

**DESIGN STANDARDS**

1. General: This section contains guidelines and criteria for the design, equipment selection and installation of campus building security monitoring and access control systems.
  - 1.1 All building security monitoring and access control systems shall be systems, equipment accessories as manufactured by Diebold and fully compatible with the current campus systems.
  - 1.2 All additional accessories or supporting hardware equipment shall be fully compatible with and able to integrate with the existing campus systems.
2. Building Perimeter Security Monitoring – All campus buildings with the exception of small service buildings shall be provided with a security monitoring and access control designed for the specific needs of the building with the following minimum requirements.
  - 2.1 Primary Entrances: Provide automatic electronic door locking that includes monitors to allow remote determination of door status: Unlocked vs. Locked, Open and unsecured vs. Locked and secure. Provide card reader or other means of identity based access.
  - 2.2 Secondary and Service Entrances: Same as primary entrances. Card reader or other means of identity based access only when required by program or the building layout.
  - 2.3 Exit only doors: Provide door sensors that allow remote monitoring of door status including: open and unsecured / closed and secure.
  - 2.4 Prop Alarm: For those doors determined through program at risk for use in theft, provide door prop alarm monitoring that allows setting the maximum time a door is allowed to remain open and unsecured after proper access either from building interior or exterior when in the secure mode.
  - 2.5 Specialty Doors: All unique or specialty doors shall include appropriate locking systems and monitoring as determined by the building program and security requirements.
  - 2.6 Automatic Doors: All automatic doors shall be fully integrated into the building security monitoring and access control system. The architect shall work with the automatic door system equipment supplier and the Diebold representative to coordinate the interface between the two systems to ensure that while providing for access to the disabled, that the proper security monitoring and access control is maintained in both the unsecured and secure modes.
  - 2.7 The final building security monitoring and access control system shall be approved by the campus police chief and the University's Project Manager.
  - 2.8 Panic Alarms: At locations determined to be at special security risks and as approved by the University's project manager, provide a concealed button placed convenient to personnel access. Activation of button shall provide a silent alarm at the University's central monitoring center alerting the police of the need for assistance.
  - 2.9 Internal Building Security: Additional internal building security monitoring and access control shall be determined through the building program and operations requirements.
3. Security and Access Control System / Equipment  
All security and access control system equipment, including controllers and power supplies, shall be located in accessible and secured rooms and may include technology rooms or building mechanical and

**DIVISION 13 – SPECIAL CONSTRUCTION  
SECURITY MONITORING AND ACCESS CONTROL**

**13200 -2**

electrical rooms secured by keyed locks. The selected room locations in the building shall allow for cabling distances appropriate for proper systems operation.

No power supplies or supporting equipment shall be located above ceiling or in concealed locations. All security monitoring and access control equipment to be on dedicated electrical circuits.

- 3.1. All controllers and power supplies shall be designed with capacity that allows for a minimum 50% expansion.
- 3.2. All new security monitoring and access control systems are to be hardwired. At a minimum, provide conduit from all monitor devices, hardware and equipment to accessible ceiling location to allow for convenient access for cabling replacement.
- 3.3. For renovation and retro-fit installations hardwiring of security monitoring and access control systems is preferred; however, wireless systems may be considered with approval by the University's project manager.

**PRODUCT STANDARDS**

1. General – Acceptable electric devices include electric strobes. Electric locks and panic devices. Magnetic locks are not desirable and may only be used when it uniquely solves the security in --- and is approved by the University's project manager.

End of Division 13 – Specialty Construction – Security Monitoring and Access Control