing Board Policy 6.00.01
Contact: Chief Information Officer, 434-5427

1.0 Purpose

Community Colleges of Spokane, recognizing the importance of providing and maintaining quality facilities and infrastructure that enhances the delivery of education and support services to our community, will provide for and operate its facilities in an effective and efficient manner. This includes establishing and implementing standards that ensure consistency, operational efficiency, maintainability, and maximum utilization of those working and learning environments. These standards represent best use of state resources and are aligned with Community Colleges of Spokane's mission, values and goals.

2.0 Limitations and Requirements

Among the concerns in implementing this procedure is utilizing systems that advance safety of faculty, staff, students and visitors, security of property, crime deterrence, loss prevention, and general risk management. Security cameras can be such a system if appropriately administered consistent with this procedure.

2.1 The Chief Information Officer (CIO) is responsible for administering this procedure in consultation with the District Director of Facilities and Director of Security.

2.2 All district owned and managed facilities are subject to this procedure without exception.

2.3 This procedure does not diminish or eliminate the standard of care owed by a consultant to CCS or relieve, in any manner whatsoever, a consultant from any professional responsibility, duty, or due diligence required toward the work.

2.4 Access to security camera systems, including access to data storage, will be limited to those with a work-related need as determined by the CIO, in consultation with the Director of Security and/or Chief Administration Officer.

3.0 Definitions

The following definitions are specific to the terms of this procedure and do not modify or revise similar terms as used in related procedures or collective bargaining agreements.

3.1 Chief Information Officer: the administrator with assigned authority over the Office of Information Technologies (IT).

3.2 District Director of Facilities: the administrator responsible for the Facilities Department.

3.3 Facility: a district owned or controlled property, building or component of that property/building.

3.4 Security Camera: Closed-circuit television (CCTV) using video cameras to transmit a silent signal to a specific place and/or a limited set of monitors. Differs from broadcast television in that the signal provides no audible recording and is not openly transmitted (though it may employ point to point (P2P), point to multipoint, or mesh wireless links). This definition covers video cameras used to advance security of property, safety of faculty, staff, students and visitors, crime deterrent, loss prevention, and general risk management.

3.5 Design Standards: developed and adopted by the CIO, these standards serve as directives and technical specification for design professionals, construction managers, planners, design committees and others participating in capital construction and/or

renovation planning. Design standards will be reviewed regularly for feasibility, currency and effectiveness. Current standards are included as Appendix A and are subject to change as technology or code necessitates, without prior notice or posting declarations.

3.6 Construction Specifications: provided for use by consultants in designing construction projects. Construction specifications are not subject to this procedure.

3.7 Open and public area: an area open to, used by and/or accessible to more than one person and for which there is no reasonable expectation of privacy under the law.

4.0 Process for Requesting Installation of a Security Camera

Requests for installation of a security camera system must contain the recommendation of the unit's appointing authority. Such requests will then be considered as follows:

4.1 Request for placement and installation of a security camera system shall be made using the Building Improvement Request (BIR) process. Requests will be considered by the District Director of Facilities, in consultation with appropriate facilities, IT and security staff. IT staff, consistent with current design standards and in consultation with security, will specify the manufacturer, model and placement of the camera.

4.2 Approval will only be granted where the following pre-conditions are met:

4.2.1 Proposed equipment will record only silent video images. Equipment will not possess the capacity or otherwise be installed/used in a manner that records sound.

4.2.2 Surveillance area will meet the definition of an open, public location with no reasonable expectation of privacy at any time.

4.2.3 Placement of the proposed surveillance equipment must further CCS' need for the supervision, control, secure, and safe operation of its facilities.

4.3 Considerations/analysis shall include, but not be limited to:

4.3.1 Would installation create right to privacy concerns or potentially violate collective bargaining agreements? Concerns shall be forwarded to the Human Resources Office (HRO) for review/direction.

4.3.2 Does the request comply with established design standards? If not, why is there a variance and, if approved, is the variance serviceable by in-house maintenance personnel or must it be outsourced to service vendors?

4.3.3 Is the requested system compatible with existing infrastructure (i.e. mechanical, electrical, plumbing, telecommunications, structural, architectural, life safety, building automated controls, security, finish and furniture systems)?

4.4 Following the above analysis, the district director of facilities, consistent with the BIR process, will respond to the requesting party and inform of decisions.

4.5 If the request is not resolved to the satisfaction of the requestor, it can be appealed to the chancellor. The chancellor's decision, respectively, will be implemented without further review.

5.0 Security Camera Design Standards

These design standards serve to clarify direction and streamline project execution. They represent the District's standardized decision and should be applied, when possible, without compromising the overall design. Each design standard includes direction on whether equivalent substitutes are acceptable.

5.1 CCS will install only security cameras, DVRs and related system equipment that meet the design standards authorized under section 3.5. Wiring standards will be as determined by the director of facilities, consistent with the design standards established by the chief information officer.

5.2 This standard does not address every conceivable condition or occupant decision point. Rather, it attempts to provide guidance based upon industry standard or where experience has indicated a standard is appropriate and prudent.

5.3 In the absence of a written design standard, the Director of Capital Construction will present options to design committees during the schematic design or design development phases so that an informed decision can be made.

5.4 In cases where the consultant, design committee or college administrator determines that the written design standard is not appropriate for the project, and wishes to deviate from the standards, they must seek approval from the Chief Information Officer prior to deviating from the written standard.

5.5 Requests for clarification of and possible alternatives to design standards shall be forwarded to Facilities capital construction staff for consideration and response.

6.0 Legal Considerations and Waivers

6.1 RCW 9.73.030 addresses the ability of individuals and agencies of the State of Washington to conduct surveillance. The code provides that it's unlawful to intercept or record any private conversation by any device electronic or otherwise designed to record or transmit such conversation regardless of how the device is powered without first obtaining the consent of all the parties engaged in the conversation.

6.1.1 CCS complies with this code by refusing to install any security camera that has audio recording capabilities.

6.2 Electronic Communications Privacy Act of 1986 prohibits the interception of any wire, oral or electronic communication and only permits the recording of communications where the parties have given prior consent.

6.2.1 CCS complies with this act by refusing to install any security camera that has audio recording capabilities.

6.3 U.S. Constitution, Amendment IV and Washington State Constitution both provide in pertinent part that no person shall be disturbed in his private affairs, or his home invaded, without authority of the law. The decision to install video surveillance cameras must take into consideration this “right to privacy.”

6.3.1 CCS complies with these constitutional amendments/sections by refusing to install a video camera system in any area where a person has a reasonable expectation of privacy at the time of taping. This is further advanced by installing systems so that only open and public areas are under surveillance. In such areas there is no reasonable expectation of privacy. The goal is to balance the individual’s right to privacy with CCS’ need to supervise, control and efficiently operate our facilities.

7.0 Storage and Retention of Images and Data

7.1 Recorded images will be stored and retained consistent with the capabilities of the system and CCS’ technology capacities. The goal will be to retain images for no less than 30 calendar days and retention may be longer in higher risk areas.

7.2 Images will not be monitored on an ongoing basis but rather will be accessed where such images may provide information critical to resolving an issue or concern regarding the

safety of faculty, staff, students and visitors, security of state property, crime activity, loss confirmation, and general risk management.

7.3 Any image that is determined to have investigative value and is downloaded for retention beyond 30 calendar days will be sealed, logged and stored in such a manner that it protects its custody and evidential integrity. Security and/or HRO staff will take possession and maintain such evidence to ensure chain-of-custody and confidentiality.

7.4 Viewing of security camera feeds, as well as access to security system data storage will be limited to those determined to have a work-related need as determined by the CIO, in consultation with the director of security.

7.5 All other requests for data, as outlined in 7.4, will be subject to CCS' public records request process.

8.0 Signage

Signs indicating the presence of video surveillance will be generally posted announcing "This area may be monitored by CCTV."

9.0 Exemptions and Exceptions

Exceptions to this procedure may exist where video surveillance is part of an ongoing employment or criminal investigation. Exceptions will be granted by the Chief Administration Officer.

10.0 Related Information

Appendix A – Design Standards

Originated: July 2013, Revised February 2016
Cabinet approval: August 26, 2013, February 29, 2016

Appendix A

1.0 General Technical Specifications

1.1 Security camera systems may take the form of standalone Network Video Recorders (NVR) and IP cameras connected to the college enterprise video system. No private company/contractor hosted system shall be deployed.

1.2 NVR systems shall be secured by credentials. Default passwords shall be changed and recorded with IT. 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.

1.3 Access levels shall be used to protect access to system configuration, specific camera groups or partitions, based on the role of the user.

1.4 Access credentials shall be person specific, using the CCS issued unique name whenever possible.

1.5 Access log capability shall be present and enabled.

1.6 Access logs shall be maintained for one year.

1.7 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.

2.0 Image and Recording Standards

2.1 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 these guidelines:

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

2.1.2 The resolution of the camera shall capture at least sixteen pixels of resolution on a subject's face at the furthest extend of the target area.

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

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

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

2.1.3.3 A minimum illumination level of 1.5 foot-candles, as measured on a horizontal plane 1 foot off the ground, is recommended for black-and-white cameras 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.

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

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

3.0 Data Networking Standard

3.1 All system wiring shall be plenum rated unless noted and approved before installation.

3.2 CAT6A cabling and patch cables shall be used for all security cameras and associated equipment.

3.3 All wiring shall be installed in accordance with the National Electric Code (NEC), the National Fire Protection Agency (NFPA), and EIA/TIA Telecommunications wiring standards.

3.4 Cables penetrating floors and firewalls must be routed through a metallic sleeve and properly fire stopped to meet national and local fire codes. All walls and floors shall maintain their existing fire rating.

4.0 Documentation

4.1 Upon completion of installation, one-line drawings of each floor plan indicating exact device locations and camera name(s) will be created and provided to the security office for reference.