Western Michigan University Security System Design Policy

Western Michigan University in its endeavor to maintain safety and security for students, faculty and staff on campus has developed this Security System Design Policy for new construction and renovation projects on University property.

This Design Guideline shall apply to all new construction and renovation projects from this date forward by the University and its contracted Professionals. Deviations from this standard require Vice President Business and Finance written approval (see Appendix A).

Lowell P. Rinker
Vice President Business and Finance and CFO
Western Michigan University

Effective Date

Table of Contents

PART 1 – GENERAL GUIDELINES 1
PART 2 – DESIGN PROCESS 2
PART 3 – DESIGN 2
  3.1 - IMPLEMENTATION CONCEPTS 2
  3.2 - APPLICATIONS 3
PART 4 – UNIVERSITY PROVIDED SERVICES 4
APPENDIX A: SECURITY GUIDELINE DEVIATION WAIVER 5

PART 1 – GENERAL GUIDELINES

At Western Michigan University security and protection for Students, Faculty and Staff is a high priority. Additionally with the advent of technology in classrooms and other areas of University buildings, property loss is a problem. The following is a summary of how the University is implementing security on campus. The ultimate goal for the University is to protect people; but in addition the University strives to protect its property and minimize the disruption of University operations.

The following guidelines have been established to meet safety and security practices for the properties of Western Michigan University and are applicable to all new construction and renovation projects on University property. All projects will be reviewed by the Security Design Team and a recommendation made to the Vice President for Business and Finance and CFO for acceptance. Security then becomes part of the project budget, planning and design.
Professional Service Contractors engaged in projects for the University shall follow, specify and include, the requirements and practices identified in this Guideline in accordance with their Professional Services Agreement with the University.

PART 2 – DESIGN PROCESS

The University, because of liability issues, assumes the responsibility of design and detailing of the security systems on campus. The University Security Committee through the office of Facility Management – Engineering Division will provide the security design for any renovation projects and all new projects.

The following process will be followed to identify the required security and design. This will be accomplished by a Security Design Committee, consisting of Public Safety representatives, Facility Management – Engineering Division representatives, and project design team members.

A. During the Design Development phase of the project and once the project spaces are established and agreed upon, a review of the design with security/access as a priority will be conducted. As the design develops the operation of the building, the lighting around the building, the location, type and number of doors will be reviewed for security issues. Security perimeters will be identified and the penetrations through these perimeters resolved. A security design project will be established and funded from the project budget.

B. A meeting with the building occupants/users and security design committee will then establish how the spaces are expected to be used, and identify any equipment or space issues that would affect access to spaces. At this time perimeters of security around and in the building would be established. Levels of security for the zones and perimeters would be established, as well as any desired spaces that need extra security, such as chemicals, laptop storage, and/or special equipment. In addition the team would also identify the equipment and systems to be used for security, including door hardware etc.

C. Following that meeting the security committee would then draft the security specifications and mark up the drawings for inclusion into the project documents. Any deviations from University accepted practices, such as reductions in security levels, or special applications would then be presented to the Vice President for Business and Finance and CFO for acceptance.

D. During Construction, Facilities Management – Engineering Division and Public Safety will monitor the installation.

E. Upon the completion of the installation the Security Design Committee will walk down the system and commission it.

PART 3 – DESIGN

The design of security systems, at the University, is intended to protect people first and then equipment. These protection designs always try to balance the inconvenience of security with the protection of people, property and functional operations. Equipment will be monitored by network connections, locks, and or patrols. In addition, video surveillance, following the Security Camera Policies and Procedures, will be utilized where needed. Designs and implementation also must meet Life Safety Code requirements for safe egress of occupants from the areas protected.

3.1 IMPLEMENTATION CONCEPTS

The best way to protect equipment or an area is to make someone responsible for the equipment or area. This is not always practical in our University environment, but is attempted. Technology
today is ever changing and the equipment used in the University’s security systems are no different. Western Michigan University, has defined various levels of security based on values of equipment installed and possible liabilities.

Intrusion alarm systems are intended to monitor spaces and equipment and detect intruders during unoccupied times. Various methods will be utilized as practical, such as door contacts, motion sensors, glass break sensors, etc. Occupants of the spaces will be required to “turn off the alarm” when the spaces are occupied, and “turn it on” when finished using the space. Occupants will utilize the card reader key pads to accomplish this.

The University Access Control System provides better control over access to a building and faster updating of the access to a building. Building coordinators will have the responsibility of maintaining the access database for their building. Access Control to a University Building includes card readers at primary entrances, motion sensors, video surveillance of exits, door switches, and delayed egress at emergency exits. This system tracks anyone entering the building, and allows the utilization of schedules for opening the building for “normal” occupancy. Special requirements for interior spaces may also be included on this system, such as office suites, special labs, or storage spaces.

The general levels of security equipment application will be established considering the following:

A. Key Access level utilizes our key and lock system with no information provided to Public Safety.

B. Alarm Only level provides intrusion detection and door position, with an alarm sent to Public Safety when the zone has been violated.

C. Video Surveillance level provides visual monitoring and recording of the area. This may or may not be in addition to Alarm Only, or Access Control levels.

D. Access Control level utilizes the card access system to control access, monitors the previous levels, Information Generating Levels: - monitored by Police station, access levels administered by building coordinator, Electronic Locked Doors

E. Access Control with video surveillance of the space.

F. Access Control with Video Surveillance and motion monitoring within the space. The system utilizes the keypad on the card reader to turn the monitoring on and off.

3.2 - APPLICATIONS

Security Perimeters or zones will be established based on the following guidelines:

Exterior Wall Perimeter: This typically consists of the building exterior walls, windows and doors. All penetrations or openings through this perimeter requires controlled access, and monitoring, including video surveillance.

Operational Areas: This typically consists of areas within the building that need to have access controlled differently then other areas. Security equipment may include card access to spaces, video surveillance and motion detection. Examples are office suites, maintenance spaces, public areas, computer labs etc.

Special Function Areas: These are areas that require special security because of the function in the area. Security equipment will be determined based on the need and application. Examples of these would be chemical storage room, computer labs, cash operations, computer server rooms etc.
Security Equipment required for these areas will be established by the Security Design Team based on best practices, and proven methods developed in other projects. Table 1 identifies the types of zones, zone security and minimum general security equipment requirements.

**TABLE 1 - TYPICAL SECURITY APPLICATIONS**

<table>
<thead>
<tr>
<th>Zones/Levels</th>
<th>Description of Zone/Level Security</th>
<th>Security Equipment Required for the Zone/Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Building Perimeter</td>
<td>Controlled access and egress scheduling during normal business hours. Limit entrance to the building through one entrance only and exiting of the building during off hours to as few as possible doors preferably the same as entrance. Video monitor all exits from the building all the time.</td>
<td>Card access at doors on each face of the building, and electric strikes at the entrances used to open during class hours and lock the doors during scheduled hours. Video monitoring of all exit paths of the building. Stairwell exits are limited to emergency exit only.</td>
</tr>
<tr>
<td>Office Suites</td>
<td>Controlled access to suites through only one entrance. Schedule control of the other exits for office hours of the suite.</td>
<td>Card access at main entrance and door strikes and alarms at other exits. Schedule door times.</td>
</tr>
<tr>
<td>Computer Server Rooms</td>
<td>Security System Controlled access to the room through only one entrance, all the time. Other exits monitored and alarmed.</td>
<td>Card access at main entrance and door alarms at the other exit.</td>
</tr>
<tr>
<td>Computer Labs</td>
<td>Controlled access to the space and video surveillance of equipment.</td>
<td>Card access on the main entrance and alarms on the other exits. Video monitoring of activities in the room.</td>
</tr>
<tr>
<td>Level “1 &amp; 2” Classrooms</td>
<td>Controlled access to classrooms.</td>
<td>Wireless Card access to entrances. Classroom unlocked for duration of class.</td>
</tr>
<tr>
<td>Level “3, &amp; 4” Classrooms</td>
<td>Control access, video surveillance, motion sensors, and alarm other entrances and exits.</td>
<td>Card Access with PIN pad at the main entrance to the room. PIN code will activate and deactivate the motion sensors in the room. Video monitoring of activities and all exits. Other exits will be unlocked by the PIN code process.</td>
</tr>
<tr>
<td>Cash Operation Areas</td>
<td>Video Surveillance, and duress buttons</td>
<td>Video Cameras surveying the operations, and duress buttons as needed.</td>
</tr>
<tr>
<td>Special Equipment Rooms</td>
<td>As necessary for the contents of the room.</td>
<td></td>
</tr>
<tr>
<td>Maintenance Areas</td>
<td>Control access to spaces</td>
<td>Card Access and door alarms on equipment access doors.</td>
</tr>
</tbody>
</table>

**PART 4 – UNIVERSITY PROVIDED SERVICES**

The Security Committee will provide the security specifications in MS Word format for the project. Standard door details will be provided in Autocad format for the Design Team’s use. In addition markups of the project floor plans indicating the security for the project will be provided. The Security Committee will also provide a "Security Schedule" indicating security for doors and areas of the building. This "Security Schedule" should be included in the specifications. No deviations or changes are to be made without written approval of the University’s Security Committee.
APPENDIX A: SECURITY GUIDELINE DEVIATION WAIVER

DATE: ___________________________  PROJECT NO.: ___________________________

PROJECT ORIGINATOR: ___________________________________________________________

BUILDING # OR LOCATION: _______________________________________________________

DESCRIPTION OF LOCATION: _______________________________________________________

______________________________________________________________________________

DESCRIPTION OF NORMALLY REQUIRED SECURITY BY THIS POLICY:

______________________________________________________________________________

______________________________________________________________________________

DESCRIPTION OF DEVIATION FROM SECURITY POLICY:

______________________________________________________________________________

______________________________________________________________________________

______________________________________________________________________________

REASON FOR DEVIATION:

______________________________________________________________________________

______________________________________________________________________________

RESOLUTION OF ACTIONS:

______________________________________________________________________________

______________________________________________________________________________

FUNDING FOR DEVIATION: _______________________________________________________

SIGNATURE/DATE:

______________________________________________________________________________

Vice President for Business and Finance
and CFO

Date

Admin_Policy_Standard DG-28-0
Campus Security Policy __2010.doc  5
Rev: 3/8/2010
Printed: 3/9/2010
END OF GUIDELINE