

A S I S I N T E R N A T I O N A L

Facilities Physical Security Measures

ASIS GDL FPSM-2009

GUIDELINE



ASIS GDL FPSM-2009

an ASIS Guideline for Security

Facilities Physical Security Measures Guideline

Safety Act Designation

In April 2005, the U.S. Department of Homeland Security (DHS) awarded ASIS International a Designation for its Guidelines Program under the SAFETY Act (Support Anti-Terrorism by Fostering Effective Technology Act of 2002). This Designation is significant in three ways: (1) it establishes that ASIS standards and guidelines are qualified to be a “technology” that could reduce the risks or effects of terrorism, (2) it limits ASIS’ liability for acts arising out of the use of the standards and guidelines in connection with an act of terrorism, and (3) it precludes claims of third party damages against organizations using the standards and guidelines as a means to prevent or limit the scope of terrorist acts.

Approved June 8, 2009

ASIS International

Abstract

This guideline assists in the identification of physical security measures that can be applied at facilities to safeguard or protect an organization’s assets—people, property, and information.

ASIS GDL FPSM-2009

NOTICE AND DISCLAIMER

The information in this publication was considered technically sound by the consensus of those who engaged in the development and approval of the document at the time of its creation. Consensus does not necessarily mean that there is unanimous agreement among the participants in the development of this document.

ASIS International standards and guideline publications, of which the document contained herein is one, are developed through a voluntary consensus standards development process. This process brings together volunteers and/or seeks out the views of persons who have an interest and knowledge in the topic covered by this publication. While ASIS administers the process and establishes rules to promote fairness in the development of consensus, it does not write the document and it does not independently test, evaluate, or verify the accuracy or completeness of any information or the soundness of any judgments contained in its standards and guideline publications.

ASIS is a volunteer, nonprofit professional society with no regulatory, licensing or enforcement power over its members or anyone else. ASIS does not accept or undertake a duty to any third party because it does not have the authority to enforce compliance with its standards or guidelines. It assumes no duty of care to the general public, because its works are not obligatory and because it does not monitor the use of them.

ASIS disclaims liability for any personal injury, property, or other damages of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, application, or reliance on this document. ASIS disclaims and makes no guaranty or warranty, expressed or implied, as to the accuracy or completeness of any information published herein, and disclaims and makes no warranty that the information in this document will fulfill any person's or entity's particular purposes or needs. ASIS does not undertake to guarantee the performance of any individual manufacturer or seller's products or services by virtue of this standard or guide.

In publishing and making this document available, ASIS is not undertaking to render professional or other services for or on behalf of any person or entity, nor is ASIS undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances. Information and other standards on the topic covered by this publication may be available from other sources, which the user may wish to consult for additional views or information not covered by this publication.

ASIS has no power, nor does it undertake to police or enforce compliance with the contents of this document. ASIS has no control over which of its standards, if any, may be adopted by governmental regulatory agencies, or over any activity or conduct that purports to conform to its standards. ASIS does not list, certify, test, inspect, or approve any practices, products, materials, designs, or installations for compliance with its standards. It merely publishes standards to be used as guidelines that third parties may or may not choose to adopt, modify or reject. Any certification or other statement of compliance with any information in this document shall not be attributable to ASIS and is solely the responsibility of the certifier or maker of the statement.

All rights reserved. Permission is hereby granted to individual users to download this document for their own personal use, with acknowledgement of ASIS International as the source. However, this document may not be downloaded for further copying or reproduction nor may it be sold, offered for sale, or otherwise used commercially.

Copyright © 2009 by ASIS International

ISBN 978-1-887056-95-3

ASIS GDL FPSM-2009

FOREWORD

The information contained in this Foreword is not part of this ASIS International Guideline and has not been processed in accordance with ASIS' requirements for a Guideline. As such, this Foreword may contain material that has not been subjected to public review or a consensus process. In addition, it does not contain requirements necessary for conformance to the Guideline.

ASIS International (ASIS) is the preeminent organization for security professionals, with more than 37,000 members worldwide. ASIS is dedicated to increasing the effectiveness and productivity of security professionals by developing educational programs and materials that address broad security interests, such as the ASIS Annual Seminar and Exhibits, as well as specific security topics. ASIS also advocates the role and value of the security management profession to business, the media, government entities, and the public. By providing members and the security community with access to a full range of programs and services, and by publishing the industry's No. 1 magazine—*Security Management*—ASIS leads the way for advanced and improved security performance.

The work of preparing ASIS Standards and Guidelines is carried out through the ASIS International Standards and Guidelines Commission and its committees. The Mission of the ASIS Standards and Guidelines Commission is *to advance the practice of security management through the development of standards and guidelines within a voluntary, nonproprietary, and consensus-based process, utilizing to the fullest extent possible the knowledge, experience, and expertise of ASIS membership, security professionals, and the global security industry.*

Suggestions for improvement of this document are welcome. They should be sent to ASIS International, 1625 Prince Street, Alexandria, VA 22314-2818, USA.

Commission Members

Jason L. Brown, Thales Australia

Steven K. Bucklin, Glenbrook Security Services, Inc.

John C. Cholewa III, CPP, Embarq Corporation

Cynthia P. Conlon, CPP, Conlon Consulting Corporation

Michael A. Crane, CPP, IPC International Corporation

Eugene F. Ferraro, CPP, PCI, CFE, Business Controls Inc.

F. Mark Geraci, CPP, Purdue Pharma L.P., Chair

Robert W. Jones, Kraft Foods, Inc.

Michael E. Knoke, CPP, Express Scripts, Inc., Vice Chair

John F. Mallon, CPP

Marc H. Siegel, Ph.D., Commissioner, ASIS Global Standards Initiative

Roger D. Warwick, CPP, Pyramid International

ASIS GDL FPSM-2009

At the time it approved this document, FPSM Guidelines Committee, which is responsible for the development of this Guideline, had the following members:

Committee Members

Committee Chairman: Geoffrey T. Craighead, CPP, Securitas Security Services USA, Inc.

Commission Liaison: Robert W. Jones, Kraft Foods, Inc.

Committee Secretariat: Sue Carioti, ASIS International

Sean A. Ahrens, CPP, Schirmer Engineering an Aon Global company
Randy I. Atlas, Ph.D., AIA, CPP, Counter Terror Design, Inc.
Daniel E. Bierman, CPP, PSP, Whitman Requardt & Associates
Elliot A. Boxerbaum, CPP, Security/Risk Management Consultants, Inc.
Ross D. Bulla, CPP, PSP, The Treadstone Group, Inc.
Nick Catrantzos, CPP, Metropolitan Water District of Southern California
Thomas Connolly, Red Hawk, a UTC Fire & Security Co.
Frederick J. Coppel, CPP, SAIC/DTRA/CXC
Joseph A. DiDona, The Reader's Digest Association, Inc.
Jack F. Dowling, CPP, PSP, JD Security Consultants, LLC
David R. Duda, PE, CPP, PSP, Newcomb & Boyd
Mary Lynn Garcia, CPP, Sandia National Laboratories
Ronald L. Martin, CPP, US Dept. of Health & Human Services
William J. Moore, PSP, Jacobs Global Buildings Group-North America
Patrick M. Murphy, CPP, PSP, Marriott International, Inc.
Robert L. Pearson, PE, The Protectorate Corporation
Thomas J. Rohr Sr., CPP, Carestream Health, Inc.
Steve Surfaro, Axis Communications
Paul P. Yung, Ph.D., Deloitte Touche Tohmatsu

Revision History

Baseline document.

Guideline Designation

This guideline is designated as ASIS GDL FPSM-2009.

Keywords

Access Control, Alarm System, Asset, Barrier, Camera, Crime Prevention Through Environmental Design (CPTED), Facility, Intrusion Detection, Lighting, Lock, Perimeter Protection, Physical Security, Physical Security Measure, Policy, Procedure, Security Manager, Risk Management, Security Officer, Site Hardening, Video Surveillance.

ASIS GDL FPSM-2009

TABLE OF CONTENTS

1. SCOPE, SUMMARY, AND PURPOSE.....	1
1.1 SCOPE.....	1
1.2 SUMMARY	1
1.3 PURPOSE	1
2. TERMS AND DEFINITIONS	2
3. RECOMMENDED PRACTICE ADVISORY	4
3.1 CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN (CPTED)	5
3.1.1 <i>Background</i>	5
3.1.2 <i>Strategies</i>	6
3.1.2.1 <i>Outer Layer</i>	9
3.1.2.2 <i>Middle Layer</i>	9
3.1.2.3 <i>Inner Layers</i>	9
3.2 PHYSICAL BARRIERS AND SITE HARDENING	10
3.2.1 <i>Physical Barriers</i>	10
3.2.1.1 <i>Fences and Walls</i>	10
3.2.1.1.1 <i>Walls</i>	11
3.2.1.1.2 <i>Chain-Link Fences</i>	11
3.2.1.1.3 <i>Expanded Metal and Welded Wire Fabric Fences</i>	12
3.2.1.1.4 <i>Ornamental Fences</i>	12
3.2.1.1.5 <i>Barbed Wire</i>	12
3.2.1.1.6 <i>Razor or Concertina Wire</i>	12
3.2.1.1.7 <i>Concrete Fences</i>	12
3.2.1.1.8 <i>Wooden Fences</i>	13
3.2.1.1.9 <i>Electric Security Fencing</i>	13
3.2.1.2 <i>Planters, Bollards, Concrete Barriers, and Steel Barricades</i>	13
3.2.1.3 <i>Premises Openings</i>	14
3.2.1.3.1 <i>Gates</i>	14
3.2.1.3.2 <i>Turnstiles</i>	14
3.2.1.3.3 <i>Doors</i>	14
3.2.1.3.4 <i>Windows</i>	15
3.2.1.3.5 <i>Other Openings</i>	16
3.2.1.4 <i>Locks</i>	16
3.2.2 <i>Site Hardening</i>	16
3.3 PHYSICAL ENTRY AND ACCESS CONTROL	17
3.3.1 <i>Access Control Barriers</i>	18
3.3.2 <i>Electronic Access Control Systems</i>	18
3.3.3 <i>Personnel Access Control</i>	19
3.3.4 <i>Locks</i>	19
3.3.4.1 <i>Mechanical Locks</i>	19
3.3.4.2 <i>Electrified Locks</i>	19
3.3.4.3 <i>Electromagnetic Locks</i>	19
3.3.4.4 <i>Credential-Operated Locks</i>	20
3.3.4.5 <i>Combination Locks</i>	20
3.3.4.6 <i>Biometric Locks</i>	20
3.3.4.7 <i>Rapid Entry Systems</i>	20
3.3.4.8 <i>Key System</i>	20
3.3.5 <i>Contraband Detection</i>	21
3.3.6 <i>Vehicle Access Control</i>	21
3.3.7 <i>Procedures and Controls</i>	21

ASIS GDL FPSM-2009

3.4	SECURITY LIGHTING	22
3.4.1	<i>Applications</i>	23
3.4.2	<i>Intensity</i>	23
3.4.3	<i>Equipment</i>	24
3.5	INTRUSION DETECTION SYSTEMS	25
3.5.1	<i>Intrusion Detection System Devices</i>	26
3.5.2	<i>Alarm Transmission, Monitoring, and Notification</i>	27
3.5.3	<i>Installation, Maintenance, and Repair</i>	27
3.6	VIDEO SURVEILLANCE.....	28
3.6.1	<i>Functional Requirements</i>	28
3.6.1.1	<i>Camera Functional Requirements</i>	29
3.6.1.2	<i>Monitoring Functional Requirements</i>	29
3.6.1.3	<i>Recording Functional Requirements</i>	30
3.6.2	<i>Cameras</i>	30
3.6.2.1	<i>Lighting</i>	30
3.6.2.2	<i>Lens Selection</i>	31
3.6.2.3	<i>Camera Types</i>	31
3.6.2.4	<i>Power and Enclosures</i>	31
3.6.3	<i>Transport Medium</i>	32
3.6.4	<i>Command Center</i>	32
3.6.5	<i>Recording</i>	32
3.6.6	<i>Maintenance</i>	33
3.7	SECURITY PERSONNEL	33
3.7.1	<i>Security Managers</i>	33
3.7.2	<i>Security Officers</i>	34
3.7.2.1	<i>Organization</i>	34
3.7.2.2	<i>Responsibilities</i>	35
3.7.2.3	<i>Preemployment Screening</i>	35
3.7.2.4	<i>Training</i>	36
3.7.2.5	<i>Equipment</i>	36
3.7.3	<i>Other Employees</i>	37
3.8	SECURITY POLICIES AND PROCEDURES	37
3.8.1	<i>Policies</i>	38
3.8.1.1	<i>Subjects to Address</i>	38
3.8.2	<i>Procedures</i>	39
3.8.2.1	<i>Subjects to Address</i>	39
3.9	SECURITY CONVERGENCE	40
A	BIBLIOGRAPHY	41

TABLE OF FIGURES

FIGURE 1:	LAYERS OF SECURITY	8
-----------	--------------------------	---

an ASIS Guideline for Security –

Facilities Physical Security Measures Guideline

1. SCOPE, SUMMARY, AND PURPOSE

1.1 Scope

This *Guideline* assists in the identification of physical security measures that can be applied at facilities to safeguard or protect an organization's assets—people, property, and information. It is not aimed at a specific occupancy, but facilities and buildings in general.

1.2 Summary

The *Guideline* outlines eight main categories of physical security measures used to protect facilities. These categories are:

1. Crime Prevention Through Environmental Design (CPTED),
2. Physical Barriers and Site Hardening,
3. Physical Entry and Access Control,
4. Security Lighting,
5. Intrusion Detection Systems,
6. Video Surveillance,
7. Security Personnel, and
8. Security Policies and Procedures.

In addition, the emerging field of security convergence is addressed.

1.3 Purpose

The purpose of this *Guideline* is to introduce readers, who may or may not have a security background, to the main types of physical security measures that can be applied to minimize the security risks at a facility.

To choose the right physical security measures and apply them appropriately, it is important to first conduct a risk assessment, such as described in the *ASIS General Security Risk Assessment Guideline*. The risk assessment, accompanied by an understanding of physical security measures provided by this guideline, makes it possible—either alone or with the help of security consultants or vendors—to select and implement appropriate physical security measures to reduce the assessed risks to a level acceptable by the organization.