

APPENDIX Y

2006 Edition, Published January 1, 2006; Document Revision Date: New December 19, 2008

Basic Security Planning Minimum Design Requirements

The following minimum design requirements are to be used in the planning and design of all renovations and new construction projects at The Ohio State University. These design intents are based on current risk assessments, however, future changes will need to be accounted for as they present themselves. The design reviewers for The Ohio State University reserve the right to specify additional enhancements or security mandates based on new threat assessments.

Design intents for the minimum perimeter building standards:

1. All building entrances are to be connected to the centrally supported Alarm and Card Access Management System (ACAMS). All card readers are to be operated by ACAMS. All building entrances require electrically unlocking door hardware or a door contact with a delayed egress exit device per fire code requirements. Exterior door locations shall be equipped with a door position switch. All exit devices shall include fully adjustable latch bolt monitoring and request to exit switches integral to the door hardware. Mortise lock doors shall include latch bolt monitoring and request to exit switches integral to the mortise lock.
2. A minimum of two building entrances are to be equipped with card reader access reporting to ACAMS. One must be near the primary parking area for after-hours access.
3. All roof access and other accessible points of entry (including operable skylights, doors, hatches, etc.) must be equipped with door position switches monitored through the centrally supported ACAMS.
4. Building perimeter security is to include a building control keypad to provide onsite building access control.
5. The project budget will be financially responsible for implementing these standards and will be defined within the Memorandum of Understanding (MOU) of a new facility project.

Design intents for classrooms:

1. All classrooms will minimally be fitted with brass key core lockset with a thumb-turn latch bolt on the inside ("office function") of the perimeter doors and shatter resistant glazing.
2. Entry doors will need to incorporate shatter resistant glazing into the frame and/or door way. Glazing should not provide a mechanism for easy access of the door handle from the inside.
3. Classroom technology should be secured in one of the following fashions:
 - .1 At a minimum, classroom doors and ceiling spaces need to have conduit runs installed with pull strings to the nearest room containing an ACAMS panel for future expansion.
 - .2 A securable closet must be provided to secure all loose equipment (TV stands, VCR's, DVD players, etc.) in a central location for classrooms sharing equipment.
 - .3 Mounted technology devices will be secured and provided with an ACAMS reporting contact alarm.
 - .4 Technology enhanced rooms will have an ACAMS card reader with alarm keypad and security door contacts on perimeter doors reporting through ACAMS.

Design intents for the “Special Case” security enhancements:

1. Duress Alarms are required:
 - .1 In close proximity to permanent structures where cash, check, or charge transaction processing areas are located.
 - .2 Any area where external threats are perceived to be likely.
2. High value asset, whether of significant historical, cultural, artistic or monetary value require appropriate security measures [including but not limited to: ACAMS card reader, keypad, door contact, passive infrared motion sensor (PIR), glass break (GB), duress]. This type of area will include the use of specialized security devices and is to be monitored by ACAMS. Specific case examples include, but are not limited to: the John Glenn collection; college records; the Heisman trophy collection; geological samples; artwork collections; check writing materials; historic memorabilia; and trademark assets.
3. Research, radiation, biological, or chemical use labs must contain the appropriate level of security based on the use and contents of the facility:
 - .1 The minimum of an ACAMS controlled and monitored card reader on entry door reporting through ACAMS.
 - .2 Lab perimeter security and safety devices can include but are not limited to: ACAMS Card Reader, Keypad, Door Contact, PIR, GB, Duress
 - .3 Additional security features are to be required based on specific regulatory requirements.
4. Emergency phones are to be ADA accessible. The amount of emergency phones and their placement is at the discretion of the Facilities Design and Construction Project Manager and a Public Safety representative.

Design intents for Closed Circuit Television (CCTV) cameras and Digital Video Recorders (DVR's):

1. All construction must integrate CCTV and DVR technologies into the building's security plan.
2. All CCTV must be recorded locally and be must able to be monitored by the Department of Public Safety. All CCTV and DVR systems must meet OSU Public Safety requirements for remote viewing.
3. Loading dock areas require recorded CCTV.
4. All after-hours access points must have an interior mounted CCTV camera 15'- 25' from each single or pair of door leaves to monitor inbound traffic.
5. Cash handling operations require CCTV.
6. Parking structures must have cameras positioned to view all pedestrian and vehicular inbound and outbound traffic lanes. Multiple cameras must be positioned to capture license plates as well as driver descriptions.

Variance Application:

The OSU Building Design Standards Security Planning Standards Variance Application is for situations where it would be appropriate to modify/adjust a part(s) of this appendix.



**OSU Building Design Standards
Security Planning Standards Variance Application
Last Revision - 12/23/2008**

Person, Company, or Department requesting Variance:

Contact Name: _____ **Date:** _____
Phone: _____
Email: _____
Company Name: _____
College Name: _____
Department: _____
Mailing Address: _____
City/State/Zip: _____

OSU Project Information:

OSU Project Manager's Name*: _____
OSU Project Name: _____
OSU Project No.: _____

Variance Request: Reference Security Planning Design Standards:

The reasons for this variance application are that concerning peculiar conditions, a strict interpretation and/or compliance would work an unnecessary hardship, and that in granting the requested variance the general intent and purposes of the security planning design standards. Listed below are the special conditions and circumstances which are peculiar to the above described variance request.

Provide description of proposal: _____

Responsible Fiscal Authority Signature: _____ **Date:** _____

(Please include all support documentation - Note that follow up documentation may be required to process this variance)

Committee Reviewers:

Department of Public Safety (PS):

Assistant Vice President Approve _____ Disapprove** _____ Signature _____

Director of Security and Protective Services Approve _____ Disapprove** _____ Signature _____

Facilities Operations and Development:

Lock Shop Manager Approve _____ Disapprove** _____ Signature _____

Manager, Key/Card Control Center Approve _____ Disapprove** _____ Signature _____

Safety Engineer, EHS Approve _____ Disapprove** _____ Signature _____

Project Manager, FDC Approve _____ Disapprove** _____ Signature _____

Variance request is Approved _____ is Denied _____

Authorization Signature: _____ **Date:** _____

Senior Director, FDC

* Send original variance application to project's Project Manager for routing of document.

** If disapproved, reviewer shall attach their documentation & reasons for disapproval.

END OF APPENDIX Y