

Facility Management: Building Security Access Control Measures

Contributed by Richard Grassie, CPP, and Behrooz (Ben) Emam, AIA, PE, CFM

Revised February 2007

The AIA collects and disseminates Best Practices as a service to AIA members without endorsement or recommendation. Appropriate use of the information provided is the responsibility of the reader.

SUMMARY

Building managers execute access control measures to specific facilities. Each building has its own set of challenges and security solutions. Access control measures that building managers may employ are included.

ACCESS CONTROL

The term *access control* generally refers to physical or behavioral measures for managing the passage of personnel and vehicles into, out of, and within a facility. An access control plan strives to exert sufficient control to protect a facility while still allowing employees enough freedom of movement to work effectively.

Access control typically consists of electronic and/or physical control processes. A mix of technology and passive barriers can secure a site perimeter. Once this is accomplished, the next step is to control access to building interiors without disrupting facility functions and activities. Perimeter security keeps unwanted individuals out. Inside the building, access control can address concerns about internal theft and limit the movement of both employees and visitors. Each building presents different challenges and requires a unique set of security solutions.

ACCESS CONTROL MEASURES

Building managers may use the following operational measures to control access into, within, and out of a given building or site:

- Post “No Trespassing” and “Authorized Access Only” signs, along with signs stating that vehicles and visitors are subject to search.
- Assign responsibility for security to someone on staff—the facility manager or security manager—to allow for an orderly implementation of security access measures and procedures and subsequent daily monitoring.
- Train all organization and affiliate agency staff in basic security methods and procedures unique to the facility.
- Ensure that security awareness and procedures become routine for all building occupants, including the lobby security staff and the organization’s tenants, employees, and visitors.
- Monitor performance of security duties such as the control of building entrances; regulation and monitoring of lobby pedestrian traffic; patrol and checks of the building and perimeter before closing and upon opening; inspection of incoming material and personnel; safety inspection of facilities and resources; and, in conjunction with the facility manager, appropriate response to special situations and security activities.
- Distribute a simple, straightforward security policy statement, prepared by the organization’s senior management to inform all employees and tenants that security is a shared responsibility and serves as the foundation for issuance of security procedures.
- Develop and distribute a handbook of the organization’s security policies and procedures, to be used primarily by guard and facility management personnel to respond to specific security events and emergencies in and around the building. The portion of the manual applicable to employees should be distributed to them with the general policy statement.
- Develop procedures to be followed for building evacuation, fire evacuation, civil disturbance, and power failure in the event of a natural or artificial disaster.
- Develop provisions concerning release of public information, availability of medical aid, emergency shutdown and restoration procedures, evacuation plans, and ways to regularly test and refine the disaster response and recovery plan.

- Use natural surveillance by arranging reception, production, and office space for easy observation of unescorted visitors.
- Restrict all visitors to building lobbies unless escorted by an authorized employee or tenant.
- Keep publicly accessible restroom doors locked, and establish a formal key control system using hardware of recognized quality. When combination locks are used, authorized employees should unlock doors for visitors.
- Keep closets, boiler rooms, and utility rooms locked at all times.
- Require all visitors to sign a visitor log and to be escorted at all times.
- Require material or equipment receipts for any material leaving the building, especially for electronic equipment such as laptop computers.
- Pay close attention to access control at loading and unloading areas.
- Institute a system of employee and contractor ID badges, and train employees to challenge persons who are not wearing badges.
- Establish a system for determining which cars, trucks, and other vehicles may enter the site; which gates, docks, or other entrances they may use; and under what conditions.
- Institute parcel inspections using magnetometers, X-ray screening, or devices to detect explosives.

ABOUT THE CONTRIBUTORS

Richard P. Grassie, CPP, is president of TECHMARK Security Integration Inc., a Boston-based firm providing security design and technology integration services. Grassie has served as a consultant to Fortune 500, institutional, and government clients in the United States and abroad. He is a board member of the International Association of Security Consultants and is past chair of the American Society of Industrial Security (ASIS) Security Architecture and Engineering Council. He has written numerous articles and conducts workshops and training seminars on security for public agencies and private industry.

Behrooz (Ben) Emam, AIA, PE, CFM, is senior manager for global facilities planning and engineering at Amazon.com. A registered architect, professional civil engineer, and certified facility manager, Emam has extensive experience in architecture and structural engineering; facility

design, construction, and project management; and emergency preparedness. He regularly teaches classes in construction and facility management and conducts seminars on seismic preparedness and disaster planning.

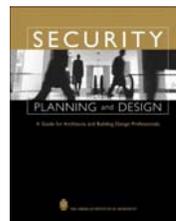
RESOURCES

More Best Practices

The following AIA Best Practices provide additional information related to this topic:

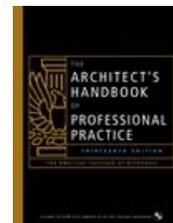
- 03.01.02 Becoming a Certified Protection Professional
- 11.10.01 Understanding Human Behavior Leads to Safer Environments
- 11.08.05 Facility Management: Operational Security Factors

For More Information on This Topic



This article is excerpted and adapted from *Security Planning and Design: A Guide for Architects and Building Design Professionals*, by the American Institute of Architects.

See also “Security Evaluation and Planning,” by Marco A. Monsalve and James R. Sutton, *The Architect’s Handbook of Professional Practice Update 2003*.



See also the 14th edition of the *Handbook*, which can be ordered from the AIA Bookstore by calling 800-242-3837 (option 4) or by email at bookstore@aia.org.



Feedback

The AIA welcomes member feedback on Best Practice articles. To provide feedback on this article, please contact bestpractices@aia.org.

Key Terms

- Building performance
- Use design
- Security