PHYSICALLY MANAGED ELECTRONIC ACCESS CONTROL, VIDEO SURVEILLANCE

Overview

1. All questions on equipment approvals in this section shall be forwarded to Card Access Security Operations (CASO) 4400 University Drive, 5A5, Fairfax, VA 20330 (703) 993-1004 option 2.
2. Requirements in this section apply to all new construction, as well as remodeling projects.
3. CASO will conduct a security assessment during the Design Development phase.
4. The purpose of the security assessment shall be to apply George Mason University security design criteria and:
    - Determine whether or not an electronic access control system shall be incorporated into the scope of the project.
    - Determine whether or not a video surveillance system shall be incorporated into the scope of the project.
    - Determine whether or not an electronic intrusion alarm system shall be incorporated into the scope of the project.
5. The security assessment will utilize the following security design criteria matrix. The following categories should follow the designs below:

Category 1

Areas

- General Purpose Elevators
- General Purpose Corridors

Requirements

- **Video Surveillance**
    - Building Interior Spaces - Genetec VMS

Category 2

Areas

- Low Risk Supply/Equipment Storage Areas

Requirements

- **Video Surveillance**
    - General Observation Entry Access Points - Genetec VMS

- **Security Keying System**
    - Building Interior - BEST GMU Standard

Category 3

Areas

- Office Suites
- Low Risk Research Laboratories
- General Purpose Classrooms

Requirements

- **Video Surveillance**
    - Entry Access Points - Genetec VMS
    - Building Interior Spaces - Genetec VMS
- **Electronic Access Control System**
    - Entry Access Points - RS2 Technologies
- **Security Keying System**
    - Entry Point – Coremax

Category 4

Areas

- High Value Supply/Equipment Storage Areas
- Technology Enhanced Classrooms
- Targeted Facility Elevators
- Targeted Facility Corridors
- Links, Tunnels, and Skyways

Requirements

- **Video Surveillance**
    - Entry Access Points - Genetec VMS
    - Building Interior Spaces - Genetec VMS
- **Electronic Access Control System**
    - Entry Access Points - RS2 Technologies
- **Security Keying System**
    - Entry Point – Coremax

Category 5

Areas

- Building Entries
- Housing and Residential Life
- High Risk Research Laboratories
- Computer Laboratories
- Pharmacies
- Controlled Substance Laboratories
- Cash Handling Areas
- Special Event Venues
- Loading Docks
- Parking Lots, Ramps, and Garages
- Federal Government Facilities
- Executive Offices and Residences

Requirements

- **Video Surveillance**
    - Entry Access Points - Genetec VMS
    - Building Interior Spaces - Genetec VMS
    - Video Analytics - Analytics compatible with Genetec VMS
        - Basis of design Hanwha P-Series cameras
- **Electronic Access Control System**
    - Entry Access Points - RS2 Technologies
- **Security Keying System**
    - Entry Point – Coremax

Electronic Access Control Systems

1. Incorporate all exterior doors with hard-wired card access for all buildings.
2. Rekeying of all exterior doors is required upon completion of installation and testing.
3. All card reader control panels shall be tied into building emergency power have a minimum 12-hour (design calculations required) battery backup, and battery standby power supplies to maintain database programming and card reader operation. Electric locking devices on perimeter doors with electric locks operated by card readers shall have battery standby power supplies.
4. The George Mason University's Access Control System operates on RS2 Technologies, Access IT! Universal platform. All card readers on perimeter doors, perimeter door access control systems, and door monitoring systems shall interface with this system.

5. Use conduit and raceways on system installation. They shall comply with conduit and raceway standards specified in Section 16131 - Raceways, and the manufacturer's requirements of the access control systems.
6. System installation shall use wire and cable that complies with wire and cable standards specified in Section 16120 - Wires and Cables, and the manufacturer's requirements of the access control systems.
7. Refer to Division 8, Section 08700 - Finish Hardware for system hardware requirements.
8. Access control systems shall have the following components/capabilities:
    - SEOS Smart Cards: Access control systems must be able to read and reference university-manufactured, encoded and issued George mason University Cards containing SEOS smart card technology and mobile credentials for Apple and Android phones.
    - HID Signo Card Readers: Card readers shall be Smart Card readers and mobile credentials for Apple and Android phones. (40TKS-01-00PBXK)
9. Nominal Card Reader Mounting Height: Card readers shall be mounted at the following heights:
    - Interior: 42 inches to center above the finished floor
    - Exterior: 36 inches to center above the finished floor
    - Elevators: 36 inches to center above the finished floor
    - Bollard Mount: 36 inches to center above the walkway.
10. A door position switch is required on all door installations.
11. An integrated request to exit detector is required on all door installations. The exit motion detector shall not be used to unlock the doors.
12. Card Reader Control Panels: Mercury Panel Based (RS2 Operating System).
    - The panel will be connected with the existing University Access Control (RS2 operating system)
    - Access Control panel Management System jack connection: Installation of a connection at least two weeks prior to being required. Locate the jack within the SCP Access Control panel.
13. Electric Lock Power Supply: Life Safety RS2 Power supplies shall include electric door control and exit devices on perimeter doors and interior doors.
    - Battery backup is required in all power supplies.
    - Power supplies must be tied to building emergency power
    - Power supply must provide 12V outputs to supply SCP and SIO board power individually.
    - Power supply must provide 24V outputs to supply lock power to each individual lock.
    - All power supplies must have ethernet network interface ability.
    - Each lock/device will have its own dedicated power output.
    - Each individual board will have its own data output.
14. Elevator Control: Elevator control shall be managed from the University Card Access Management System with the following components/capabilities, if elevator controller is required:
    - One controller per elevator that services four or more floors
    - Cable and wire that connects the card reader to the access system elevator controller. Refer to Division 14, Section 14200 – Elevators
15. Basis of Design Access Control and Site Management System Manufacturers

- RS2 Technologies. (Access Control System Control Processors, Reader Controllers, Input/Output Monitor/Control Modules, Entry/Display Terminals, Multiplexers, Channel Input/Output Modules, System Application Software)
- Mercury Hardware (System Control Panels, and Interface Panels) (RS2 OEM certified)
- HID Signo Card readers (Card Readers) (Mobile credential programmed, Apple and Android, George Mason University elite key)
- Sargent Manufacturing (Integrated Card Reader Locking Devices and Accessories)
- Securitron Corporation (Door Position Switches)
- Life Safety FPO150 (Power Supplies)
- Life Safety RS2 panels

Video Surveillance Systems

1. Video Surveillance shall be incorporated into the design of all building access points (above and below grade) within new construction projects.
2. Video surveillance installations shall be Physically monitored and recorded by CASO in accordance with university archive and retrieval policy.
    - When special circumstances create the need for specific business use of video surveillance (Genetec VMS), a standalone installation may be used. Such installations require a written exemption from the Director of CASO and written acceptance of liability by the Director of the customer unit.
3. Video surveillance systems shall have the following components and capabilities:
    - Video surveillance systems shall include digital recording, multiplexing and Internet-based server capabilities.
    - Exterior cameras shall be both environmentally protected and heated. Provisions for preventing snow and ice build-up shall be included.
    - Daytime and nighttime cameras equipped with an electronic auto iris are required for all exterior applications.
    - Interior cameras shall be premium grade and provide high resolution color images. Applications that have variable lighting conditions shall require an auto iris lens on each interior camera.
    - Acceptable equipment shall include:
        - Genectec VMS Platform
        - Servers housing Digital Video Recordings shall be managed by the CASO Team. These servers must match existing servers in the data center. Funding must be included to contribute to this server node expansion.
        - Fixed Cameras shall be Hanwha or Axis IP with suitable housing, mount, and accessories to provide a functional camera system.
        - If the camera is located in a low light area, an IP day/night camera option will be used.
        - All locations that would normally use a pan tilt and scan camera will use an IP based 180-degree or 360-degree camera based on the accepted brands, with suitable housing, mount, and accessories to provide a functional camera system.
        - Outdoor installations will require an Axis or Hanwha cameras and associated mounts (as well as other needed connected devices).

Key Control

1. To maintain strict security controls within new construction and renovation projects, all cylinders, cores, and keys shall be supplied at a cost to the project by the Locksmith Services unit within the department of Key Control, 4000 University Drive, DE5, Fairfax, VA 20330. (703) 993-2823.
    - Product type shall be determined based upon security design criteria and specified by Key Control, in agreement with the end user.
    - For new buildings, specify small format seven-pin BEST cylinders with interchangeable cores, provided by the GMU Key Control unit.
    - Internal lock cylinder set screws are prohibited. The contractor shall pay for removing internal lock cylinder set screws that have been installed.
2. Key Control Locksmith Services shall participate in the Design Development phase of the project to determine keying systems, schedules, and costs.
3. The A/E shall set up a planning meeting six months before a building is occupied to review final keying schedules. Keying schedules shall be agreed upon by GMU Key Control.
4. The preliminary planning meeting shall include the A/E, a representative from the primary building occupant(s) and representative(s) from the GMU Key Control unit.
5. A GMU locksmith representative will order and install the cores.
6. For security purposes, construction cores will be used in the absence of existing permanent cores. At the end of the project, permanent cores will replace all construction cores.
7. Re-keying of all exterior doors is required upon completion of installation and testing. Emergency bypass keys shall be created and distributed as follows to:
    - Fire Department Lock Box
    - Building Systems Automation Center