Camera and Card Access

ROWAN UNIVERSITY

Title: *Camera and Card Access Policy*
Subject: *Information Security*
Policy No: *ISO:2013:17*
Applies: *University-Wide*
Issuing Authority: Senior Vice President for Information Resources and Technology and Chief Information Officer
Responsible Officer: *Director of Information Security*
Adopted: *07/01/2015*
Last Revision: *07/20/2018*
Last Review: *07/20/2018*

I. PURPOSE

The purpose of this policy is to regulate the use of access control and camera systems used to monitor access, observe and record public areas for the purposes of safety and security. The existence of this policy does not imply or guarantee that access control or cameras will be monitored in real time 24 hours a day, seven days a week.

II. ACCOUNTABILITY

Under the direction of the President, the Chief Information Officer, Assistant Vice President of Public Safety, and the Director of Information Security shall implement and ensure compliance with this policy. The Deans, Vice Presidents, and other members of management will implement this policy.

III. APPLICABILITY

This policy applies to all University departments, administrative units, and auxiliaries. This policy does not address the use of general-purpose web cameras for special interest applications or University promotion purposes, but it should be noted that such cameras must not be used as a substitute for a security system.

IV. DEFINITIONS

1. ***Access Control*** - The use of computer-controlled entry and locking devices to limit and log access to areas of a physical facility, usually by means of a digitally-enclosed identification card or biometric device.
2. ***Information Technology Security Board (ITSB)*** - A unified effort jointly managed by the Chief Information Officer and the Director of Information Security, working closely with Risk Management, Network and System Service (NSS), Public Safety, Facilities Services, and other University units, as warranted. The ITSB governs technical and operational security solutions specific to the University's needs. The ITSB will recommend security measures compliant with this policy, and security best practices.
3. ***Security Control Owner*** – The Department, Dean, or VP who is responsible for the area that is being secured by a camera and/or control access system.
4. ***Video Surveillance*** - The use of image capture, processing, transmission and storage equipment for authorized monitoring of public areas. This includes full-motion and still images, use of network transmission capacity, and digital storage and retrieval software. Audio recording is specifically excluded from this definition.

V. REFERENCES

1. Rowan University Information Security Policy

POLICY

1. Rowan University is committed to enhancing the quality of life of the campus community by integrating the best practices of safety and security with technology. A critical component of a comprehensive security plan is the utilization of physical security (including access control and camera systems) and information security. The access control and surveillance of public areas is intended to deter crime and assist in protecting the safety and property of the Rowan University communities. This policy addresses the university's safety and security needs while respecting and preserving individual privacy.
2. To ensure the protection of individual privacy rights in accordance with the university's core values and state and federal laws, this policy is adopted to formalize procedures for the installation of access control systems and surveillance equipment and the handling, viewing, retention, dissemination, and destruction of surveillance records.
3. The University has the authority to select, coordinate, operate, manage, and monitor all campus access controls and security surveillance systems pursuant to this policy. All departments using access control or camera surveillance are responsible for implementing and complying with this policy in their respective operations. All existing uses of security access control or camera systems will be required to comply with the policy at a future date. A notification of the compliance date will be made 12 months in advance. Unapproved or nonconforming systems may need to be removed prior to the compliance date.
4. Responsibilities
    a. Public Safety and the Information Security Office must review and approve any proposed or existing installation of video or access control security systems on properties owned, leased, or controlled by the University. All video and access control security systems must conform to federal and state law in addition to University policy. Video and access control security systems must conform to standards established by the ITSB so recorded data and log records are easily retrievable
    b. Except for the work counter where cashiering services are performed or money is exchanged during the regular course of business, video monitoring will not be used to view or record workstations, including private offices; desks or cubicles; classrooms or rooms where students and/or faculty commonly work, study or hold discussions; living areas; or other common-use areas where a reasonable expectation of privacy exists.
    c. Video and access control security records will not be used for purposes related to the routine evaluation of employee job performance, nor will they be used as a means to track employee attendance and/or as a timekeeping record. However, the University may use such records in support of disciplinary proceedings against faculty, staff, or student(s), or in a civil suit against person(s) whose activities are shown on the recording and are relevant to the suit.
    d. Nothing in this policy shall be interpreted to prevent the use of video monitoring or surveillance in connection with an active criminal investigation or specific court order.
    e. Any person who tampers with or destroys a camera or access control system may be prosecuted in the criminal justice system as well as the campus judicial system.
5. Operational Considerations
    a. Video and access control system review or monitoring for security purposes will be conducted in a professional, ethical, and legal manner. Personnel involved in video review or monitoring will be appropriately trained and supervised in the responsible use of this technology
    b. The focus of cameras used in video surveillance will not cover areas where there is an expectation of privacy. This does not preclude monitoring the exterior of buildings, building lobbies, parking lots, roadways, or public areas.
    c. All recording or monitoring of activities of individuals or groups by university security cameras and access control systems will be conducted in a manner consistent with university policies, state and federal laws, and will not be based on the subjects' personal characteristics, including age, color, disability, gender, national origin, race, religion, sexual orientation, or other protected characteristics. Furthermore, all recording or monitoring will be conducted in a professional, ethical, and legal manner. All personnel with access to university security cameras or access control systems should be trained in the effective, legal, and ethical use of monitoring equipment.

In addition they will receive a copy of the Video Surveillance & Access Control Policy and will provide written acknowledgement that they have read and understood it. Failure to provide written acknowledgement does not excuse violation of the policy.

d. University security cameras and access control systems may not be monitored continuously under normal operating conditions but may be monitored for legitimate safety and security purposes that include, but are not limited to, the following: high risk areas, restricted access areas /locations, in response to an alarm, special events, and specific investigations authorized by Public Safety or the Information Security Office.
e. Depending on the situation, the information obtained in violation of the Video Surveillance & Access Control Policy may or may not be used in a disciplinary proceeding against a member of the University's faculty, staff, or student population. It is not the intent of this policy to use video cameras for the monitoring of employees for disciplinary purposes, performance evaluation, or corrective action.
f. All access to live or recorded camera and access control information shall be limited to authorized personnel only. The copying, duplicating and/or retransmission of this information must be authorized by Public Safety and the Information Security Office.
g. Personnel are prohibited from using or disseminating information acquired from university access control or security cameras, except for official purposes. All information and/or observations made in the use of access control or security cameras are considered confidential and can only be used for official university and law enforcement purposes.
h. The installation of "dummy" cameras that do not operate is prohibited. Unless being used for criminal investigations, all video camera installations should be visible.

6. Placement of Camera
    a. The locations where cameras are installed may be restricted access sites such as a departmental computer lab; however, these locations are not places where a person has a reasonable expectation of privacy. Cameras will be located so that personal privacy is maximized.
    b. No audio shall be recorded except in areas where no one is routinely permitted. Requests to utilize audio surveillance that does not comply with this requirement will be evaluated on a case by case basis by Public Safety or the Information Security Office.
    c. Camera positions and views of residential housing shall be limited. The view of a residential housing facility must not violate the standard of a reasonable expectation of privacy.
    d. Unless the camera is being used for criminal investigations, monitoring by security cameras in the following locations is prohibited:
        i. Student dormitory rooms in the residence halls
        ii. Bathrooms
        iii. Locker rooms
        iv. Offices
        v. Classrooms not used as a lab
7. Storage and Retention of Recordings
    a. No attempt shall be made to alter any part of any surveillance recording or access control system. Access control and surveillance camera systems will be configured to prevent tampering with the transmission, storage, and duplication of recorded information.
    b. Access control or surveillance records shall not be stored by individual departments. All surveillance and access control records shall be stored in a secure university centralized location for a minimum of 30 days (or longer for sensitive data) and will then promptly be erased or written over, unless retained as part of a criminal investigation or court proceedings (criminal or civil). Individual departments shall not store video surveillance or access control information.
    c. A log shall be maintained of all instances of access to or use of surveillance and access control records. The log shall include the date and identification of the person or persons to whom access was granted
8. Requests for Camera and Access Control Systems
    a. All requests for new cameras/access control systems must be submitted through the IT Acquisition Process with budget approval from the Department Head who is making the request. Once approved by the department head, the request must also be approved by Public Safety and the Information Security Office before the project can be started. Each new system must be assigned a Security Control Owner.

b. All requests for changes to existing cameras/access control systems, and removal of cameras /access control systems must be approved by Public Safety and the Information Security Office in advance.
c. All requests for individual user access to specific card access readers or security control areas must be approved by the Card Office or the designated "Security Control Owner"
d. All requests, as defined in this policy, must be initiated through the IT Acquisition Process (for new installations) or the IRT Support Desk (for all other requests). There are three convenient ways to submit a request to the IRT Support Desk:
    i. On the Internet visit http://support.rowan.edu. Login with your network username and password. If you do not know your username or password go to http://www.rowan.edu/password to reset your password and retrieve your username.
    ii. Send mail to support@rowan.edu.
    iii. By telephone, if on campus call **Extension 4400**. If you are off campus dial 856.256.4400.
e. All *facility work orders* for Cameras or Card Access Systems must not be started until the work is approved by Public Safety and the Information Security Office. Each work order must reference an approved IRT request ticket to ensure compliance with Audit requirements.
f. All *facility projects* that include Cameras or Card Access Systems must be approved by Public Safety and the Information Security Office. Each project must reference an approved IRT request ticket to ensure compliance with Audit requirements. An IRT request ticket should be submitted once the final security design is completed. Any changes to the final security design must be approved in the same manner throughout the project lifecycle.
g. All requests for "*Administrator Access*" must be reviewed and approved by the Information Security Office prior to any changes.
h. All requests will be logged and tracked through the IRT request system initially to ensure compliance with Audit requirements. Once approved, requests can then be tracked though additional systems used by Facilities, the Card Office, Public Safety, and the Information Security Office as needed.
i. The ITSB reserves the right to update the above request processes as needed to ensure compliance with this polic

9. Exceptions
    a. This policy does not apply to cameras used for academic purposes. Cameras that are used for research would be governed by other policies involving animal or human subjects and are, therefore, excluded from this policy.
    b. This policy does not address the use of Webcams for general use by the university. This policy also does not apply to the use of video equipment for the recording of public performances or events, interviews, or other use for broadcast or educational purposes. Examples of such excluded activities would include video recording of athletic events for post-game review, video recording of concerts, plays, and lectures, or video recorded interviews of persons. Automated teller machines (ATMs), which may utilize cameras, are exempt from this policy.

VII. NON-COMPLIANCE AND SANCTIONS

Any departments that violate this policy may be required to remove and replace of any unapproved Camera or Card Access System at the department's expense. In addition, any individual who violates this policy may be subject to discipline or dismissal from the University as well as civil and criminal penalties. Sanctions shall be applied consistently to all violators regardless of job titles or level in the organization

VIII. ATTACHMENTS

1. Attachment 1, Camera and Access Control System Standard

By Direction of the CIO:

Mira Lalovic-Hand,
SVP and Chief Information Officer

ATTACHMENT 1
ACCESS CONTROL DESIGN AND CONSTRUCTION STANDARD

1. GENERAL
    a. This Access Control Design and Construction standard applies to all new construction and renovation projects, as well as single device installations on the Rowan University campus, and any other location or campus subject to the University.
    b. This standard applies to employees, contractors, design professionals, and tradespeople involved in the design, procurement, or installation of electronic security devices or systems.
    c. The electronic security devices/systems encompass computers, network connections (including wireless), data transmissions, communication devices, multiple points of monitoring, interfacing controls, sensors, and actuators. Some functions may be supported locally as well as University-supported.
    d. For the purposes of this standard, electronic security systems or devices include:
        i. access control (wired and wireless)
        ii. networked video surveillance
    e. Security and access control systems must be integrated with the University central systems unless an exemption has been granted.
        i. For **Access Control and Video Surveillance systems**: the Director of Information Security, Director of Network and System Service (NSS), Public Safety and Facilities Services shall be consulted during the initial design or planning, during schematic and construction design reviews, during construction if a scope change occurs or clarification is needed, and prior to building occupation, a signoff is required by all groups listed above
    f. Electronic security systems/devices are not to be connected by hardware, integrated by software, or otherwise interfaced with any other control systems (ex. Building Automation Control System) or life safety systems unless specifically required by code or approved by appropriate system owner and the Director of Information Security, Network and System Service (NSS), Public Safety and Facilities Services.
    g. Electronic security systems/devices planning should be incorporated into the overall building design. Physical security devices and measures, as well as electronic devices and connections, are to be considered at the same time as comfort, function, energy efficiency, maintainability, life safety, accessibility, environment, inspiration and any other primary feature attributed to a facility.
2. QUALITY ASSURANCE
    a. The design of all security and/or access system installations shall be performed by a qualified individual, either licensed as a Professional Engineer or certified as a security professional. Consultant shall provide credentials to the Rowan University project manager upon request.
    b. The integrated security and/or access system including all equipment, components, and accessories shall be Underwriters Laboratories (UL) listed for this purpose.
    c. The Contractor providing the security and/or access system must be certified and licensed to install security and access control systems.
3. SYSTEM DESIGN
    a. For all renovations and new-construction projects, consultants shall engage the Director of Information Security, Network and System Service (NSS), Public Safety and Facilities Services.
    b. The following elements should be incorporated into the basis of all designs:
        i. Type of security or access system
        ii. List applicable Codes and Standards
        iii. Identify Building Occupancy Type
        iv. Sequence of operation (especially when fire alarm and access control systems are interconnected)
        v. Wiring type
        vi. Main equipment locations
        vii. Special considerations (for example, when a facility houses animals or human remains

c. Drawings and Specifications shall include all requirements for Submittals and for As-Built information. Submittals shall contain the following information:
    i. Product information for all installed components
    ii. System diagram with typical equipment and device connection and labeling (a detailed connection diagram is not required until project completion)
    iii. Wire schedule
    iv. Battery stand-by calculations
    v. Special system requirements (interlocks with other systems, for example)
    vi. System labeling materials and methods
    vii. Surveillance system storage capacity calculation
d. Surveillance Camera Lay-out
    i. Place cameras near entrances and exits to school buildings
    ii. Install surveillance for campus parking lots
    iii. Mount cameras in at-risk areas such as poorly lit walking paths and locations where students and faculty might find themselves alone and defenseless
    iv. Position cameras in campus stores, cashier offices, and other areas where money is exchanged
    v. Have proper video surveillance for sports facilities
    vi. Monitor common areas such as stairways, lobbies
    vii. Install security cameras at all residence hall

    Note: Typically we would recommend one interior camera per perimeter door, one interior camera per building lobby and perhaps one interior camera per elevator lobby. Special attention will be given to areas within the building that require special attention, but those could be handled on a case by case base.
    The exterior requirements will be flexible because each building is different and some may not require any coverage. However, if the building is adjacent to a student walkway, is isolated, or is used for student congregation, exterior cameras will be required to adequately monitor those areas

4. SUBMITTALS
    a. To ensure compliance with the intent of this standard, all system final designs and associated contract submittals shall be reviewed by the Director of Information Security, Network and System Service (NSS), Public Safety and Facilities Services.
    b. One (1) copy of each new project submittal shall be sent to the Director of Information Security, Network and System Service (NSS), Public Safety and Facilities Services for review and comment prior to releasing final approved submittals to the contractor
5. SYSTEM DESCRIPTION
    a. Card Access Systems :Wired/Wireless: are comprised of card reader, door contacts, electric hinge or power transfer (wired systems), door strike, latch, reader interface module, interconnecting power and communication wiring, head-end intelligent system controller. All systems, unless exempted from University policy, are centrally monitored - transmitting data to and received by the Access Control System.
    b. Network Video Surveillance Systems :Wired/Wireless: are comprised of IP-enabled cameras, interconnecting power and communication wiring via POE (power over Ethernet). Cameras must be connected to a POE-enabled switch with ports enable on the appropriate security VLAN unless approved by the Director of Information Security and/or Network and System Service (NSS). All systems, unless exempted from University policy, are capable of being centrally monitored - transmitting data to and received by the Video Management Systems.
6. PRODUCTS
    a. Manufacturers
        i. All equipment must be designed with open system architecture.
        ii. All systems and infrastructure components that support the video surveillance and access control systems shall be equipped with battery backup in the event of a power failure and capable of operating for a minimum of 8 hours.

iii. All system components installed must be compliant with a current version of this standards document, defined as any version of this document valid within 120 days of installation of the system. Requests for the current version of the standard can be submitted to support@rowan.edu.
iv. Subject to compliance with requirements, provide products by one of the following

Note: All non-standard existing security access control or camera systems will be required to comply with this standard at a future date.

Description	Manufacture	Where deployed (if known)	Standard or Non-Standard
Access Control Software	RS2 https://rs2tech.com	SOM deployed, applies to all future deployments of any size	Standard
Access Control Panel /Microprocessor Hardware	Mercury http://www.mercury-security.com/	SOM deployed, applies to all future deployments of any size.	Standard
Video Management System/Software (VMS) Enterprise Level Only	Exacqvision https://exacq.com	For all Rowan locations	Proposed New Standard
Video Surveillance Camera – (Indoor) Individual scenario will dictate what model camera should be used	AXIS, Sony, and Arecont Vision www.axis.com https://pro.sony.com/bbsc/ssr/mkt-security/ www.arecontvision.com	For all Rowan locations	Proposed New Standard
Video Surveillance Camera – (Outdoor) Individual scenario will dictate what model camera should be used	AXIS, Sony, and Arecont www.axis.com https://pro.sony.com/bbsc/ssr/mkt-security/ www.arecontvision.com	For all Rowan locations	Proposed New Standard
Video Management System/Software (VMS)	Exacqvision https://exacq.com See section entitled "Video Management System Environment" for software licensing and configuration details.	For all Rowan locations	Proposed New Standard
Management System Hardware	See section entitled "Video Management System Environment" for software licensing	For all Rowan locations	Currently use

	and configuration details.		d as Standard
Intelligent Locksets.	Sargent (wireless and online types only) http://www.sargentlock.com/products/product_landing.php?item_id=1589	For selected Rowan Locations. (Request assistance from office of Director of Information Security prior to selecting appropriate intelligent locks)	Proposed New Standard
Intelligent Locksets	Allegion (Wireless and Wired types) www.allegion.com	For selected Rowan Locations. (Request assistance from office of Director of Information Security prior to selecting appropriate intelligent locks)	Proposed New Standard
Intelligent Locksets	Salto (Sallis and CVN) http://www.salto.us/	For selected Rowan Locations. (Request assistance from office of Director of Information Security prior to selecting appropriate intelligent locks)	Proposed New Standard
Access Control Card Readers	Allegion MT series	For all Rowan Locations	Standard
Video Surveillance Manager (VMS)	Cisco	Camden, Glassboro residential spaces	Non-Standard
Video Surveillance Camera	Cisco (Pelco)	Camden, Glassboro residential spaces	Non-Standard
Access Control for entry doors, elevators, stairwells, etc.	Blackboard	Camden (Medical school), Glassboro (CGCE)	Non-Standard
Video Surveillance Camera - Advidia (A-44-IR)	Advidia	CGCE	Non-Standard
Video Surveillance Camera - Elevator camera (ELV-650)	Advidia	CGCE	Non-Standard
Video Surveillance Camera - ACTi (KCM-7911)	Act-I	CGCE	Non-Standard

Video Management System/Software (VMS)	Video Insight	CGCE	Non-Standard
Video Surveillance Camera – Access P3367	Access	Glassboro residential locations	Non-Standard
Video Surveillance Camera – Access 216	Access	Glassboro residential locations	Non-Standard
Video Surveillance Camera – Access PIZ	Access	Glassboro residential locations	Non-Standard

b. Video Management System Hardwar
The security integrator shall provide all required software for at least one recording server, one Enterprise Management Server and at least one fail-over server as follows. All server hardware (excepting the EMS server) will be provided by the integrator, and will be installed in a main campus datacenter by the integrator in coordination with the Information Security Office (ISO) and Network and System Services:
   i. The VMS Recording server hardware will meet the following minimum requirements:
      1. Required Server Model: HP DL380 G9
      2. Intel Xeon 8-core x 20MB Cache (minimum)
      3. 64 GB RAM
      4. NIC: 4x1000 Mbps
      5. Redundant Power Supplies
      6. Windows Server 2012 Enterprise
      7. Four post rack mounting kit
      8. Storage:
         a. Minimum 20TB raw storage
         b. Minimum two hot spare drives
         c. Sufficient storage to meet retention requirements with all cameras recording at their highest available resolution at 10 FPS based on 50% motion for indoor cameras and 24/7 recording for outdoor cameras.
         d. Storage calculation should include 30 day retention requirement for non-clinical areas, 90 day retention requirement for clinical areas.
         e. No drive larger than 4TB. No drive smaller than 3TB.
         f. Storage calculations, including RAID and hot spare overhead as well as disk usage per day per camera based on the above specifications, must be included in all proposal submittals.
         g. Dedicated operating system partition of 60GB (minimum)
      9. If storage requirement exceeds the capacity of a DL 380 G9 multiple servers may be necessary.
      10. Enterprise Level Video Management software for serve
      11. Four year next business day warranty direct from HP
      12. Professional series camera software licenses for each connected camera/device. Provide 10% spare licenses above quantity required for project.
      13. Three year software support agreement to cover upgrades
   ii. The Failover VMS Recording server hardware will meet the following minimum requirements:
      1. Required Server Model: HP DL380 G9
      2. Intel Xeon 8-core x 20MB Cache (minimum)

3. 64 GB RAM
4. NIC: 4x1000 Mbps
5. Redundant Power Supplies
6. Windows Server 2012 Enterprise
7. Four post rack mounting kit
8. Storage:
    a. Minimum 20TB raw storage
    b. Minimum two hot spare drives
    c. Sufficient storage to meet retention requirements with all cameras recording at their highest available resolution at 10 FPS based on 50% motion for indoor cameras and 24/7 recording for outdoor cameras.
    d. Total usable storage capacity after RAID and hot spare overhead must provide 7 (seven) days retention for all cameras the system is intended to provide failover for.
    e. No drive larger than 4TB. No drive smaller than 3TB.
    f. Storage calculations, including RAID and hot spare overhead as well as disk usage per day per camera based on the above specifications, must be included in all proposal submittals.
    g. Dedicated operating system partition of 60GB (minimum).
9. If storage requirement exceeds the capacity of a DL 380 G9 multiple servers may be necessary.
10. Enterprise Level Video Management software for server
11. Four year next business day warranty direct from HP
12. Professional series camera software failover licenses for each connected camera /device. Provide 10% spare licenses above quantity required for project.
13. Three year software support agreement to cover upgrades

iii. Enterprise System Manage
1. License for Enterprise System Failover (EVESM)
2. Three year software support agreement to cover upgrades.
3. Server environment for ESM will be provided by the University

iv. System Operation and Performance
1. System operation and performance should include, but not be limited to, the following features
    a. Proper activation of door hardware when a valid credential is presented
    b. Appropriate shunting of the alarm upon exit from secured space
    c. Video signal being transmitted over IP
    d. Alarm initiation
    e. Trouble initiation
    f. Activation of alarm notification
    g. Activation of trouble notification
    h. Total supervision, monitoring of abnormal conditions in the system
    i. Activation of off-premise signals that are sent to the VMS via the Access Control System or Ethernet