Division 28. Electronic Safety and Security

28 10 00. Electronic Access Control and Intrusion Detection

28 11 00. Electronic Access Control

28 11 05. Electronic Access Control for New Construction

1. General Requirements:

1.1. At a minimum for new construction projects, access control shall be provided on the following doors: exterior points of entry (electronic locks for the purpose of remote lock/unlock on all – prox reader doors will be limited to the amount needed for sensible traffic flow dependent upon building size and occupancy), access to animal care areas, personnel record storage, sensitive and critical mechanical spaces, telecom rooms, server rooms and those rooms deemed necessary by the building occupants.

1.1.1. Install access control on building façade and walls whenever possible instead of installing a separate "bollard" which are susceptible to damage.

1.2. It shall be noted that when the ability to alarm an area (door position switch) is absent, and physical security features are lacking (such as latch guards and pinned door hinges), an access control device does not provide a higher level of security than a standard key lock; however, it does provide key control, and access logging, which standard keying does not.

1.3. Andover "Continuum" product, is the campus standard, implemented in large part by the UW Electric Shop. All decisions for access control systems within new construction shall be coordinated jointly with the building occupants, UWPD, UW Electric Shop, and UW Facilities Planning & Management.

1.4. The design team shall be responsible for engineering the system in cooperation with those listed above.

1.5. A basis-of-design specification is available. The Nursing building is currently the campus standard.

1.6. The Electrical Contractor shall provide and install all pathways, card readers, and pin code devices, and other devices such as electric locks and local alarm horns. The Electrical Contractor shall also be responsible for installing the Andover panels, which are provided by the Owner. These items shall be installed according to UW Physical Plant specifications.

1.7. Rack-based head end equipment usually resides in the MDF. Any rooms housing head end equipment shall have electronic access control devices. Net controller panels (by Andover) shall be located on each floor, in reasonably close proximity to the doors which they serve, preferably in TRs or electrical rooms, consistent floor to floor. The design team shall be responsible for educating themselves on the system in order to determine panel sizes and required and capacity issues.

1.8. The UW Electric Shop, not the Electrical Contractor, shall install tamper switches in all access control panels.

1.9. UWPD shall issue HID proximity cards for contractors. All UW-Madison Affiliates are eligible for a WISCard through the WISCard office at Union South. Contractors shall be directed to the UWPD access control card office, currently located at 1433 Monroe St. All entities shall be billed quarterly for cards, by department.

1.10. UWPD shall work with the building occupants to set up their security groups. A single representative for the new facility or a representative for each department (school) housed within the facility, shall work with UWPD to assign area rights to individual end users and shall use a "web client" to modify access for authorized users, after the initial system is set up.

1.11. Latch guards and pinned hinges shall be used on all out-swinging publicly accessible doors that lead into a secured area.

1.12. All hardware groups for doors receiving card readers and electric locks shall have door contacts and Request to Exit (REX) devices included. Both door in a pair and inactive-leaf doors shall also use door contacts. UWPD shall not allow motion detector-type REX's to be used for unlocking mag-lock doors, as they can easily be defeated. Internal REX devices are required, but when existing conditions do not permit, these locations may be equipped with motion detector-PIR type REX devices. Providing door contacts now, will allow for future reporting back to UWPD. Doors are not actively monitored at this time by UWPD unless special arrangements have been made.

1.13. The UW utilizes magnetic hold-opens but does not permit magnetic locks unless this is the only way to secure the door.

1.14. UWPD uses a number of configurations to describe attributes they require on doors with access control. Possible sample configurations are as follows:

Config 1 - Card reader with Biometric access, REX (Request to Exit), door contacts.

Config 2 - Electronic latch retraction (crash bar), card reader, REX device, door contacts. Latch bolt status monitor (optional).

Config 3 - Electronic latch retraction (crash bar), door contacts, latch bolt status monitor (optional). Internal REX device. No Card Reader

Config 4 - Card reader with keypad, door contacts , electric lock, and REX

Config 5 - Card reader (standard), door contacts, electric lock and REX

Config 6 - Electric Locks, door contacts, and REX

Config 7 - Emergency egress device (crash bar), door contacts, local alarm

1.15. The entire access control system for UW-Madison buildings is funded by the project and designed and installed via a partnership between the design team, UWPD, the UW Electric Shop, and the Electrical Contractor.

1.16. During the design development phase of the project, once the security requirements for the building are understood, cameras are located, and doors are noted as having or not having access control features, the UW Electric Shop shall receive a work order to begin their one-line diagrams and cost estimate.

1.17. The UW Electric Shop typically provides the following documents and drawings during this phase.

1.17.1. Door location drawings
1.17.2. Andover panel layout
1.17.3. Door detail drawing
1.17.4. Riser prints
1.17.5. Panel take-offs
1.17.6. Contractor termination details
1.17.7. Related Cut Sheets
1.17.8. Resistor pack layout
1.17.9. Camera locations

1.18. The UW Electric Shop shall provide commissioning services for the following equipment.

1.18.1. Andover head end equipment
1.18.2. Control cabinet
1.18.3. End of the line resistors
1.18.4. Termination of the head end equipment
1.18.5. Commissioning of the system

1.19. The UW Electric Shop typically provides the following materials funded through the project in the commissioning estimate.

1.19.1. Andover head end equipment
1.19.2. Control cabinet
1.19.3. End of the line resistors

1.20. The UW Electric Shop typically provides the following labor funded through the project in the commissioning estimate.

1.20.1. Termination of the head end equipment
1.20.2. Commissioning of the system

1.21. Field devices, i.e. card readers, door position switches, request to exit devices, cabling, raceways, and door hardware, are supplied and installed by others.

2. Assistance Alarms:

2.1. Assistance alarms are discouraged as they are the least reliable and least informative tool for summoning help. 911 by telephone is the best form of assistance communication. If the occupants of the building require, assistance alarms can be installed using an RF system whereby an emergency signal is sent to a location within the building and the UWPD simultaneously. Examples of this include panic alarms at cashiering stations or a nurse call device within health care settings. The current standard is the UL listed Ademco Vista system which is available hard-wired or wireless.

3. Code Blue:

3.1. A code blue option shall be available for elevator lobbies if it is determined that an override may be needed for emergencies by the occupants of the building. This is not related to the fire department override.

3.2. A code blue phone shall be available for use in UW parking ramps and other areas where personal safety is a concern. The push button directly connects the person to UWPD 911. The current standard is Code Blue model CB2-s. This is the campus standard for parking ramps. The campus standard for occupied non parking structures shall be the Code Blue model CB 4-s. The campus standard exterior "pedestal" style phone is Code Blue model CB-s, safety red color pedestal. The word 'Emergency' shall be stenciled on the side.

4. Security Alarms:

4.1. Security alarms can be set up for afterhours monitoring/reporting if the building occupants require. These alarms may utilize glass break, motion detection, or door contact hardware, along with Ademco alarm control panels tied in to the Andover access control system.

5. Announcements/Drills:

5.1. Overhead paging can be run through the fire alarm system if the building occupants require. Custom voice-over can be included as well as pre-recorded messages. If this is the case, an additional panel is required, and all devices shall be tamper-proof.

6. Stairs and Elevators:

6.1. There shall be a provision within each passenger elevator for an access control device.

6.2. All freight elevators shall be prepped for a future access control device unless the building occupants prefer otherwise. Elevator prep shall be determined on a project-by-project basis.

6.3. Depending on the needs of the building occupants, stairs can be provided with access control at each floor. All egress doors shall be provided minimally with a door contact (DPS) to alert if a door is opened. If the door is used for normal egress along with emergency egress, the door must also have a REX device. If electronic locking is included in egress doors, these devices will "fail safe and remain latched" in an emergency. For emergency egress, the REX device must be internal to the exit hardware.

Note: As this is a "living" document, the configuration list may change dependent upon any new Federal regulations and changes in available technology.

28 20 00. Electronic Surveillance

28 23 00. Video Surveillance

28 23 23. Video Surveillance Systems Infrastructure

1. All use of security cameras and video equipment shall comply with the UW Security Surveillance Camera and Video Administrative Policy.
See *Security Surveillance Camera and Video Administrative Policy* at the end of the division.

2. Cameras:

2.1. Cameras, where desired by UWPD, shall be the "fixed" type with wide angle or as required for specific intended purpose. They shall be ceiling mounted and housed in a lexan bubble. They shall record by movement to a digital storage device (DVR) or network storage device (NVR) which is compatible with the Andover system. The DVR/NVR shall be located in a secure room which shall be accessible by UWPD and the UW Electric shop only for their review of the digital output. A connection shall be provided for laptop use by those reviewing.

2.2. Typical camera locations include exterior entrances, loading docks, elevator lobbies, where there are cashiering functions, alarmed locations, and other locations as determined by the building occupants.

2.3. In most cases, fixed cameras will be I.P. cameras, with minimum 1.3 megapixel resolution. Hardware shall be determined by the UW Electric Shop. In some locations, distance considerations may preclude the use of I.P. cameras. Where I.P. cameras are not feasible, UW Electric Shop will specify an alternative camera and lens based on site specific needs with input from UWPD.

2.4. Cameras record but are not actively monitored by UWPD unless special arrangements have been made.

2.5. The Wisconsin Office of the Attorney General provides digital storage recommendations based on Wisconsin State Statutes. These statutes outline the time frame to file a notice of claim against the state. The Attorney General suggests storing video for a minimum of 120 days. UWPD and UW Electric Shop shall determine storage needs on a project–by–project basis.

At a minimum for new construction projects, access control shall be provided on the 28 30 00. Electronic Detection and Alarm

28 31 00. Fire Detection and Alarm

1. Most campus facilities are considered common use areas and as such, require both audible and visual fire alarms. Visual fire alarms shall be synchronized so each device flashes at the same time and the cycle of the flashes shall be no less than 2 seconds.

2. Shops and docks shall have heat detectors used in place of smoke detectors, if allowed by the code.

3. Care shall be taken to follow building codes with respect to the design of exterior overhangs and soffits. When these are constructed of combustible materials, smoke detection shall be incorporated.

4. Most spaces separated by a door from audible alarms require their own audible alarms to meet minimum dB.

Security Surveillance Camera and Video Administrative Policy

UW-Madison Administrative Policy

Security Surveillance Camera and Video Policy

Effective Date:	Oct. 1, 2014
Last Updated:	Sept.16, 2014
Last Reviewed:	Sept. 16, 2014
Next Review:	Oct. 1, 2015

Functional Owner	Lieutenant of Infrastructure Security, UW-Madison Police Department
Executive Sponsor	AVC Chief of Police, Susan Riseling
Policy Contact	AVC Chief of Police, Susan Riseling, riseling@wisc.edu

Policy Summary

The policy codifies the use of cameras and video equipment in the protection of lives, research, and property of the University of Wisconsin-Madison campus community. Video surveillance (CCTV and Web Cam) is used to enhance security, safety and quality of life of the community by integrating best practices with state-of-the-art technology. The policy outlines when and how fixed security cameras are to be installed, how images and data are to be stored and recorded, and the conditions under which stored images, video or data are to be used and released. The existence of this policy does not imply or guarantee that cameras will be monitored in real time 24 hours a day, seven days a week.

Who This Policy Applies To

The policy is applicable to current and future UW-Madison and UW System sites and facilities which fall under the operational jurisdiction of ***any or all*** of the following entities of the UW-Madison: Police Department (UWPD), Division of Information Technology (DoIT), Facilities Planning and Management (FP&M) Physical Plant Electric Shop.

The policy applies to all personnel, schools, colleges, departments, offices and other divisions of the University of Wisconsin-Madison that utilize video surveillance except those exempted below.

The following are **exempt** from this policy:

- Video recording equipment used by the UWPD for evidentiary or investigative purposes
- Cameras used for academic and research purposes, including libraries
- Video equipment used for the recording of public events or for broadcast, educational or operational purposes. Examples include videotaping of athletic events for post-game review; videotaping of concerts, plays and lectures; videotaped interviews of persons; Automated Teller Machines.
- Transportation Services parking gate cameras used for operational purposes (to the extent that FP&M Transportation Services personnel may view the camera images without permission, but the video will be stored in a secure location as specified below).

Rationale

The policy is in place to:

- Ensure people viewing video surveillance are authorized to do so
- Ensure individuals requesting video surveillance and/or recording are authorized to do so
- Ensure a process of accountability for the use of video surveillance and/or recording

- Ensure that standard equipment is being installed campus-wide
- Ensure compliance with Federal, State and/or University of Wisconsin guidelines

Policy Detail

SCOPE: Monitoring of public areas for security purposes will be conducted in a manner consistent with all existing university policies, including Non-Discrimination Policy, Sexual Harassment Policy and CLERY. Monitoring of public areas for security purposes is limited to uses that do not violate the reasonable expectation of privacy as defined by law. Examples include but are not limited to individual dormitory rooms, restrooms and locker rooms.

When applicable, staff involved in video monitoring will be appropriately trained and supervised by a member of the UWPD in the responsible use of this technology. Video information obtained through monitoring will be used exclusively for safety, security, risk management, training, and law enforcement purposes. Recorded data will be stored in a secure location with access limited to authorized staff.

I. RESPONSIBILITIES

A. The UWPD is authorized to oversee and coordinate the use of video surveillance.
B. The Associate Vice Chancellor/Chief of Police or designee must authorize all video surveillance.
C. The Associate Vice Chancellor/Chief of Police or designee will review all requests to release video records. Any request for release of records will be made in writing.
D. The UWPD Lieutenant of Infrastructure Security (IS) is appointed the administrator of the campus surveillance camera and video system.
E. The Associate Vice Chancellor/Chief of Police, Associate Vice Chancellor for FP&M and the Director of DoIT will serve on the video surveillance oversight board and will review this policy annually to recommend revisions, if needed.
F. DoIT will manage the servers associated with cameras and video surveillance.
G. FP&M Physical Plant Electric Shop or their designee will be responsible for, and have the authority over, the execution of construction activities of premise wiring in all UW-Madison buildings to ensure that all installations are both code compliant and meet University standards. FP&M Physical Plant Electric Shop will coordinate all installations with UWPD and DoIT.
H. Requests for repair, maintenance and replacement will be routed through the UWPD to the FP&M Physical Plant Electric Shop.
I. Purchasing of cameras will be handled by UWPD in consultation with DoIT and FP&M Physical Plant Electric Shop regarding specifications such as camera types and megapixels.
J. UWPD IS Unit, DoIT and FP&M Physical Plant Electric Shop will review campus standards pertaining to cameras annually and make necessary adjustments.
K. Deans, Directors or designees of each School or College are responsible for the full implementation of this policy within their respective areas.

II. SECURITY SURVEILLANCE CAMERA ACCESS AND RECORDED DATA USE AND OPERATION

A. UWPD will have access to all video surveillance.
B. UWPD, DoIT and FP&M will monitor developments in the law, technology and security industry practices to ensure that camera surveillance is consistent with best practices and compliant with federal and state laws.
C. UWPD will review any complaints regarding the utilization of surveillance camera systems and determine whether this policy is being followed and report results to the oversight board.
D. UWPD staff involved in video monitoring will be appropriately trained in responsible use of the technology.
E. UWPD's IS Unit, in conjunction with DoIT, will provide periodic administrative updates and guidance to video surveillance camera systems operators including Web-Client users.

F. Video surveillance information obtained through monitoring will be used exclusively for safety, security, risk management, training and law enforcement purposes, except where noted as "exempt" above.
G. Monitoring of individuals solely based on characteristics of race, gender, sexual orientation, disability or other protected classification is explicitly prohibited.
H. Authorized Web Client users or operators of video surveillance systems located in their respective buildings are individuals who have been assigned responsibility by deans, directors, or other executive authorities. The list of the authorized users will be updated annually by the UWPD IS Unit.
I. All surveillance records will be stored in a secure centralized location for a period of 120 days.
J. Any Select Agent (SA) location will be on its own video network, separate from the general campus-wide security surveillance network. The SA labs and research areas will be equipped with a notification system informing DoIT and UWPD of problems or issues with the video surveillance system.

III. INSTALLATION AND ISSUANCE

A. UWPD will make assessments for new camera locations not already in existence. The assessments will be made in consultation with building occupants, DoIT and FP&M Physical Plant as needed and appropriate.
B. UWPD's IS Unit will maintain a current inventory of permanent camera installations.
C. UWPD's IS Unit will facilitate access to recorded images of possible crimes and incidents requiring investigation.
D. All requests for installing video surveillance on UW-Madison property must be routed to the IS Unit of the UWPD. A representative of the IS Unit will then conduct a security survey (also called a SCOPE report) and forward to the appropriate entities, i.e., FP&M Physical Plant, DoIT, AIMS, to develop a cost estimate for the requestor.
E. All video surveillance equipment must comply with current University standards. See Appendix.
F. Notification of camera and network problems or issues will occur through an alarm or other notification system authorized by DoIT.
G. Video surveillance will connect to the authorized server and in circumstances identified by the UWPD IS Unit, will be encrypted.
H. All new installations of video surveillance scheduled after the effective date of this policy must be in compliance with the terms and conditions of this policy and must meet the technical specifications and campus standards listed in the Appendix.
I. Existing installations must be brought into compliance with this policy at the time that replacement or upgrades of security surveillance camera systems and components occurs.
J. All original recorded images generated by surveillance cameras must be stored in a secure location established by DoIT and UWPD.

Consequences for Non-Compliance

VIOLATIONS AND SANCTIONS:

Violations of this policy by operators of surveillance camera systems will be considered misconduct on the part of the employee and will be subject to institutional or criminal sanctions.

UWS 18.06 Conduct on University Lands

(6) PHYSICAL SECURITY COMPLIANCE. (a) No person may ignore, bypass, circumvent, damage, interfere with, or attempt to deceive by fraudulent means, any university authorized security measure or monitoring device, whether temporary or permanent, that is intended to prevent or limit access to, or enhance the security of, university lands, events, facilities or portions thereof. (b) No person may duplicate, falsify or fraudulently obtain a university key or access control device, or make any unauthorized attempt to accomplish the same. (c) No person who is authorized to possess a university key or access control device may transfer a university key or access control device to an unauthorized person, nor may any unauthorized person be in possession of a university key or access control device. (d) Any university

key or access control device in the possession of an unauthorized person may be confiscated by any authorized University official.

UWS 18.13 Penalties

Unless otherwise specified, the penalty for violating any of the rules in ss. UWS 18.06 to 18.12 shall be a forfeiture of not more than $500, as provided in s. 36.11(1)(c), Stats.

Note: Violations of the rules in ss. UWS 18.06 to 18.12 will be processed in accordance with the citation procedure established in s. 778.25, Stats.

History: Cr. Register, March, 1976, No. 243, eff. 4-1-76; am. Register, November, 1991, No 431, eff. 12-1-91; CR 08-099: renum. From UWS 18.07 and am. Register August 2009 No. 644, eff. 9-1-09.

Supporting Tools

Appendix: Camera Specifications from 2014 Request for Proposal – UW-Madison Standards

---

Responsibilities

This policy will be maintained by the Video Surveillance Oversight Board and revisions may be made as needed.
Members: UW-Madison Associate Vice Chancellor/Chief of Police, UW-Madison Associate Vice Chancellor for Facilities Planning and Management and the Director of the UW-Madison Division of Information Technology.

Appendix – Camera Specifications from 2014 Request for Proposal

All Cameras:

- Work with the Milestone XProtext Corporate Edition
- PoE
- Work within WI temperatures Indoors- -10C to 50C, Outdoors -40C to 50C

PTZ (Point to Zoom) Outdoor Cameras:

- Day/Night Functionality
- H.264 compliant
- Tour Recording Capable
- 20x optical zoom or better
- Wide Dynamic Range compatible with the ability to account for varying environmental conditions
- 1080p compliant or better
- Image stabilization
- SD/ Card compatible with ability up to or more than 64gb
- Standard 3 year warranty or better
- Auto focus
- IR Illuminator

PTZ Indoor:

- Wide Dynamic Range compatible with the ability to account for varying environmental conditions
- H.264 Compliant
- Tour Recording Capable

- 20x optical zoom or better
- 1080p compliant or better
- Image stabilization
- SD/ Card compatible with ability up to or more than 64gb
- Standard 3 year warranty or better
- Auto focus
- Day/Night Functionality
- IR Illuminator

Indoor-Fixed:

- Auto focus
- Wide Dynamic Range compatible with the ability to account for varying environmental conditions
- 1080p compliant or better
- H.264 compliant
- 4x digital zoom or better

Outdoor Fixed:

- Auto focus
- Wide Dynamic Range compatible with the ability to account for varying environmental conditions
- 1080p Compliant or better
- H.264 Compliant
- 4x digital zoom or better
  180 degree