NFPA®

730

Guide for Premises Security

2023

Documents
Document Sharing Hub
Copyright © NFPA. For exclusive use on NFPA Free Access platform. Not for distribution, downloading, or printing.
For inquiries contact custserv@nfpa.org. To report unauthorized use, contact legal@nfpa.org.
Full document details: NFPA 730 2023

NFPA® 730

Guide for Premises Security

2023 Edition

NFPA, 1 Batterymarch Park, Quincy, MA 02169-7471
An International Codes and Standards Organization

AVA Documents
Document Sharing Hub

Full document details: NFPA 730 2023

Documents
Document Sharing Hub

Full document details: NFPA 730 2023

IMPORTANT NOTICES AND DISCLAIMERS CONCERNING NFPA® STANDARDS

NFPA® codes, standards, recommended practices, and guides ("NFPA Standards"), of which the document contained herein is one, are developed through a consensus standards development process approved by the American National Standards Institute. This process brings together volunteers representing varied viewpoints and interests to achieve consensus on fire and other safety issues. While the NFPA administers the process and establishes rules to promote fairness in the development of consensus, it does not independently test, evaluate, or verify the accuracy of any information or the soundness of any judgments contained in NFPA Standards.

The NFPA 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, or reliance on NFPA Standards. The NFPA also makes no guaranty or warranty as to the accuracy or completeness of any information published herein.

In issuing and making NFPA Standards available, the NFPA is not undertaking to render professional or other services for or on behalf of any person or entity. Nor is the NFPA 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.

The NFPA has no power, nor does it undertake, to police or enforce compliance with the contents of NFPA Standards. Nor does the NFPA list, certify, test, or inspect products, designs, or installations for compliance with this document. Any certification or other statement of compliance with the requirements of this document shall not be attributable to the NFPA and is solely the responsibility of the certifier or maker of the statement.

REVISION SYMBOLS IDENTIFYING CHANGES FROM THE PREVIOUS EDITION

Text revisions are shaded. A Δ before a section number indicates that words within that section were deleted and a Δ to the left of a table or figure number indicates a revision to an existing table or figure. When a chapter was heavily revised, the entire chapter is marked throughout with the Δ symbol. Where one or more sections were deleted, a • is placed between the remaining sections. Chapters, annexes, sections, figures, and tables that are new are indicated with an *N*.

Note that these indicators are a guide. Rearrangement of sections may not be captured in the markup, but users can view complete revision details in the First and Second Draft Reports located in the archived revision information section of each code at www.nfpa.org/docinfo. Any subsequent changes from the NFPA Technical Meeting, Tentative Interim Amendments, and Errata are also located there.

REMINDER: UPDATING OF NFPA STANDARDS

Users of NFPA codes, standards, recommended practices, and guides ("NFPA Standards") should be aware that these documents may be superseded at any time by the issuance of a new edition, may be amended with the issuance of Tentative Interim Amendments (TIAs), or be corrected by Errata. It is intended that through regular revisions and amendments, participants in the NFPA standards development process consider the then-current and available information on incidents, materials, technologies, innovations, and methods as these develop over time and that NFPA Standards reflect this consideration. Therefore, any previous edition of this document no longer represents the current NFPA Standard on the subject matter addressed. NFPA encourages the use of the most current edition of any NFPA Standard [as it may be amended by TIA(s) or Errata] to take advantage of current experience and understanding. An official NFPA Standard at any point in time consists of the current edition of the document, including any issued TIAs and Errata then in effect.

To determine whether an NFPA Standard has been amended through the issuance of TIAs or corrected by Errata, visit the "Codes & Standards" section at www.nfpa.org.

ISBN: 978-145592990-0 (Print)

AVA Documents
Document Sharing Hub

Full document details: NFPA 730 2023

ADDITIONAL IMPORTANT NOTICES AND DISCLAIMERS CONCERNING NFPA® STANDARDS

Updating of NFPA Standards

Users of NFPA codes, standards, recommended practices, and guides ("NFPA Standards") should be aware that these documents may be superseded at any time by the issuance of a new edition, may be amended with the issuance of Tentative Interim Amendments (TIAs), or be corrected by Errata. It is intended that through regular revisions and amendments, participants in the NFPA standards development process consider the then-current and available information on incidents, materials, technologies, innovations, and methods as these develop over time and that NFPA Standards reflect this consideration. Therefore, any previous edition of this document no longer represents the current NFPA Standard on the subject matter addressed. NFPA encourages the use of the most current edition of any NFPA Standard [as it may be amended by TIA(s) or Errata] to take advantage of current experience and understanding. An official NFPA Standard at any point in time consists of the current edition of the document, including any issued TIAs and Errata then in effect.

To determine whether an NFPA Standard has been amended through the issuance of TIAs or corrected by Errata, visit the "Codes & Standards" section at www.nfpa.org.

Interpretations of NFPA Standards

A statement, written or oral, that is not processed in accordance with Section 6 of the Regulations Governing the Development of NFPA Standards shall not be considered the official position of NFPA or any of its Committees and shall not be considered to be, nor be relied upon as, a Formal Interpretation.

Patents

The NFPA does not take any position with respect to the validity of any patent rights referenced in, related to, or asserted in connection with an NFPA Standard. The users of NFPA Standards bear the sole responsibility for determining the validity of any such patent rights, as well as the risk of infringement of such rights, and the NFPA disclaims liability for the infringement of any patent resulting from the use of or reliance on NFPA Standards.

NFPA adheres to the policy of the American National Standards Institute (ANSI) regarding the inclusion of patents in American National Standards ("the ANSI Patent Policy"), and hereby gives the following notice pursuant to that policy:

NOTICE: The user's attention is called to the possibility that compliance with an NFPA Standard may require use of an invention covered by patent rights. NFPA takes no position as to the validity of any such patent rights or as to whether such patent rights constitute or include essential patent claims under the ANSI Patent Policy. If, in connection with the ANSI Patent Policy, a patent holder has filed a statement of willingness to grant licenses under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license, copies of such filed statements can be obtained, on request, from NFPA. For further information, contact the NFPA at the address listed below.

Law and Regulations

Users of NFPA Standards should consult applicable federal, state, and local laws and regulations. NFPA does not, by the publication of its codes, standards, recommended practices, and guides, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

NFPA Standards are copyrighted. They are made available for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of safe practices and methods. By making these documents available for use and adoption by public authorities and private users, the NFPA does not waive any rights in copyright to these documents.

Use of NFPA Standards for regulatory purposes should be accomplished through adoption by reference. The term "adoption by reference" means the citing of title, edition, and publishing information only. Any deletions, additions, and changes desired by the adopting authority should be noted separately in the adopting instrument. In order to assist NFPA in following the uses made of its documents, adopting authorities are requested to notify the NFPA (Attention: Secretary, Standards Council) in writing of such use. For technical assistance and questions concerning adoption of NFPA Standards, contact NFPA at the address below.

For Further Information

All questions or other communications relating to NFPA Standards and all requests for information on NFPA procedures governing its codes and standards development process, including information on the procedures for requesting Formal Interpretations, for proposing Tentative Interim Amendments, and for proposing revisions to NFPA standards during regular revision cycles, should be sent to NFPA headquarters, addressed to the attention of the Secretary, Standards Council, NFPA, 1 Batterymarch Park, P.O. Box 9101, Quincy, MA 02269-9101; email: stds_admin@nfpa.org.

For more information about NFPA, visit the NFPA website at www.nfpa.org. All NFPA codes and standards can be viewed at no cost at www.nfpa.org/docinfo.

AVA Documents
Document Sharing Hub

Full document details: NFPA 730 2023

Copyright © 2022 National Fire Protection Association®. All Rights Reserved.

NFPA® 730

Guide for

Premises Security

2023 Edition

This edition of NFPA 730, *Guide for Premises Security,* was prepared by the Technical Committee on Premises Security. It was issued by the Standards Council on November 29, 2022, with an effective date of December 19, 2022, and supersedes all previous editions.

This edition of NFPA 730 was approved as an American National Standard on December 19, 2022.

Origin and Development of NFPA 730

The genesis of NFPA 730 was a request in 1994 to develop a burglary/security document. The project did not materialize until 2000, when the Standards Council appointed a committee to develop a premises security document. The committee responded by developing two documents, NFPA 731, *Standard for the Installation of Premises Security Systems,* and NFPA 730, *Guide for Premises Security.*

The 2006 edition of NFPA 730 included updated references and other minor modifications. The chapter on Industrial Facilities was modified to include requirements for key control measures, security operations, infrastructure protection, and a new section on water treatment facilities.

The 2008 edition of NFPA 730 was updated to add new requirements for industrial security. Specifically, new material was added for the protection of water treatment facilities. Other changes reflected corrections, updated references, and clarifications.

The 2011 edition updated many of the references. The guide also added more material on crime prevention through environmental design (CPTED). The majority of the other changes were editorial in nature.

The 2014 edition was revised to update many of the referenced publications. Section 4.3 was revised to clarify some of the requirements for security planning, including the prioritization of risks identified in the security vulnerability assessments (SVA) and the frequency of the SVA review and update. This edition also added a graph that could be used as a guide to sort the risks identified in the SVA. The responsibility for the SVA was also clarified and other changes relative to the qualifications of the SVA provider were addressed. Section 8.4 was revised to further detail both the need and criteria for protective lighting.

The major changes to the 2018 edition included the following:

(1) All the definitions in Chapter 3 were reviewed and correlated with those in NFPA 731, *Standard for the Installation of Premises Security Systems.*
(2) The term *key* was replaced by *key/credential* throughout the document to provide for more modern technology, such as access control cards and other means for unlocking or locking doors.
(3) Subsections 5.2.3 and 5.3.2 pertaining to security planning and SVAs were revised to recognize that there are comparable security risk assessment methodologies and to provide guidance for certification organizations on security or crime prevention.
(4) The terms *lockdown, lockout,* and *shelter-in-place* were added. Paragraph 11.1.3.2 pertaining to educational facilities, colleges, and universities was revised to provide for education and training for these conditions and to provide for semiannual security-related drills. Paragraph 11.2.1.3 was updated to address visitor identification and paragraph 11.3.4.6 was revised to provide criteria for exterior portal windows and sidelights.

The 2020 edition saw an alignment of definitions between NFPA 730 and NFPA 731, *Standard for the Installation of Premises Security Systems.* The definitions in Chapter 3 were reviewed and many revised to ensure consistency with those of NFPA 731. Definitions that were not used in NFPA 730

NFPA and National Fire Protection Association are registered trademarks of the National Fire Protection Association, Quincy, Massachusetts 02169.

AVA Documents Document Sharing Hub

Full document details: NFPA 730 2023

were deleted. The SI/metric conversions were reviewed throughout the document and many values were revised to ensure conversion accuracy.

To provide greater security, additional criteria were added pertaining to credentials for visitors entering a facility. The definition of *educational facility* was revised to provide clarity relative to the requirements for K–12 and college and university buildings. In addition, areas in the text were addressed to provide information relative to foliage, shrubbery, and trees close to buildings that could pose security risks. New criteria for network connectable products to address cybersecurity were also added.

The 2023 edition of NFPA 730 has updated references.

Documents
Document Sharing Hub
Full document details: NFPA 730 2023

Technical Committee on Premises Security

James P. Simpson, *Chair*
Electrical Training Alliance, MN [L]
Rep. International Brotherhood of Electrical Workers

Randall I. Atlas, Atlas Safety & Security Design, Inc., FL [IM]

Paul H. Aube, City Of Montreal, Canada [E]

Douglas P. Bassett, Xfinity Home, FL [IM]
Rep. Electronic Security Association

George Bish, Amazon/Ring Protect Inc., NC [M]

Louis Chavez, UL LLC, IL [RT]

David S. Collins, The Preview Group, Inc., OH [SE]
Rep. American Institute of Architects

Stephen B. Coppola, Vivint, MA [IM]
Rep. The Monitoring Association

David A. Dagenais, Partners/Wentworth-Douglass Hospital, NH [U]
Rep. NFPA Health Care Section

Dennis R. Elledge, De/SL LLC DBA CompSecure, MO [SE]

Lauris V. Freidenfelds, Telgian Engineering & Consulting, IL [SE]

Matthew Jakusz, ADT Commercial, FL [M]

Charles B. King, III, U.S. Department of Homeland Security, VA [E]

Scott Lord, Envision Technology Group, KS [U]
Rep. Partner Alliance for Safer Schools

Maria B. Marks, Siemens Industry, Inc., MD [M]

Anthony Mucci, Johnson Controls, FL [M]

James Murphy, Vector Security Inc., PA [IM]

Richard Jay Roberts, Honeywell Fire Safety, IL [M]
Rep. National Electrical Manufacturers Association

Robert H. Stagg, Self Employed, NC [SE]

Barry Stanford, AEG, CA [U]

Michael Tierney, Kellen Company, CT [M]
Rep. Builders Hardware Manufacturers Association

William F. Wayman, Jr., JENSEN HUGHES, MD [SE]

James M. Wenck, GHD, NC [SE]

Alternates

Shane M. Clary, Bay Alarm Company, CA [IM]
(Alt. to Stephen B. Coppola)

David Dressler, Minnesota Statewide Limited Energy JATC, MN [L]
(Alt. to James P. Simpson)

Mark A. Farus, Siemens Industry, Inc., GA [M]
(Alt. to Maria B. Marks)

Bruce E. Johnson, UL LLC, NY [RT]
(Alt. to Louis Chavez)

Douglas D. Quick, Sielox, LLC, GA [M]
(Alt. to Anthony Mucci)

Kurt A. Roeper, ASSA ABLOY, CT [M]
(Alt. to Michael Tierney)

John R. Schertel, Jr., Bosch Security Systems, LLC., NY [M]
(Alt. to Richard Jay Roberts)

Rick D. Sheets, AT&T Digital Life, TX [IM]
(Alt. to Douglas P. Bassett)

Chad Duffy, NFPA Staff Liaison

This list represents the membership at the time the Committee was balloted on the final text of this edition. Since that time, changes in the membership may have occurred. A key to classifications is found at the back of the document.

NOTE: Membership on a committee shall not in and of itself constitute an endorsement of the Association or any document developed by the committee on which the member serves.

Committee Scope: This Committee shall have primary responsibility for documents on the overall security program for the protection of premises, people, property, and information specific to a particular occupancy. The Committee shall have responsibility for the installation of premises security systems.

AVA Documents 2023 Edition Document Sharing Hub

Full document details: NFPA 730 2023

Contents

Chapter 1 Administration **730–** 6
1.1 Scope. **730–** 6
1.2 Purpose. **730–** 6
1.3 Application. **730–** 6
1.4 Retroactivity. **730–** 6
1.5 Equivalency. **730–** 6
1.6 Units and Formulas. **730–** 6

Chapter 2 Referenced Publications **730–** 6
2.1 General. **730–** 6
2.2 NFPA Publications. **730–** 6
2.3 Other Publications. **730–** 6
2.4 References for Extracts in Advisory Sections. **730–** 7

Chapter 3 Definitions **730–** 7
3.1 General. **730–** 7
3.2 NFPA Official Definitions. **730–** 7
3.3 General Definitions. **730–** 7

Chapter 4 General **730–** 9
4.1 Fundamental Principles. **730–** 9
4.2 Classification of Assets. **730–** 9
4.3 Security Planning. **730–** 9
4.4 Security Plan Evaluation. **730–** 10
4.5 System Design and Installation. **730–** 10
4.6 Maintenance. **730–** 10

Chapter 5 Security Planning **730–** 10
5.1 General. **730–** 10
5.2 Security Vulnerability Assessment (SVA). **730–** 10
5.3 Qualifications. **730–** 10
5.4 Security Plan. **730–** 10
5.5 Planning for Acts of Intimidation or Violence. . **730–** 11

Chapter 6 Administrative Controls **730–** 11
6.1 General. **730–** 11
6.2 People Management. **730–** 11
6.3 Material Receiving. **730–** 12
6.4 Information and Data Security. **730–** 12
6.5 Workplace Violence. **730–** 12

Chapter 7 Security Perimeters **730–** 12
7.1 General. **730–** 12
7.2 Area Designations. **730–** 13
7.3 Exterior Perimeters. **730–** 13
7.4 Interior Perimeters. **730–** 13
7.5 Portal Control. **730–** 13

Chapter 8 Crime Prevention Through Environmental Design **730–** 14
8.1 General. **730–** 14
8.2 Crime and Loss Prevention. (Reserved) **730–** 14
8.3 Human Behavior. (Reserved) **730–** 14
8.4 Lighting. **730–** 14
8.5 Landscaping. **730–** 14
8.6 Aesthetics. (Reserved) **730–** 14

Chapter 9 Security Systems **730–** 14
9.1 General. **730–** 14
9.2 Contraband Detection. (Reserved) **730–** 14
9.3 Personnel Safety Alerting Systems. (Reserved) . **730–** 14
9.4 Property Protection Monitoring Systems. **730–** 14
9.5 Security Monitoring. (Reserved) **730–** 15

Chapter 10 Accessory Property **730–** 15
10.1 General. **730–** 15
10.2 Parking. **730–** 15
10.3 Storage. (Reserved) **730–** 15
10.4 Exterior Areas. (Reserved) **730–** 15

Chapter 11 Educational Facilities, Colleges, and Universities **730–** 15
11.1 General. **730–** 15
11.2 Administrative Controls. **730–** 16
11.3 Security Perimeters. **730–** 16
11.4 Crime Prevention Through Environmental Design (CPTED). **730–** 17
11.5 Security Systems. **730–** 17
11.6 Accessory Property. **730–** 18

Chapter 12 Health Care **730–** 18
12.1 General. **730–** 18
12.2 Administrative Controls. **730–** 19
12.3 Security Perimeters. **730–** 19
12.4 Crime Prevention Through Environmental Design (CPTED). **730–** 20
12.5 Security Systems. **730–** 20

Chapter 13 Reserved **730–** 20

Chapter 14 Lodging **730–** 20
14.1 General. **730–** 20
14.2 Administrative Controls. **730–** 20
14.3 Security Perimeters. **730–** 21
14.4 Crime Prevention Through Environmental Design (CPTED). **730–** 21
14.5 Security Systems. **730–** 21
14.6 Accessory Property, Parking. **730–** 22

Chapter 15 Multi-Dwelling Unit Buildings **730–** 22
15.1 General. **730–** 22
15.2 Administrative Controls. **730–** 22
15.3 Security Perimeters. **730–** 22
15.4 Crime Prevention Through Environmental Design (CPTED). **730–** 23
15.5 Security Systems. **730–** 23
15.6 Accessory Property, Parking. **730–** 23

Chapter 16 Restaurants **730–** 23
16.1 General. **730–** 23
16.2 Administrative Controls. **730–** 23
16.3 Security Perimeters. **730–** 23
16.4 Crime Prevention Through Environmental Design (CPTED). **730–** 24
16.5 Security Systems. **730–** 24

Chapter 17 Shopping Centers **730–** 24
17.1 General. **730–** 24
17.2 Administrative Controls. **730–** 24
17.3 Security Perimeters. **730–** 24
17.4 Crime Prevention Through Environmental Design (CPTED). **730–** 24
17.5 Security Systems. **730–** 24
17.6 Accessory Property, Parking. **730–** 25

Chapter 18 Retail Establishments **730–** 25
18.1 General. **730–** 25
18.2 Administrative Controls. **730–** 25
18.3 Security Perimeters. **730–** 25
18.4 Crime Prevention Through Environmental Design (CPTED). **730–** 26
18.5 Security Systems. **730–** 26
18.6 Accessory Property, Parking. **730–** 26

AVA Documents
Document Sharing Hub
Full document details: NFPA 730 2023

Chapter 19 Office Buildings **730**– 26
19.1 General. **730**– 26
19.2 Administrative Controls. **730**– 26
19.3 Security Perimeters. **730**– 27
19.4 Crime Prevention Through Environmental Design (CPTED). (Reserved) **730**– 27
19.5 Security Systems. **730**– 27
19.6 Accessory Property, Parking. **730**– 27

Chapter 20 Industrial Facilities **730**– 27
20.1 General. **730**– 27
20.2 Administrative Controls. **730**– 28
20.3 Security Perimeters. **730**– 28
20.4 Crime Prevention Through Environmental Design (CPTED). (Reserved) **730**– 28
20.5 Security Systems. **730**– 28
20.6 Accessory Property, Parking. **730**– 28

Annex A Explanatory Material **730**– 28
Annex B Homeland Security Advisory System **730**– 53
Annex C Critical Infrastructure Protection **730**– 59
Annex D Special Events **730**– 61
Annex E Special Topics **730**– 63
Annex F Sample Forms **730**– 85
Annex G Informational References **730**– 86
Index **730**– 90

Documents 2023 Edition Document Sharing Hub
Full document details: NFPA 730 2023

NFPA 730

Guide for

Premises Security

2023 Edition

IMPORTANT NOTE: This NFPA document is made available for use subject to important notices and legal disclaimers. These notices and disclaimers appear in all publications containing this document and may be found under the heading "Important Notices and Disclaimers Concerning NFPA Standards." They can also be viewed at www.nfpa.org/disclaimers or obtained on request from NFPA.

UPDATES, ALERTS, AND FUTURE EDITIONS: New editions of NFPA codes, standards, recommended practices, and guides (i.e., NFPA Standards) are released on scheduled revision cycles. This edition may be superseded by a later one, or it may be amended outside of its scheduled revision cycle through the issuance of Tentative Interim Amendments (TIAs). An official NFPA Standard at any point in time consists of the current edition of the document, together with all TIAs and Errata in effect. To verify that this document is the current edition or to determine if it has been amended by TIAs or Errata, please consult the National Fire Codes® Subscription Service or the "List of NFPA Codes & Standards" at www.nfpa.org/docinfo. In addition to TIAs and Errata, the document information pages also include the option to sign up for alerts for individual documents and to be involved in the development of the next edition.

NOTICE: An asterisk (*) following the number or letter designating a paragraph indicates that explanatory material on the paragraph can be found in Annex A.

A reference in brackets [ ] following a section or paragraph indicates material that has been extracted from another NFPA document. Extracted text may be edited for consistency and style and may include the revision of internal paragraph references and other references as appropriate. Requests for interpretations or revisions of extracted text shall be sent to the technical committee responsible for the source document.

Information on referenced and extracted publications can be found in Chapter 2 and Annex G.

Chapter 1 Administration

1.1 Scope. This guide describes construction, protection, occupancy features, and practices intended to reduce security vulnerabilities to life and property.

1.1.1 NFPA 730 is referred to herein as "this guide" or "the guide."

1.1.2 This guide should not supersede government statutes or regulations.

1.2* Purpose. The purpose of this guide is to provide criteria for the selection of a security program to reduce security vulnerabilities.

1.3 Application. The application of this guide is based on the risk considerations determined in Chapter 5.

1.4 Retroactivity.

1.4.1 This guide applies to both new and existing buildings, structures, and premises.

1.4.2 Existing buildings or installations that do not comply with the provisions of the referenced documents should be permitted to be continued in service.

N **1.4.3** When an existing noncompliant building is altered or the site is altered, the alteration should incorporate compliance with the provisions of this guide.

1.5 Equivalency. Nothing in this guide is intended to prevent the use of systems, methods, or devices of equivalent or superior quality, strength, fire resistance, effectiveness, durability, and safety over those prescribed by this guide.

1.6 Units and Formulas.

1.6.1 SI Units. Metric units of measurement in this guide are in accordance with the modernized metric system known as the International System of Units (SI).

1.6.2 Primary and Equivalent Values. If a value for a measurement as given in this guide is followed by an equivalent value in other units, the first stated value should be regarded as the standard; the given equivalent value might be approximate.

1.6.3 Conversion Procedure. SI units have been converted by multiplying the quantity by the conversion factor and then rounding the result to the appropriate number of significant digits.

Chapter 2 Referenced Publications

2.1 General. The documents or portions thereof listed in this chapter are referenced within this guide and should be considered part of the recommendations of this document.

Δ **2.2 NFPA Publications.** National Fire Protection Association, 1 Batterymarch Park, Quincy, MA 02169-7471.

NFPA 72®, National Fire Alarm and Signaling Code®, 2022 edition.

NFPA *101®, Life Safety Code®,* 2021 edition.

NFPA 731, *Standard for the Installation of Premises Security Systems,* 2023 edition.

2.3 Other Publications.

2.3.1 BHMA Publications. Builders Hardware Manufacturers Association, 355 Lexington Avenue, 15th Floor, New York, NY 10017.

ANSI/BHMA A156 Series, *Categories of Builders Hardware.*

ANSI/BHMA A156.3, *Exit Devices*, 2014.

Δ **2.3.2 UL Publications.** Underwriters Laboratories Inc., 333 Pfingsten Road, Northbrook, IL 60062-2096.

UL 294, *Access Control System Units*, 2018.

UL 305, *Panic Hardware*, 2012.

UL 437, *Key Locks*, 2013, revised 2017.

UL 768, *Combination Locks*, 2013, revised 2018.

UL 1034, *Burglary-Resistant Electric Locking Mechanisms*, 2011, revised 2020.

UL 2802, *Performance Testing of Camera Image Quality*, 2013, revised 2019.

AVA Documents Document Sharing Hub

Full document details: NFPA 730 2023

UL 2058, *Outline of Investigation for High-Security Electronic Locks*, 2005.

2.3.3 Other Publications.

Merriam-Webster's Collegiate Dictionary, 11th edition, Merriam-Webster, Springfield, MA 2003.

Δ 2.4 References for Extracts in Advisory Sections.

NFPA 72®, National Fire Alarm and Signaling Code®, 2022 edition.

NFPA 731, *Standard for the Installation of Premises Security Systems*, 2023 edition.

NFPA 5000®, Building Construction and Safety Code®, 2021 edition.

Chapter 3 Definitions

3.1 General. The definitions contained in this chapter apply to the terms used in this guide. Where terms are not defined in this chapter or within another chapter, they should be defined using their ordinarily accepted meanings within the context in which they are used. *Merriam-Webster's Collegiate Dictionary*, 11th edition, is the source for the ordinarily accepted meaning.

3.2 NFPA Official Definitions.

3.2.1* Approved. Acceptable to the authority having jurisdiction.

3.2.2* Authority Having Jurisdiction (AHJ). An organization, office, or individual responsible for enforcing the requirements of a code or standard, or for approving equipment, materials, an installation, or a procedure.

3.2.3 Guide. An NFPA standard that is advisory or informative in nature and that contains only nonmandatory provisions. A guide may contain mandatory statements such as when a guide can be used, but the NFPA standard as a whole is not suitable for adoption into law.

3.2.4 Labeled. Equipment or materials to which has been attached a label, symbol, or other identifying mark of an organization that is acceptable to the authority having jurisdiction and concerned with product evaluation, that maintains periodic inspection of production of labeled equipment or materials, and by whose labeling the manufacturer indicates compliance with appropriate standards or performance in a specified manner.

3.2.5* Listed. Equipment, materials, or services included in a list published by an organization that is acceptable to the authority having jurisdiction and concerned with evaluation of products or services, that maintains periodic inspection of production of listed equipment or materials or periodic evaluation of services, and whose listing states that either the equipment, material, or service meets appropriate designated standards or has been tested and found suitable for a specified purpose.

3.2.6 Shall. Indicates a mandatory requirement.

3.2.7 Should. Indicates a recommendation or that which is advised but not required.

3.3 General Definitions.

3.3.1* Access Control. The act of managing ingress or egress through a portal by validating a credential or an individual. [**731,** 2023]

3.3.2* Accessible Opening. An opening in a protected perimeter.

3.3.3 Alarm.

3.3.3.1* *False Alarm.* Notification of an alarm condition when no evidence of the event that the alarm signal was designed to report is found. [**731,** 2023]

3.3.3.2* *Holdup Alarm.* An alarm that originates from a point where holdup protection is used, such as a bank teller window or store cash register.

3.3.4* Annunciator. A unit containing one or more visible or audible indicators, alphanumeric displays, monitors, or other equivalent means in which each indication provides status information about a circuit, condition, system, or location.

3.3.5 Area.

3.3.5.1* *Controlled Area.* A room, office, building, or facility to which access is monitored, limited, or controlled.

3.3.5.2* *Restricted Area.* A room, office, building, or facility to which access is strictly and tightly controlled.

3.3.6* Capacitance Sensor. A sensor that detects a change in capacitance when a person touches or comes in close proximity to an object.

3.3.7 Change Key/Credential. See 3.3.23.1.

3.3.8 Confidential Information. See 3.3.22.1.

3.3.9 Control Unit. A system component that monitors inputs and controls outputs through various types of circuits. [**72,** 2022]

3.3.10 Controlled Area. See 3.3.5.1.

3.3.11 Deterrent. Any physical or psychological device or method that discourages action.

3.3.12* Electromagnetic Lock. A door lock that uses an electrically actuated magnetic attraction to secure the door.

3.3.13 Expanded Metal. An open mesh formed by slitting and drawing sheet metal, made in various patterns and metal thicknesses, with either a flat or irregular surface.

3.3.14 Facility Classification.

3.3.14.1 *Educational Facility.* A facility used for educational purposes through the twelfth grade and facilities of colleges and universities used by six or more persons for 4 or more hours per day or more than 12 hours per week.

3.3.14.2* *Health Care Facilities.* Buildings, portions of buildings, or mobile enclosures in which medical, dental, psychiatric, nursing, obstetrical, or surgical care is provided. [**5000,** 2021]

3.3.14.3 *Industrial Facility.* A facility in which products are manufactured or in which processing, assembling, mixing, packaging, finishing, decorating, or repair operations are conducted.

Documents 2023 Edition Document Sharing Hub

Full document details: NFPA 730 2023

3.3.14.4 ***Lodging Facility.*** Facilities that provide housing and generally, but not always, food, beverage, meeting facilities, retail shops, recreational facilities, and other services, including but not limited to hotels, motels, motor hotels, resort hotels, inns, country clubs, and conference centers.

3.3.14.5 ***Multi-Dwelling Unit.*** A facility with more than three dwelling units.

3.3.14.6 ***Office Building.*** A facility used for office, professional, or service-type transactions, including but not limited to storage of records and accounts.

3.3.14.7 ***One- and Two-Family Dwelling.*** Facilities containing one or two dwelling units that are occupied primarily on a permanent basis.

3.3.14.8 ***Parking Facility.*** A structure or space where the primary use is storage of vehicles.

3.3.14.9 ***Restaurant.*** Restaurants include fast food establishments, convenience stores, walk-up-style facilities, and larger assembly-type facilities with full table service, lounges, and so forth.

3.3.14.10 ***Retail Establishment.*** A facility used for the display and sale of merchandise.

3.3.14.11 ***Shopping Center.*** A group of retail and other commercial establishments that is planned, developed, and managed as a single property.

3.3.15 False Alarm. See 3.3.3.1.

3.3.16* Foil. An electrically conductive ribbon used for a sensing circuit.

3.3.17 Grandmaster Key/Credential. See 3.3.23.2.

3.3.18 Hinge Dowel. A dowel or pin that projects from a door jamb into an opening in the edge of a door at its hinge that prevents removal of the locked door even if the hinges or hinge pins are removed.

3.3.19 Holdup Alarm. See 3.3.3.2.

3.3.20 Holdup Alarm System. See 3.3.40.1.

3.3.21 Human/Machine Interface (HMI). The point at which people control or monitor the condition of an electronic premises security system.

3.3.22 Information.

3.3.22.1* ***Confidential Information.*** Information to which access is restricted.

3.3.22.2 ***National Security Information.*** Designated information that requires protection in the interest of national defense or foreign relations of the United States, that is, information classified in accordance with Executive Order 12356 and not falling within the definition of Restricted Data or Formerly Restricted Data.

3.3.23 Key/Credential.

3.3.23.1 ***Change Key/Credential.*** A key/credential that will operate only one lock or group of keyed-alike locks, as distinguished from a master key/credentials.

3.3.23.2 ***Grandmaster Key/Credential.*** The key/credential that operates two or more separate groups of locks, each of which is operated by different master keys/credentials.

3.3.24 Keypad. A device that is a type of human/machine interface (HMI) with numerical or function keys that can incorporate an annunciator or a signaling device. [**731,** 2023]

3.3.25* Line Supervision. Automatic monitoring of circuits and other system components for the existence of defects or faults that interfere with receiving or transmitting an alarm.

3.3.26 Lockdown. A state where the building is secured and occupants are sequestered in the nearest safe location and not allowed to move within the building.

3.3.27 Lockout. A state where the perimeter of the building or property is secured for ingress and occupants are free to move within the building.

3.3.28* Machine Readable Credential. A device or scheme containing some knowledge, an identifying credential, or a biometric identifier.

3.3.29* Microwave Sensor. An active intrusion sensor that detects the movement of a person or object through a pattern of microwave energy.

3.3.30* Monitoring Station. A facility that receives signals from electronic premises security systems and has personnel in attendance at all times to respond to these signals. [**731,** 2023]

3.3.31 National Security Information. See 3.3.22.2.

3.3.32 Perimeter Protection. A scheme of protection that uses devices to detect or deter intrusion into a protected area.

3.3.33 Post Orders. The written procedures from the facility management that list the duties and direct the actions of security officers.

3.3.34* Reader. A device that allows a machine readable credential to be entered into an access control system. [**731,** 2023]

3.3.35 Restricted Area. See 3.3.5.2.

3.3.36* Screens. An array of wires usually interwoven every 6 in. (2.5 cm) either horizontally or vertically on a screen or alarm screening that protects areas or openings, such as skylights and crawl spaces. [**731,** 2023]

3.3.37* Security Vulnerability Assessment (SVA). A systematic and methodical process for examining ways an adversary might exploit an organization's security vulnerabilities to produce an undesired outcome.

3.3.38* Shelter-in-Place. Occupants within the building remain indoors until given further instructions.

3.3.39 Surreptitious Entry. The unauthorized entry into a facility or security container in a manner such that evidence of the entry is not discernable under normal circumstances.

3.3.40 System.

3.3.40.1* ***Holdup Alarm System.*** A system or portion thereof that connects to holdup alarm initiating devices. [**731,** 2023]

3.3.41 Top Guard. Antipersonnel device, usually of barbed or concertina wire, installed at the tops of fences and along roof edges.

AVA Documents Document Sharing Hub

Full document details: NFPA 730 2023

3.3.42 Unauthorized Person. A person who does not have permission to enter a protected premises or is not authorized to have access to specific confidential information.

3.3.43* Vault (as related to premises security). A fixed-in-place structure with all boundary surfaces constructed of reinforced materials such as poured concrete or engineered modular panels designed for such applications and secured with listed doors and locks. [**731,** 2023]

3.3.44 Zone. A defined area within a protected premise. A zone can define an area from which a signal can be received, an area in which a signal can be sent, or an area in which a form of control can be executed.

Chapter 4 General

4.1 Fundamental Principles.

4.1.1 The primary goals of this guide should be as follows:

(1) To provide an environment for the occupants inside or near a building that is reasonably safe from security threats
(2) To provide reasonable safeguards for protection of property from security threats

4.1.2 Implementing the goals of this guide should require a security plan.

4.1.3 A security plan should address the following security objectives:

(1) Restrict area perimeter — secure and monitor the perimeter of the facility
(2) Secure site assets — secure and monitor restricted areas or potentially critical targets within the facility
(3) Screen and control access — control access to the facility and to restricted areas within the facility by screening and/or inspecting individuals and vehicles as they enter, including the following:
    (a) Measures to deter the unauthorized introduction of dangerous substances and devices that could facilitate an attack or actions having serious negative consequences
    (b) Measures implementing a regularly updated identification system that checks the identification of facility personnel and other persons seeking access to the facility and that discourages abuse through established disciplinary measures
(4)* Deter, detect, or delay — deter, detect, or delay an attack, creating sufficient time to implement countermeasures between detection of an attack and the point at which the attack becomes successful
(5) Shipping, receipt, and storage — secure and monitor the shipping, receipt, and storage of hazardous materials for the facility
(6) Theft and diversion — deter theft or diversion of assets
(7) Sabotage — deter insider sabotage
(8) Response — develop and exercise an emergency plan to respond to security incidents internally and with assistance of local law enforcement and first responders
(9) Monitoring — maintain effective monitoring, communications, and warning systems, including the following:
    (a) Measures designed to ensure that security systems and equipment are in good working order and inspected, tested, calibrated, and otherwise maintained
    (b) Measures designed to regularly test security systems, note deficiencies, correct for detected deficiencies, and record results so that they are available for inspection
    (c) Measures to allow the facility to promptly identify and respond to security system and equipment failures or malfunctions
(10) Training — ensure proper security training, exercises, and drills of facility personnel
(11) Personnel surety — perform appropriate background checks on and ensure appropriate credentials for facility personnel and, as appropriate, for unescorted visitors with access to restricted areas or critical assets, including the following:
    (a) Measures designed to verify and validate identity
    (b) Measures designed to check criminal history
    (c) Measures designed to verify and validate legal authorization to work
    (d) Measures designed to identify people with terrorist ties
(12) Elevated threats — escalate the level of protective measures for periods of elevated threat
(13) Significant security incidents and suspicious activities — identify, investigate, report, and maintain records of significant security incidents and suspicious activities in or near the site
(14) Officials and organization — establish official(s) and an organization responsible for security and for compliance with these guides
(15) Records — maintain appropriate records

4.1.4 A security plan should include a security vulnerability assessment (SVA).

4.2 Classification of Assets.

4.2.1 Assets should be classified by risk.

4.2.2* The security assessment for assets should be in accordance with the applicable occupancy chapter (Chapters 11 through 20).

4.2.3 Classification of assets should be subject to the ruling of the owner or the owner's designee where there is a question of proper classification in any individual case.

4.3 Security Planning.

4.3.1 The security plan should comply with all of the following:

(1) Chapter 5
(2) Chapters 11 through 20 for the occupancy involved
(3) Chapters 6 through 10 when referenced from Chapters 11 through 20 for the occupancy involved

4.3.2 The SVA should identify the security risks in the physical and operational environment of the organization.

4.3.3* Risks identified in the SVA should be arranged by frequency and severity.

4.3.4 Procedures and controls should be implemented to satisfy all of the following:

(1)* The organization's tolerance to risk
(2) The goals listed in 4.1.1

Documents 2023 Edition Document Sharing Hub
Full document details: NFPA 730 2023

(3) The objectives listed in 4.1.3

4.4 Security Plan Evaluation.

4.4.1* Periodic drills should be conducted at various times and locations.

4.4.1.1 The drills should be critiqued for plan effectiveness and to identify opportunities for improvement.

4.4.1.2 Identified opportunities for improvement should be incorporated into the security plan.

4.4.2* The review and update of the SVA should be based on the level of risk, threats, crime, and change of conditions within the organization.

4.5 System Design and Installation. Any security system, building service equipment, or safeguard and all associated software provided for security should be designed, installed, maintained, and approved in accordance with applicable adopted codes and standards, including NFPA 731, the manufacturer's specifications, applicable UL standards, the AHJ, and nationally recognized industry standards, guides, and practices.

4.6 Maintenance.

4.6.1 Any device, equipment, system, condition, arrangement, level of protection, or any other feature provided in accordance with this guide, should be maintained to function as installed.

4.6.2* Emergency and security equipment should be repaired on a priority based on the SVA.

4.6.3 A repair log should list repairs, including but not limited to the following:

(1) The system impairment
(2) The time and date of the impairment
(3) Repairs that were completed
(4) The time and date of each repair

4.6.4 Repair logs should be retained for not less than 1 year.

Chapter 5 Security Planning

5.1 General.

5.1.1 The security plan should document the protection of an organization's defined critical assets.

5.1.2 The property building owner, or owner's designated representative should be responsible for the SVA.

5.2 Security Vulnerability Assessment (SVA).

5.2.1* Security planning should begin with an SVA.

5.2.2* An SVA should assess the current status of an organization's vulnerabilities, including but not limited to threat exposures, security features, and preparedness.

5.2.3 A security vulnerability assessment should utilize a recognized, analytical methodology to assess the security-related risks and vulnerabilities of an organization, its property, and personnel. This assessment should include, but not be limited to the following:

(1)* *Step 1: Formation of team.* Form a team of personnel from pertinent organizational areas and other stakeholders.
(2)* *Step 2: Organization/facility characterization.* Characterize the organization and the facilities to be protected.
(3) *Step 3: Threat assessment.* Classify threats using an assessment process that includes but is not limited to the following:
    (a) Classification of critical assets
    (b) Identification of potential targets
    (c) Consequence analysis (i.e., effect of loss, including potential off-site consequences)
    (d) Definition of potential threats (i.e., identifying potential adversaries and what is known about them)
(4)* *Step 4: Threat vulnerability analysis.* Conduct a threat vulnerability analysis identifying actual and potential threat scenarios and estimate a relative security risk level.
(5)* *Step 5: Define specific security countermeasures.* Define countermeasures using information from the previous four steps, including characterization, threat, and vulnerability analysis.
(6) *Step 6: Assess risk reduction.* Reassess the relative security risk levels developed in Step 4, taking into account the countermeasures defined in Step 5, and implement additional security risk reduction measures (security countermeasures) where appropriate.
(7) *Step 7: Document findings and track implementation.* Document findings and recommendations and track the implementation of accepted recommendations.

5.3 Qualifications.

5.3.1 The SVA provider should provide evidence of its qualifications, education, certification, or experience when requested by the property building owner or the owner's designated representative.

5.3.2* The SVA provider's personnel conducting the SVA should be certified by a nationally recognized certification organization in security or crime prevention.

5.4 Security Plan.

5.4.1 The security plan should include but not be limited to the following *(for special events, see Annex E)*:

(1) Statement of purpose
(2) Organizational policies and procedures
(3) Description of the facility and organizational structure
(4) Security vulnerability assessment, including threat assessments and risks
(5) Instructions for using the plan
(6) Description of the features of protection
(7) Organization's security-related measures and procedures
(8) Information needed to implement the security measures and procedures
(9) List of the intended users of the plan
(10) Plan distribution list
(11) Location of the master copy
(12) Organization for security operations
(13) Procedures for employee, visitor, and vendor safety

5.4.2 Plan components should be based on the potential threats facing the organization or facility as determined by the SVA.

5.4.3 The objectives of the security plan should be specific, measurable, achievable, relevant, and timely.

AVA Documents Document Sharing Hub
Full document details: NFPA 730 2023

5.4.4 The security plan should follow the organizational mission and policies.

5.4.5 The security plan should include procedures for movement, communication, facility management, reacting to security incidents, and reporting and analyzing incidents.

5.4.6 Supporting information should be documented and maintained.

5.4.7 Supporting information should include but not be limited to the following:

(1)* Personnel contact information
(2) A list of cooperating agencies, contact people, telephone numbers, and radio frequencies
(3) Mutual aid agreements
(4)* Important outside contacts
(5)* Maps
(6)* Emergency supply inventory

5.4.8* The plan should include response actions to be implemented in the event of a security incident.

5.4.9 An emergency action plan should include but not be limited to the following:

(1) Nature of expected incidents
(2)* Incident response procedures
(3) Emergency contact information
(4) Division of responsibilities and authority among the facility personnel, including who can initiate the plan
(5) Identification of who is covered by the plan (e.g., who is to be evacuated)
(6) Resources needed for the management of the incident
(7) Guidance on the emergency use of funds, disposition of project property, and personal effects
(8) List of annexes to the plan, including but not limited to maps, floor plans, forms, location of personnel, telephone numbers, radio frequencies, and extraordinary procedures

5.4.10 Since the security plan has public and private components, the private components should be maintained as confidential information.

5.5 Planning for Acts of Intimidation or Violence. An organization or facility should include in the security plan, to the extent identified by the SVA, measures to be taken in the event of acts of intimidation or violence.

Chapter 6 Administrative Controls

6.1 General. The recommendations of Chapter 6 should apply when specifically referenced from Chapters 11 through 20.

6.2 People Management.

6.2.1 Employees.

6.2.1.1* Employers should promote trustworthiness by using the following personnel practices for employees with access to critical assets:

(1)* Background screening
(2) Verification of background screening of contracted personnel acting in the capacity of employees
(3) Drug testing program

6.2.1.2* Identification badges should have a photograph of the bearer and the bearer's name.

6.2.1.3 When identification badges are issued, employees should, as indicated in the security plan, do one of the following:

(1) Display the badge at all times
(2) Display the badge on demand

6.2.2 Visitors. When identification badges are issued, visitors should, as indicated in the security plan, do one of the following:

(1) Display the badge at all times
(2) Display the badge on demand

6.2.3* Vendors and Contractors.

6.2.3.1 Employers should verify the background screening of vendors and contractors with access to critical assets.

6.2.3.2 When identification badges are issued, vendors and contractors should, as indicated in the security plan, do one of the following:

(1) Display the badge at all times
(2) Display the badge on demand

6.2.4* Security Personnel. Security personnel deployed at a protected premises should comply with the recommendations of this section.

6.2.4.1 Personnel Requirements.

6.2.4.1.1 The number of security personnel should be determined by the security plan and the person responsible for facility security.

6.2.4.1.2 Selection criteria for security personnel should include but not be limited to the following:

(1) Federal, state, and local laws and regulations
(2) Knowledge of criminal activities and proper law enforcement response procedures
(3) Good judgment and emotional stability
(4) Experience and demonstrated ability to retain composure under pressure
(5)* Disclosure of charges or convictions for felonies or crimes involving dishonesty or moral turpitude

6.2.4.2* Security Duties. Security personnel should perform the services prescribed in the post orders.

6.2.4.2.1 Facilities with security personnel should have post orders.

6.2.4.2.2 Post orders should contain a list of the duties of the security officer and instructions to cover reasonably foreseeable events security personnel might encounter.

6.2.4.2.2.1 Post orders should list the name of the facility, the date issued, effective date, and purpose.

6.2.4.2.2.2 Post orders should list security personnel duties, including but not be limited to the following:

(1) Authority of security personnel
(2) Emergency response procedures
(3) Job classification
(4) Uniforms
(5) Authorized weapons, including firearms, batons, and mace

Documents 2023 Edition Document Sharing Hub
Full document details: NFPA 730 2023

(6) Reporting times
(7) Security patrols
(8) Hours of coverage
(9) Facility rules and regulations
(10) Applicable federal, state, and local laws
(11) Other duties to be assigned

6.2.4.2.2.3* Instructions should be lawful and endeavor to protect the safety of security personnel and those they interact with in performance of their duties.

6.2.4.2.3 Post orders should be reviewed and updated as required by the SVA.

6.2.4.2.3.1 Facility management and security management should frequently assess post orders to identify and correct operational problems.

6.2.4.2.3.2 A procedure should be established to inform security personnel of changes in post orders.

6.2.4.3* Supervision.

6.2.4.3.1* Security patrols should be supervised.

6.2.4.3.2 Records should be kept, including but not limited to the following:

(1) Crimes discovered by or reported to security personnel
(2) Frequency of patrols
(3) Activity log
(4)* Exceptions log

6.2.4.3.3 Security records should be retained for not less than 5 years or until the expiration of the appropriate statute of limitations, whichever is longer.

6.2.4.4 Security Personnel Communications. Field security personnel should have a process and means to communicate with a security office or public safety agencies.

6.2.4.5* Weapons and Equipment.

6.2.4.5.1 Security personnel should carry only authorized equipment.

6.2.4.5.2 Where weapons are authorized, policies and procedures governing their storage, handling, and use should be established.

6.2.4.6* Training.

6.2.4.6.1 Security personnel should be trained in the performance of their duties.

6.2.4.6.2 Security personnel who carry weapons should be trained in their storage, handling, and use.

6.2.4.6.3 Armed security personnel should have firearms training.

6.3 Material Receiving.

6.3.1 Commercial Receivables.

6.3.1.1* Shipments coming into facilities should be stopped for entry authorization and dock assignment.

6.3.1.1.1 Shipments coming in should be expected and have corresponding purchase orders or requisitions.

6.3.1.1.2 Undocumented deliveries should not be accepted.

6.3.1.2 Receipt of hazardous materials should be documented and tracked.

6.3.2 Package Deliveries.

6.3.2.1 Packages being delivered should be inspected for evidence of tampering or damage.

6.3.2.2* Any damaged or suspicious packages should be reported to the carrier.

6.3.3 Mail.

6.3.3.1* Employees who handle mail should evaluate the appearance of incoming packages to determine if they fit the characteristics of mail normally received.

6.3.3.2 The recipient of a letter or package should evaluate the delivery to determine if a package is from an unknown, unsolicited source.

6.3.4 Couriers.

6.3.4.1 Couriers making deliveries should provide identification.

6.3.4.2 Courier identification should be entered into a delivery log or attached to the item being delivered.

6.4 Information and Data Security. Organizations should have a policy and procedure for the storage, handling, and use of sensitive information and data, both electronic and printed.

6.4.1 Management of Sensitive Security Information. (Reserved)

6.4.2 Physical Security. (Reserved)

6.4.3 Electronic Security. (Reserved)

6.4.4 Retention and Disposal. (Reserved)

6.5 Workplace Violence.

6.5.1* Employers should develop a program for workplace violence prevention.

6.5.2* An effective approach to preventing workplace violence should include but not be limited to the following key components:

(1) Management commitment
(2) Employee involvement
(3) Worksite hazard analysis
(4) Hazard prevention and control
(5) Safety and health training
(6) Evaluation

Chapter 7 Security Perimeters

7.1 General.

7.1.1 The recommendations of Chapter 7 should apply when specifically referenced in Chapters 11 through 20.

7.1.2 The area covered by the security plan should be defined in the security vulnerability assessment (SVA).

7.1.3* The primary security perimeter should include the total area in the security plan.

AVA Documents Document Sharing Hub
Full document details: NFPA 730 2023

7.1.4* Secondary security perimeters within the primary security perimeter should be areas identified as either secured or unsecured.

7.1.5* Movement through every portal in a secured perimeter should be controlled.

7.1.6 Physical barriers or security systems utilized or installed in security perimeters should comply with applicable fire code or other life safety requirements.

7.2* Area Designations. Areas within secondary security perimeters should be designated as one of the following:

(1) Unsecured
  (a) Open
  (b) Protected
(2) Secured
  (a) Controlled
  (b) Restricted

7.3 Exterior Perimeters.

7.3.1* General. Exterior security devices and systems should include but not be limited to the following:

(1) Fences and other physical barriers
(2) Walls
(3) Roofs
(4) Protective lighting
(5) Ironwork (e.g., bars and grilles)
(6) Glazing materials
(7) Passive barriers
(8) Electronic security devices

7.3.2 Fences.

7.3.2.1* Sight lines should be maintained at fence lines.

7.3.2.2* Warning signs should be maintained.

7.3.2.3* Fences should be maintained for integrity.

7.3.3* Walls. When a wall serves as a component of an exterior security perimeter, it should be resistant to penetration.

7.3.4* Roofs. Roofs serving as a component of an exterior security perimeter should comply with 7.3.4.1 through 7.3.4.3.

7.3.4.1 The roof should be protected against unauthorized access.

7.3.4.2 The roof should be resistant to penetration.

7.3.4.3 Openings in the roof should be protected.

7.3.5* Openings to Be Secured. Openings should be protected against entry by unauthorized persons.

7.4 Interior Perimeters.

7.4.1* Where a secure area designation defines an interior room or space, the interior perimeter of such room or space should be protected so that only authorized personnel are permitted to enter.

7.4.2* Access to controlled or restricted areas should be in accordance with Section 7.5.

7.4.3 Factors to be considered in securing an interior perimeter should include but not be limited to the following:

(1) Sensitivity or criticality of the operation
(2) Facility vulnerability to damage, interruption, alteration, or other harm
(3) Sensitivity or value of the information or property stored within or at the facility
(4)* Location of the facility and vulnerability to intrusion
(5) Other forms of protection in place or available
(6) Law enforcement or responder capability
(7) Occupants of the area
(8) Life safety, egress, and information dissemination

7.5 Portal Control.

7.5.1 General.

7.5.1.1 The number of portals in a security perimeter should be restricted to the minimum required for safe and efficient operation of the facility.

7.5.1.2* Movement through portals in security perimeters should be controlled.

7.5.2 Exterior Portals.

7.5.2.1 Exterior entrances should be provided with locking devices.

7.5.2.2 Exterior hinge pins on doors in security perimeters should be secured against removal.

7.5.3 Locks.

7.5.3.1* Egress and fire resistance provisions relating to doors and hardware should be maintained.

Δ **7.5.3.2** Individual products should be listed to the following standards as applicable:

(1)* ANSI/BHMA A156 Series, *Categories of Builders Hardware*, for builders' hardware
(2) UL 1034, *Burglary-Resistant Electric Locking Mechanisms*, for burglary-resistant electronic locking mechanisms
(3) UL 437, *Key Locks*, for key locks
(4) UL 768, *Combination Locks*, for combination locks
(5) UL 294, *Access Control System Units*, for access control system units
(6) UL 2058, *Outline of Investigation for High-Security Electronic Locks*, for high-security electronic locks
(7) UL 305, *Panic Hardware*, and ANSI/BHMA A156.3, *Exit Devices*, for exit panic devices

7.5.3.3 Locking devices should be properly installed and in good working order.

7.5.3.4* Doors intended to be continuously secured should automatically close and securely latch.

7.5.4* Key/Credential Control.

7.5.4.1 The integrity of key/credential systems should be protected by the use of key/credential control.

7.5.4.2 Key/credential control procedures should include but not be limited to the following:

(1) Re-keying when a key to a designated controlled or restricted area is lost
(2) Maintaining access lists for persons authorized to draw master keys
(3)* Maintaining security of key/credential storage containers and cabinets
(4) Performing security checks of key/credential storage containers and cabinets

Documents 2023 Edition Document Sharing Hub
Full document details: NFPA 730 2023

(5) Performing an inventory of keys/credentials annually or as dictated by the security plan
(6) Maintaining a record of key/credential issuance requests, approvals, and issuances
(7) Destroying or maintaining security on keys/credentials not issued or no longer needed
(8) Discretely identifying keys/credentials and key/credential tags by use of a coding system
(9)* Training employees on key/credential control policy and procedure

7.5.4.3* Key/credential control records should include but not be limited to the following:

(1) Number assigned to each key/credential and lock
(2) Location of each lock (room number)
(3) Person to whom each key/credential has been issued
(4) Date of issuance
(5) Date of return
(6)* Documented acceptance for each key/credential issued and returned

Chapter 8 Crime Prevention Through Environmental Design

8.1* General. The recommendations of Chapter 8 should apply when specifically referenced from Chapters 11 through 20.

8.2 Crime and Loss Prevention. (Reserved)

8.3 Human Behavior. (Reserved)

8.4* Lighting. Protective lighting should accomplish the objectives in 8.4.1 through 8.4.8.

8.4.1* Lighting should meet the following criteria:

(1) Be lumen efficient
(2) Be designed to create adequate light levels without being excessive
(3) Minimize night sky pollution

8.4.2 Lighting should meet the recommendations of the security vulnerability assessment (SVA).

8.4.3* For the purpose of natural surveillance and normal use, reasonable illumination should be provided and maintained for exterior areas, including but not limited to the following:

(1) Pedestrian entrances and walkways
(2) Exterior doors
(3) Vehicular entrances
(4) Perimeter fence line where indicated by the SVA
(5) Sensitive areas or structures within the secure perimeter
(6) Parking areas

8.4.4 Constant interior lighting should be maintained for the following:

(1) Egress lighting
(2) Minimum lighting levels for areas under video surveillance

8.4.5* Guard posts should be illuminated based on the SVA.

8.4.6* Redundancy of lighting should be provided based on the SVA.

8.4.7* Security lighting should be protected from vandalism and sabotage.

8.4.8* Security lighting should be maintained.

8.5* Landscaping. Foliage and shrubbery should be trimmed and maintained.

8.6 Aesthetics. (Reserved)

Chapter 9 Security Systems

9.1 General.

9.1.1 The recommendations of Chapter 9 should apply when specifically referenced from Chapters 11 through 20.

9.1.2 Electronic premises security systems should be installed in compliance with the requirements of NFPA 731.

9.2 Contraband Detection. (Reserved)

9.2.1 Weapon Detection (Magnetometers and X-Ray). (Reserved)

9.2.2 Explosive Detection (Man Portal, Parcel/Freight, and Portable). (Reserved)

9.2.3 Radiation Detection (Man Portal, Parcel/Freight, and Portable). (Reserved)

9.2.4 Narcotics Detection (Man Portal and Portable). (Reserved)

9.2.5 Biological and Chemical Agent Detection (Fixed and Portable). (Reserved)

9.3 Personnel Safety Alerting Systems. (Reserved)

9.3.1 Emergency Communication System. (Reserved)

9.3.2 Holdup, Duress, Ambush, and Man Down Alarms. (Reserved)

9.3.3 Threat/Door/Miscellaneous Alarms. (Reserved)

9.3.4 Video Surveillance Analytics Alerting Systems. (Reserved)

9.4 Property Protection Monitoring Systems.

9.4.1 Asset Tracking. (Reserved)

9.4.2 Intrusion Detection Systems.

9.4.2.1* Intrusion detection systems should be designed to protect against vulnerabilities identified by a security vulnerability assessment (SVA).

9.4.2.2 Intrusion detection systems should be installed in accordance with the requirements of NFPA 731.

9.4.2.3 Signals from an intrusion detection system alarm should be in accordance with the requirements of 5.1.3 of NFPA 731.

9.4.2.4 The alarm system should be periodically tested and properly maintained as required in Chapter 10 of NFPA 731.

9.4.3 Access Control Systems.

9.4.3.1* Access control systems should be designed to control movement through portals as determined by the SVA.

AVA Documents Document Sharing Hub
Full document details: NFPA 730 2023

9.4.3.2 Access control systems should be installed in accordance with the requirements of NFPA 731.

9.4.3.3 Access to unissued active machine readable credentials should be controlled.

9.4.4 Video Surveillance.

9.4.4.1* Video surveillance systems performance requirements should be designed in accordance with the intent of the SVA.

9.4.4.2 Video surveillance systems should be installed in accordance with the requirements of NFPA 731.

9.4.4.3* Where video surveillance is installed, the system should be monitored or recorded.

9.4.4.4 Where signs are installed, the signs should be maintained.

9.4.4.5* Video surveillance systems should be maintained so that the system will continue to perform as determined by the design in 9.4.4.1.

Δ **9.4.4.6** Where the SVA requires a particular image quality for video surveillance, the camera should be evaluated to a standard such as UL 2802, *Performance Testing of Camera Image Quality*.

9.4.5* Guard Tour Systems. (Reserved)

9.5 Security Monitoring. (Reserved)

Chapter 10 Accessory Property

10.1 General.

10.1.1 The recommendations of Chapter 10 should apply when specifically referenced from Chapters 11 through 20.

10.1.2 A security vulnerability assessment (SVA) should be conducted for accessory properties as part of the security plan.

10.2 Parking.

10.2.1 General.

10.2.1.1 Section 10.2 provides recommendations to control security vulnerabilities in parking facilities, whether a structure or a space, used for the storage of motor vehicles.

10.2.1.2* A parking facility should have a security plan complying with Chapter 5.

10.2.1.3* Owners and operators of parking facilities should take proactive measures shown as needed by the SVA.

10.2.2* Administrative Controls. Security patrols should comply with 6.2.4.

10.2.3 Security Perimeters.

10.2.3.1* Area Designations. Vehicle entrance and exit portals should be limited to the minimum required for operation of the parking facility.

10.2.3.2* Exterior. (Reserved)

10.2.3.3 Interior. (Reserved)

10.2.3.4 Portal Control. (Reserved)

10.2.4 Crime Prevention Through Environmental Design (CPTED).

10.2.4.1 Crime and Loss Prevention.

10.2.4.2* Human Behavior. Parking areas should be well marked.

10.2.4.3* Lighting. Lighting should comply with Section 8.4.

10.2.4.4* Landscaping. Foliage and shrubbery should be trimmed and maintained.

10.2.4.5 Aesthetics. (Reserved)

10.2.5 Security Systems.

10.2.5.1* Duress Alarms. Public duress alarm systems, where present, should be installed and maintained in accordance with NFPA 731.

10.2.5.2 Access Control. Access control systems should be in accordance with 9.4.3.

10.3 Storage. (Reserved)

10.4 Exterior Areas. (Reserved)

Chapter 11 Educational Facilities, Colleges, and Universities

11.1 General.

11.1.1 Scope.

11.1.1.1 This chapter addresses measures to mitigate security vulnerabilities in educational facilities.

11.1.1.2 Facilities within the scope of this chapter should include public and private primary and secondary schools (K–12), colleges, and universities.

11.1.1.3 Assets within the primary security perimeter should be classified in accordance with their use.

11.1.1.4 Assets used as other than educational facilities should comply with the requirements of this chapter and the appropriate occupancy chapter (Chapters 12 through 20).

11.1.2 Security Plan.

11.1.2.1* An educational facility should have a security plan.

11.1.2.2 The security plan should include but not be limited to the following security vulnerabilities:

(1) Vandalism
(2) Theft
(3) Burglary
(4) Embezzlement
(5) Sexual predation
(6) Assault
(7) Weapons violations
(8) Robbery

11.1.2.3* The educational facility should conduct a security vulnerability assessment (SVA) as part of the security plan.

Documents 2023 Edition Document Sharing Hub
Full document details: NFPA 730 2023

11.1.2.3.1* The SVA should evaluate the potential security risks posed by the physical and operational environment of the educational facility to all assets at the facility.

11.1.2.3.2 The facility should implement procedures and controls in accordance with the SVA.

11.1.2.4 The security plan should be coordinated with emergency response, disaster, and business recovery plans.

11.1.3 Responsible Person.

11.1.3.1 A person(s) should be appointed by the management of the educational facility to be responsible for security management activities.

11.1.3.2 The duties of the responsible person(s) should be as identified in the SVA and include, but not be limited to, the following:

(1) Providing identification badges or machine-readable credentials
(2) Controlling movement through portals
(3) Defining and implementing procedures for security incidents including, but not limited to, the following:
    (a) Active shooters
    (b) Access to emergency areas
    (c) Hostage situations
    (d)* Bombs
    (e) Criminal threats
    (f) Labor actions
    (g) Disorderly conduct
    (h) Workplace violence
    (i) Response to restraining orders
    (j) Abductions
    (k) Incidents involving VIPs
    (l) Incidents involving the media
(4) Managing asset protection procedures
(5) Implementing procedures for interaction with emergency services
(6) Ensuring compliance with applicable laws, regulations, and standards regarding security management operations
(7) Establishing education and training programs to address the following:
    (a) Customer service
    (b) Use of force
    (c) Response criteria
    (d) Fire watch procedures
    (e)* Lockdown, lockout, clear the halls, and shelter-in-place procedures
    (f) Emergency notification procedures
(8) Establishing recordkeeping procedures
(9)* Conducting at least one of the following security-related drills semiannually:
    (a) Lockdown
    (b) Lockout
    (c) Shelter-in-place
    (d) Clear the halls

11.2 Administrative Controls.

11.2.1 People Management.

11.2.1.1 Employees.

11.2.1.1.1 Employee practices should comply with 6.2.1.

11.2.1.1.2* Employees should be instructed how to exercise reasonable care in protecting personal property.

11.2.1.1.3* Employees and tenants should receive training on their roles in the security plan.

11.2.1.2 Students.

11.2.1.2.1 Students should be notified of significant security-related incidents.

11.2.1.2.2 Where identification badges are provided, students should display identification badges as recommended in 6.2.1.2 for employees.

11.2.1.3 Visitors.

11.2.1.3.1* All visitors should enter buildings through a monitored and designated visitor entrance(s).

11.2.1.3.2 All visitors should be issued school visitor identification.

11.2.1.3.3 All visitors should be required to show government-issued, photo identification to a staff member to be issued school visitor identification.

11.2.1.3.4 All visitors should be required to wear school visitor identification visible at all times.

11.2.1.4* Vendors and Contractors. (Reserved)

11.2.1.5 Security Personnel.

11.2.1.5.1* The decision to provide security personnel should be based on the SVA.

11.2.1.5.2 Security personnel should comply with 6.2.4.

11.2.1.5.3 Security patrols should be conducted in accordance with the facility security plan.

11.2.2 Material Receiving. The receipt of materials should comply with Section 6.3 and the applicable occupancy chapter (Chapters 12 through 20).

11.2.3 Information and Data Security. (Reserved)

11.2.4 Workplace Violence.

11.2.4.1 A workplace violence plan should be required.

11.2.4.2 The workplace violence plan should be in accordance with Section 6.5.

11.3 Security Perimeters.

11.3.1 Area Designations.

11.3.1.1 Areas identified in the SVA should be classified in accordance with Sections 7.1 and 7.2.

11.3.2 Exterior — Primary School (K-12) Property.

11.3.2.1 Exterior security perimeters should be designated and protected in accordance with Chapter 7.

11.3.2.2 In accordance with Section 7.2, secondary exterior security perimeters should include, but not be limited to, the following areas:

(1) Exterior locations used by students for school activities that are designated as unsecured and protected
(2) Parking lots that are designated as secured and controlled

AVA Documents Document Sharing Hub
Full document details: NFPA 730 2023

(3) Building exterior walls and portals that are designated as secured and controlled

11.3.2.2.1 Where feasible, there should be designated parking areas for the following:

(1) Staff
(2) Students
(3) Visitors
(4) Vendors
(5) Bus loading/unloading

11.3.2.2.2 Designated parking areas should be clearly distinguishable and protected through the use of signage and/or physical or electronic security barriers such as gates or security posts.

11.3.2.3 All portals in the building perimeter should be controlled in accordance with Section 7.5.

11.3.2.4 The building perimeter should have dedicated portals for the following occupants:

(1) Students
(2) Staff
(3) Visitors
(4) Vendors

11.3.2.4.1 The student portal(s) should have the following controls in place:

(1) Visual monitoring by a staff member or volunteer during student arrival and dismissal times
(2) Locks to prevent entry except at arrival and dismissal times

11.3.2.4.2 The staff portal(s) should be locked at all times with entry requiring a valid key/credential.

11.3.2.4.3 Entry at the visitor and vendor portal(s) should be controlled by one or more of the following:

(1) Monitoring by a staff member or volunteer
(2) Electronic access control

11.3.3 Interior. (Reserved)

11.3.4 Portal Control.

11.3.4.1 Portals in security perimeters should comply with Section 7.5.

11.3.4.2 Procedures should be established for collecting keys/credentials from terminated employees, employees on vacation, and student residents who have vacated the premises.

11.3.4.3 Keys/credentials should not be identified in a manner such that a person finding a lost key/credential could trace it back to the school.

11.3.4.4* The degree of portal control should be a function of the campus layout and the needs shown in the SVA.

11.3.4.5 The portal control system should be designed to meet life safety and fire code regulations, as well as legal requirements for accessibility by people with disabilities.

11.3.4.6 At a minimum, all exterior portal windows and sidelights should be designed to prevent or delay entry if the glazing is attacked.

11.3.4.7* All classroom doors should be equipped with locking hardware that allows for a single motion egress as defined by NFPA *101*.

11.3.4.7.1 All classroom-locking hardware should be lockable from inside the classroom without special knowledge, tools, or credentials.

11.3.4.7.2 All classroom-locking hardware should be unlockable from the hallway side with a key or credential.

11.3.4.8 Classroom door sidelights should be located on the hinge side of the door and be designed not to allow unauthorized persons from breaking the sidelight glass and accessing the door locking hardware.

11.3.4.9 Classroom door sidelights and door windows should be designed so that if the glass is broken, a person cannot gain access to the interior of the classroom.

11.4* Crime Prevention Through Environmental Design (CPTED).

11.4.1 Crime and Loss Prevention. (Reserved)

11.4.2* Human Behavior. A code of conduct that clearly defines each regulation and assigns a specific penalty for each infraction should be developed, publicized, and strictly enforced.

11.4.3 Lighting.

11.4.3.1 Lighting should comply with Section 8.4.

11.4.3.2 The following areas should be illuminated in addition to those areas listed in Section 8.4:

(1) Corridors
(2) Stairwells
(3) Elevators

11.4.4* Landscaping. Foliage and shrubbery should be trimmed and maintained.

11.4.5 Aesthetics. (Reserved)

11.5 Security Systems. The installation of electronic premises security systems should be in accordance with Section 9.4.

11.5.1 Contraband Detection. (Reserved)

11.5.2 Personnel Safety Alerting Systems.

11.5.2.1 Emergency Communication System.

11.5.2.1.1 Emergency communication systems should comply with *NFPA 72* and applicable laws.

11.5.2.1.2* Educational facilities should have a communication policy and a communication method for providing information on safety and crime.

11.5.2.1.3* Educational facilities should have an established policy on communication with local emergency responders.

11.5.2.2 Holdup, Duress, Ambush, and Man Down Alarms. Holdup, duress, ambush, and man down alarms should comply with the requirements of NFPA 731.

11.5.2.3 Threat, Door, and Miscellaneous Alarms. Threat and door alarms and other alarms relating to the safety of people should be monitored by security personnel.

Documents 2023 Edition Document Sharing Hub
Full document details: NFPA 730 2023

11.5.3* Property Protection Monitoring Systems. The installation of electronic premises security systems should be in accordance with Section 9.4.

11.5.3.1 Asset Tracking. (Reserved)

11.5.3.2* Intrusion Detection Systems. Intrusion detection systems should comply with 9.4.2.

11.5.3.3* Access Control Systems. Access control systems should comply with 9.4.3.

11.5.3.4* Video Surveillance Systems. Video surveillance systems should comply with 9.4.4.

11.6 Accessory Property.

11.6.1 Parking. Parking should comply with Section 10.2.

11.6.2* Campus Housing. Based upon the need shown in the SVA, schools that provide housing for students should provide a security program for residence halls, including, but not limited to, the following:

(1) Training students regarding their security responsibilities and role in maintaining the integrity of the security program
(2) Requiring that the exterior portals to residence halls be restricted or guarded at all times
(3) Limiting access to residence halls through the smallest number of portals possible (without conflicting with life safety requirements)
(4) Requiring that one key/credential be used to gain entrance into the residence hall and another key/credential into student rooms; using machine readable credentials programmed for residence hall access and limited access to the proper student room; or requiring the use of two-factor authorization for access to student rooms
(5) Immediately re-keying whenever a student room key/credential is lost or deactivating machine-readable credentials when lost
(6) Having security patrols check that accessible doors and windows to the common areas are locked at night
(7) Having rules, verification, and enforcement to address the propping open of doors by students for convenience (e.g., self-closers on doors and local alarms that sound when doors are left propped open)
(8)* Providing a means for visitors to contact residents from the main entrance
(9) Requiring that visitors, vendors, contractors, and delivery persons be escorted at all times in residence halls
(10) Requiring that visitors, workers, and delivery persons always wear identification badges in residence halls
(11) Having special security procedures for housing students during low-occupancy periods, such as holidays and vacation periods

11.6.3* Educational Research Laboratories. Based upon need shown in the SVA, a security program for research laboratories should include but not be limited to the following:

(1) Training faculty and students in the proper handling and security of sensitive, hazardous, or dangerous materials
(2) Fostering a security culture with respect to laboratories and sensitive materials
(3) Controlling access to laboratories and material storage areas to essential personnel
(4) Establishing effective inventory control and handling processes
(5) Providing facilities to secure sensitive materials
(6) Electronically monitoring laboratories and storage areas with sensitive materials
(7) Providing increased or dedicated security patrols of research areas
(8) Providing reliable means for laboratory occupants to alert security personnel to off-normal events such as an accidental material release, materials theft, and intrusion/duress situation
(9) Providing proper disposal of sensitive, hazardous, or dangerous materials

Chapter 12 Health Care

12.1 General.

12.1.1 Scope. This chapter addresses measures to mitigate security vulnerabilities in health care facilities.

12.1.2 Security Plan.

12.1.2.1* A health care facility should have a security management plan.

12.1.2.2 A security vulnerability assessment (SVA) should be conducted for the health care facility as part of the security plan.

12.1.2.2.1 The SVA should evaluate the potential security risks posed by the physical and operational environment of the health care facility to all assets in the facility.

12.1.2.2.2 The facility should implement procedures and controls in accordance with the risks identified by the SVA.

12.1.3 Responsible Person.

12.1.3.1 A person(s) should be appointed by the management of the health care facility to be responsible for security management activities.

12.1.3.2 The duties of the responsible person(s) should include but not be limited to the following:

(1) Providing identification, as shown by review of the SVA, for patients, staff, and other people entering the facility
(2) Controlling access into and out of security-sensitive areas as identified in the SVA
(3) Defining and implementing procedures for the following situations:
    (a) Security incident
    (b) Hostage situation
    (c)* Bomb
    (d) Criminal threat
    (e) Labor action
    (f) Disorderly conduct
    (g) Workplace violence
    (h) Restraining orders
    (i) Infant or pediatric abduction
    (j) Situations involving VIPs or the media
    (k) Ensuring access to emergency areas
    (l) Active shooter(s)
(4) Providing security at alternative care sites or vacated facilities
(5) Controlling vehicular traffic control on the facility property

AVA Documents Document Sharing Hub
Full document details: NFPA 730 2023

(6) Protecting the facility assets, including property and equipment
(7) Establishing a policy for interaction with law enforcement agencies
(8) Ensuring compliance with applicable laws, regulations, and standards regarding security management operations
(9) Putting into place education and training of the facility security force to address the following:
    (a) Customer service
    (b) Use of physical restraints
    (c) Use of force
    (d) Response criteria
    (e) Fire watch procedures
    (f) Lockdown procedures
    (g) Emergency notification procedures

12.2 Administrative Controls.

12.2.1 People Management.

12.2.1.1 Employees. Employee screening should comply with 6.2.1.

12.2.1.2 The Public. Public visitation controls should be enforced.

12.2.1.2.1 After-hours entrance by the public should be restricted to designated areas such as entrance lobbies and emergency departments.

12.2.1.2.2 Health care facility security controls and procedures should comply with life safety requirements for egress.

12.2.1.3* The Media. The security management plan should include procedures to accommodate media representatives.

12.2.1.3.1 A person should be designated to serve as media contact and representative for the organization in regard to media interactions.

12.2.1.3.2 An area should be designated for assembly of media representatives.

12.2.1.3.2.1 A security or facility staff member should remain with the media representative(s) at all times.

12.2.1.3.2.2* Media representatives should be escorted when granted access to the health care facility outside of the area designated in 12.2.1.3.2.

12.2.1.4* Crowd Control.

12.2.1.4.1 The security management plan should provide procedures for control of a crowd demanding access to a health care facility.

12.2.1.4.2 The procedures for managing crowd control should provide for coordination and collaboration of security and law enforcement.

12.2.1.5 Security Personnel.

12.2.1.5.1 The use of security personnel should comply with 6.2.4.

12.2.1.5.2 Security personnel in health care facilities should have additional training, including but not limited to the following:

(1) Customer service
(2) Emergency procedures
(3) Patrol methods
(4) De-escalation training
(5) Use of physical restraints
(6) Use of force

12.2.2 Material Receiving. The receipt of materials into a health care facility should comply with Section 6.3.

12.3 Security Perimeters.

12.3.1 Area Designations.

12.3.1.1 Areas identified in the SVA should be classified in accordance with Sections 7.1 and 7.2.

12.3.1.2 The areas in 12.3.1.2.1 through 12.3.1.2.7 should be classified as controlled or restricted.

12.3.1.2.1 Emergency department security should include but not be limited to appropriate protection such as the following:

(1)* A visible security presence
(2) A private duress alarm at the nurse's station and reception for summoning immediate assistance
(3) An access-controlled treatment area
(4) A lockdown procedure to secure the area when conditions threaten the viability of the department
(5) Bullet-resisting glazing material as shown by review of the SVA

12.3.1.2.2 Pediatric and infant care areas should have a security plan for the prevention of and response to pediatric and infant abduction, including but not limited to appropriate protections such as the following:

(1) Controlling and limiting access by the general public
(2) Screening by nursing staff of persons seeking access to infant care areas
(3) Establishing a protocol with staff clearance to match infants with their parents
(4) Establishing a system to monitor and track the location of pediatric and infant patients
(5)* Requiring facility alert system, lockdown, and staff inspection of all packages leaving the premises
(6) Using electronic monitoring, tracking, and access control equipment
(7) Using an automated and standardized facility-wide alerting system to announce pediatric or infant abduction
(8) Using remote exit locking or alarming
(9) Establishing facility lockdown procedures and requiring staff inspection of all persons and packages leaving the premises
(10) Prohibiting birth announcements by staff
(11) Ensuring detection of the presence of nonidentified individuals, which constitutes a security breach
(12) Requiring the movement of infants to bassinets only, no hand carries
(13) Requiring unique identification or uniforms for health care staff
(14) Setting up secure storage of scrubs and uniforms, both clean and dirty
(15) Providing education about pediatric and infant abduction as follows:
    (a) To familiarize health care staff with infant abduction scenarios
    (b) To let parents know not to leave a child or infant unattended or in the care of an unidentified person

Documents 2023 Edition Document Sharing Hub
Full document details: NFPA 730 2023

(16) Informing visiting family and friends that they are not permitted to enter any nursery area with an infant or newborn from the outside
(17) Conducting infant abduction drills periodically to test effectiveness of chosen measures

12.3.1.2.3* Medication storage and work areas should be secured against admittance of unauthorized personnel through the use of the following:

(1) Physical access control
(2) Unique identification for the area
(3) Secure storage and controlled dispensing of drugs

12.3.1.2.4 Clinical and research laboratories should be secured against admittance of unauthorized personnel through appropriate protections such as the following:

(1) Physical access control
(2) Unique identification for the area
(3) Secure storage and controlled dispensing of regulated chemical, biological, and radiological materials

12.3.1.2.5 Dementia and behavioral health units should be secured against the admittance or release of unauthorized personnel or contraband through appropriate protections such as the following:

(1) Physical access control
(2) Unique identification for the area
(3)* A procedure to prevent entry of contraband prior to a person being admitted into the unit or department
(4) Elopement precautions
(5) Information in patient files to aid in identification

12.3.1.2.6 Forensic patient treatment areas should provide appropriate protections such as the following:

(1) Law enforcement attending the patient at all times
(2) Treatment performed in an area separate from other patients
(3) Restraints applied or removed only under forensic staff control

12.3.1.2.7 Communications, data infrastructure, and medical records storage areas should be secured against the admittance of unauthorized personnel or unauthorized release of confidential information through the use of appropriate protections such as the following:

(1) Physical access control
(2) Unique identification for the area
(3) Surveillance equipment
(4) Data encryption and password protection

12.3.2 Exterior Perimeters. The security plan should include processes and procedures for controlling access to the health care facility.

12.3.3 Interior Perimeters. (Reserved)

12.3.4 Portal Control. Entrances to health care facilities should comply with Section 7.5 for portal control.

12.4 Crime Prevention Through Environmental Design (CPTED).

12.5 Security Systems. The installation of electronic premises security systems should be in accordance with Section 9.4.

Chapter 13 Reserved

Chapter 14 Lodging

14.1 General.

14.1.1* Scope. This chapter addresses measures to mitigate security vulnerabilities in lodging facilities.

14.1.2 Security Plan.

14.1.2.1* A lodging facility should have a security management plan.

14.1.2.2 A security vulnerability assessment (SVA) should be conducted as part of the security plan for a lodging facility.

14.1.2.2.1 The SVA should evaluate the potential security risks posed by the physical and operational environment of the lodging facility to all assets in the facility.

14.1.2.2.2 The facility should implement procedures and controls in accordance with the risks identified by the SVA.

14.2 Administrative Controls.

14.2.1* People Management.

14.2.1.1 Employees.

14.2.1.1.1 Employee screening should comply with 6.2.1.

14.2.1.1.2 Staff should be trained in security and emergency procedures.

14.2.1.1.3 Staff should wear photo identification badges.

14.2.1.1.4 Staff should be instructed to report suspicious activities to management.

14.2.1.2 Guests. Guests should receive warning of criminal activity in and around the facility.

14.2.1.3 Vendors and Contractors. Vendors and contractors should comply with 6.2.3.

14.2.1.4 Security Personnel.

14.2.1.4.1 The decision to provide security personnel should be based on the SVA.

14.2.1.4.2 Security personnel should comply with 6.2.4.

14.2.1.4.3* Security patrols should be conducted in accordance with the facility security plan.

14.2.2* Material Receiving. The receipt of materials should comply with Section 6.3.

14.2.3 Information and Data Security. Front desk personnel should be trained in guest privacy and security procedures, including but not limited to those outlined in 14.2.3.1 through 14.2.3.6.

14.2.3.1 Front desk personnel should not announce guest room numbers when registering guests or calling for staff.

14.2.3.2 Identification should be required of guests at check-in.

14.2.3.3 Front desk personnel should control issuance of guest room keys/credentials.

AVA Documents Document Sharing Hub
Full document details: NFPA 730 2023

14.2.3.3.1 A history log of guestroom key/credential distribution should be maintained.

14.2.3.3.2 Identification should be requested for the reissuance of room keys/credentials.

14.2.3.3.3* Guest keys/credentials should be retrieved or expire at check-out.

14.2.3.4 Guests should show identification to retrieve fax or written messages.

14.2.3.5 Phone calls to guest rooms should be connected to the room without the room number being identified.

14.2.3.6 Folios, credit card numbers, and other guest information should be kept confidential.

14.3 Security Perimeters.

14.3.1 Area Designations.

14.3.1.1 Areas identified in the SVA should be classified in accordance with Sections 7.1 and 7.2.

14.3.1.2* Access to the property should be monitored or controlled.

14.3.1.3* Unauthorized persons should be evicted from guest rooms and guest room corridors.

14.3.1.4* Nonpublic areas should be classified as controlled or restricted, including but not limited to the following:

(1) Kitchens
(2) Laundries
(3) Mechanical spaces
(4) Electrical distribution rooms

14.3.2 Exterior.

14.3.2.1* Exterior entrances other than the main lobby entrance(s) should have automatic door closers and locks.

14.3.2.2 Exterior doors should comply with 7.5.2.

14.3.2.3 The exterior of the facility should be regularly checked for the following:

(1) Signs of vandalism
(2) Transients or vagrants living on or around the property

14.3.3 Interior.

14.3.3.1 Guest room doors and windows should comply with the following:

(1) Applicable federal, state, and local requirements regarding locks and latches
(2) Solid wood or steel construction
(3) Frames made of steel or otherwise reinforced, with the clearance between the door and the frame less than ⅛ in. (3.175 mm)
(4)* Deadbolts on entry doors
(5)* Auxiliary locking device on entry doors
(6) Individual room re-keying whenever a key/credential is reported lost or stolen
(7) Housekeeping personnel pick up keys/credentials left in rooms by guests and return them to the front desk as soon as possible
(8)* Door viewer
(9) Locking devices on operable windows and windows or doors that face balconies, terraces, and gardens
(10) Connecting-room doors provided with 1 in. (25.4 mm) deadbolts capable of being unlocked from inside the protected guest room side only

14.3.3.2 Guest rooms should be provided with 24-hour telephone service.

14.3.3.3 Guests should receive notice of the availability of safe deposit boxes.

14.3.3.4 Guests should be provided with brochures or other material offering safety and security tips.

14.3.4 Portal Control.

14.3.4.1 Portals in security perimeters should comply with Section 7.5.

14.3.4.2 Procedures should be established for collecting keys/credentials from terminated employees, employees on vacation, and guests who have vacated their rooms.

14.3.4.3 Hotel keys/credentials should not be identified in a manner such that a person finding a lost key/credential could trace it back to the hotel.

14.4* Crime Prevention Through Environmental Design (CPTED).

14.4.1 Crime and Loss Prevention. Management should be informed of crime trends in and around the facility by taking the following measures:

(1) Researching the history of violent and property crime in the immediate neighborhood and on the premises in the past 3 years
(2) Developing a relationship with local law enforcement agencies to make them familiar with the property
(3) Requesting that local police include the facility in their patrol routes
(4) Maintaining communication with local police to keep informed of crime and crime trends in the neighborhood or area
(5) Participating in local security associations or industry trade groups as a means of sharing common security concerns and solutions

14.4.2 Human Behavior. (Reserved)

14.4.3 Lighting.

14.4.3.1 Lighting should comply with Section 8.4.

14.4.3.2 The following areas should be illuminated in addition to those areas listed in Section 8.4:

(1) Corridors
(2) Stairwells
(3) Elevators
(4) Access routes to public areas, including laundry rooms, exercise rooms, swimming pools, and so forth

14.4.3.3 Lights in public areas, including laundry rooms, exercise rooms, and vending areas, should be controlled by tamperproof switches.

14.4.4 Landscaping. (Reserved)

14.4.5 Aesthetics. (Reserved)

14.5 Security Systems. The installation of electronic premises security systems should be in accordance with Section 9.4.

Documents 2023 Edition Document Sharing Hub
Full document details: NFPA 730 2023

14.5.1 Contraband Detection. (Reserved)

14.5.2* Personnel Safety Alerting Systems. Elevator cars should have means to allow seeing inside the car before entrance.

14.5.3 Property Protection Monitoring Systems.

14.5.3.1 Asset Tracking. (Reserved)

14.5.3.2 Intrusion Detection Systems. (Reserved)

14.5.3.3 Video Surveillance.

14.5.3.3.1 The lobby and front desk areas should have video surveillance.

14.5.3.3.2 Routes to public areas, including laundry rooms, exercise rooms, swimming pools, and so forth, should have video surveillance.

14.6 Accessory Property, Parking. Parking should comply with Section 10.2.

Chapter 15 Multi-Dwelling Unit Buildings

15.1 General.

15.1.1* Scope. This chapter addresses measures to mitigate security vulnerabilities in multi-dwelling unit buildings of more than three units.

15.1.2 Security Plan.

15.1.2.1* A residential facility should have a security management plan.

15.1.2.2 A security vulnerability assessment (SVA) should be conducted as part of the security plan for a residential facility.

15.1.2.2.1* The SVA should evaluate the potential security risks posed by the physical and operational environment of the facility.

15.1.2.2.2 The facility should implement procedures and controls in accordance with the risks identified by the SVA.

15.1.3* Property Management Responsibility.

15.2 Administrative Controls.

15.2.1 People Management.

15.2.1.1 Employees.

15.2.1.1.1* Employee screening should comply with 6.2.1.

15.2.1.1.2 Staff should be trained in security and emergency procedures.

15.2.1.1.2.1 Staff should record identification information for prospective tenants prior to showing rental units.

15.2.1.1.2.2* Security procedures should include instructions on safety precautions when showing units.

15.2.1.1.3* Staff should be instructed to report suspicious activities to management.

15.2.1.2* Residents.

15.2.1.2.1 Residents should receive security plan procedures and policies that relate to resident safety.

15.2.1.2.2 Residents should sign a statement attesting to their receipt of the information required in 15.2.1.2.1.

15.2.1.2.3 Residents should receive warning of criminal activity in and around the facility.

15.2.1.3* Vendors and Contractors.

15.2.1.4 Security Personnel.

15.2.1.4.1 The decision to provide security personnel should be based on the SVA.

15.2.1.4.2 Security personnel should comply with 6.2.4.

15.2.1.4.3* Security patrols should be conducted in accordance with the facility security plan.

15.2.2 Material Receiving. (Reserved)

15.2.3 Information and Data Security. (Reserved)

15.2.4* Workplace Violence.

15.3 Security Perimeters.

15.3.1 Area Designations.

15.3.1.1 Areas identified in the SVA should be classified in accordance with Sections 7.1 and 7.2.

15.3.1.2 Nonpublic areas should be classified as controlled or restricted, including but not limited to the following:

(1) Dwelling units
(2)* Common spaces separated from public entry lobbies
(3)* Roofs
(4) Laundry rooms
(5) Exercise rooms

15.3.2 Exterior.

15.3.2.1* Exterior entrances to common areas should have automatic door closers and locks.

15.3.2.2 Exterior doors should comply with 7.5.2.

15.3.2.3 Exterior-accessible openings should be protected against forcible entry, including but not limited to the following:

(1) Basement doors
(2) Accessible windows
(3) Air-conditioning units
(4) Doors to balconies
(5) Exterior doors of dwelling units

15.3.2.4 Bars or gates on windows or doors of dwelling units should be designed to allow emergency egress in case of fire.

15.3.3 Interior.

15.3.3.1 Entry doors to dwelling units should have a door viewer.

15.3.3.2* Entry doors to dwelling units should be of solid-core construction.

15.3.4 Portal Control.

15.3.4.1 Portals in security perimeters should comply with Section 7.5.

AVA Documents Document Sharing Hub
Full document details: NFPA 730 2023

15.3.4.2 Procedures should be established for collecting keys/credentials from terminated employees, employees on vacation, and vacated tenants.

15.3.4.3 Locks on doors to rental units should be replaced or re-keyed/credentialed when there is a change in tenancy.

15.4 Crime Prevention Through Environmental Design (CPTED).

15.4.1 Crime and Loss Prevention. Neighborhood crime experience evaluation should include but not be limited to the following criteria:

(1) Location of property (i.e., urban, suburban, or rural area)
(2) The crime rate in the area
(3) Recent incidents of crime in the immediate neighborhood and on the premises
(4) Location of commercial establishments nearby that will attract shoppers and outsiders
(5) The extent of the local police presence
(6) The existence of a Neighborhood Crime Watch program

15.4.2 Human Behavior. (Reserved)

15.4.3 Lighting.

15.4.3.1 Lighting should comply with Section 8.4.

15.4.3.2 The following area should be illuminated in addition to those areas listed in Section 8.4:

(1) Corridors
(2) Stairwells
(3) Elevators
(4) Access routes to common areas such as laundry rooms, exercise rooms, and storage rooms

15.4.4* Landscaping.

15.4.5 Aesthetics. (Reserved)

15.5 Security Systems. The installation of electronic premises security systems should be in accordance with Section 9.4.

15.5.1 Contraband Detection. (Reserved)

15.5.2* Personnel Safety Alerting Systems. Elevator cars should have means to allow users to see inside the car before entering.

15.5.3 Property Protection Monitoring Systems

15.5.3.1 Asset Tracking. (Reserved)

15.5.3.2 Intrusion Detection Systems. Where an intrusion detection system is installed, residents should receive written instructions on how to operate the system.

15.6 Accessory Property, Parking. Parking should comply with Section 10.2.

Chapter 16 Restaurants

16.1 General.

16.1.1 Scope. This chapter addresses measures to mitigate security vulnerabilities in restaurant establishments.

16.1.2 Security Plan.

16.1.2.1 A restaurant should have a security management plan.

16.1.2.2* A security vulnerability assessment (SVA) should be conducted as part of the security plan for a restaurant.

16.1.2.2.1 The SVA should evaluate the potential security risks posed by the physical and operational environment of the facility.

16.1.2.2.2 The facility should implement procedures and controls in accordance with the risks identified by the SVA.

16.2 Administrative Controls.

16.2.1 People Management.

16.2.1.1 Employee screening should comply with 6.2.1.

16.2.1.2* Staff should be trained in security and emergency procedures.

16.2.1.2.1* Management should establish a policy of nonresistance and give it top priority in a training program.

16.2.1.2.2* Delivery personnel should be instructed not to enter any location where they feel threatened or unsafe and to hand over all goods and cash if threatened.

16.2.1.3* Delivery orders should be verified by a telephone number identification system.

16.2.2 Material Receiving. (Reserved)

16.3 Security Perimeters.

16.3.1 Area Designations.

16.3.1.1 Areas identified in the SVA should be classified in accordance with Sections 7.1 and 7.2.

16.3.1.2 Access to employee-only areas should be controlled.

16.3.2* Exterior. Garbage areas and external walk-in freezers or refrigerators should be located to enhance the safety of employees who use them.

16.3.3 Interior.

16.3.3.1 Goods at high risk to burglary, such as meats and alcoholic beverages, should be stored in a locked closet, security cage, or locked freezer.

16.3.3.2* Cash should be secured during non-business hours in a burglary-resistant safe or vault or other means as determined by the SVA.

16.3.3.2.1 The safe combination should be guarded by limiting the distribution to the minimum number of people requiring access.

16.3.3.2.2 The combination should not be written in an easily accessible place such as on a desk blotter.

16.3.3.2.3 The combination number should be changed on a regular basis.

16.3.4 Portal Control.

16.3.4.1* Other than entry doors, doors should be locked at all times.

16.3.4.2 Locked doors should comply with Section 7.5.

Documents 2023 Edition Document Sharing Hub
Full document details: NFPA 730 2023

16.4* Crime Prevention Through Environmental Design (CPTED).

16.4.1 Crime and Loss Prevention.

16.4.1.1* Cash on the premises should be kept at the lowest possible amount required to conduct business.

16.4.1.2* The elements of a security program to control burglary should include but not be limited to the following:

(1) Physical security devices
(2) Burglary-resistant safes
(3) Intrusion detection systems

16.4.2 Human Behavior. (Reserved)

16.4.3 Lighting.

16.4.3.1 Lighting should comply with Section 8.4.

16.4.3.2* The entrances and the interior of the premises should be illuminated.

16.4.4 Landscaping. (Reserved)

16.4.5* Aesthetics. Product displays, posters, and advertisements in windows should not obstruct visibility into or out of the premises.

16.5 Security Systems. The installation of electronic premises security systems should be in accordance with Section 9.4.

16.5.1 Contraband Detection. (Reserved)

16.5.2 Personnel Safety Alerting Systems. (Reserved)

16.5.3 Property Protection Monitoring Systems.

16.5.3.1 Asset Tracking. (Reserved)

16.5.3.2 Intrusion Detection Systems.

16.5.3.2.1* The safe, security closet, or security cage should be protected by the alarm system.

16.5.3.2.2 The alarm system should be periodically tested and properly maintained.

Chapter 17 Shopping Centers

17.1 General.

17.1.1* Scope. This chapter addresses measures to mitigate security vulnerabilities in shopping centers.

17.1.2 Security Plan.

17.1.2.1* A shopping center should have a security management plan.

17.1.2.2 A security vulnerability assessment (SVA) should be conducted as part of the security plan for a shopping center.

17.1.2.2.1 The SVA should evaluate the potential security risks posed by the physical and operational environment of the shopping center to all assets in the facility.

17.1.2.2.2 The facility should implement procedures and controls in accordance with the risks identified by the SVA.

17.1.2.3 Individual tenants should comply with the recommendations of the applicable occupancy chapter(s).

17.1.3 Responsible Person. The duties of the person responsible for security should include but not be limited to the following:

(1) Development of policies and procedures
(2) Risk assessment
(3)* Implementation of security measures
(4)* Law enforcement liaison
(5)* Emergency procedures
(6) Security staffing

17.2 Administrative Controls.

17.2.1 People Management.

17.2.1.1 Employees.

17.2.1.1.1 Employee screening should comply with 6.2.1.

17.2.1.1.2 Staff should be trained in security and emergency procedures.

17.2.1.2* Tenants. Tenants should be notified of significant security-related incidents.

17.2.1.3 Security Personnel.

17.2.1.3.1* The decision to provide security personnel should be based on the SVA.

17.2.1.3.2 Security personnel should comply with 6.2.4.

17.2.1.3.3* Security patrols should be conducted in accordance with the facility security plan.

17.2.1.3.4 Patrols should be conspicuous, since the emphasis is on deterrence rather than apprehension.

17.2.2 Material Receiving. The receipt of materials should comply with Section 6.3.

17.3* Security Perimeters.

17.3.1 Area Designations.

17.3.1.1 Areas identified in the SVA should be classified in accordance with Sections 7.1 and 7.2.

17.3.1.2 Access to employee-only areas should be controlled.

17.4* Crime Prevention Through Environmental Design (CPTED).

17.4.1 Crime and Loss Prevention. (Reserved)

17.4.2 Human Behavior. (Reserved)

17.4.3* Lighting. Lighting should comply with Section 8.4.

17.4.4* Landscaping.

17.4.5 Aesthetics. (Reserved)

17.5 Security Systems. The installation of electronic premises security systems should be in accordance with Section 9.4.

AVA Documents Document Sharing Hub
Full document details: NFPA 730 2023

17.5.1 Contraband Detection. (Reserved)

17.5.2 Personnel Safety Alerting Systems. (Reserved)

17.5.3 Property Protection Monitoring Systems.

17.5.3.1 Asset Tracking. (Reserved)

17.5.3.2 Intrusion Detection Systems. (Reserved)

17.5.3.3* Video Surveillance.

17.6* Accessory Property, Parking. Parking should comply with Section 10.2.

Chapter 18 Retail Establishments

18.1 General.

18.1.1 Scope. This chapter addresses measures to mitigate security vulnerabilities in retail establishments.

18.1.2 Security Plan.

18.1.2.1* A retail establishment should have a security management plan.

18.1.2.2 A security vulnerability assessment (SVA) should be conducted as part of the security plan for a retail establishment.

18.1.2.2.1 The SVA should evaluate the potential security risks posed by the physical and operational environment of the retail establishment to all assets in the facility.

18.1.2.2.2 The facility should implement procedures and controls in accordance with the risks identified by the SVA.

18.1.2.3* The elements of a security program to control robbery should include but not be limited to the following:

(1) Control of cash
(2) Access control
(3) Security equipment
(4) Personnel
(5) Employee training

18.2 Administrative Controls.

18.2.1 People Management.

18.2.1.1 Employees.

18.2.1.1.1 Employee screening should comply with 6.2.1.

18.2.1.1.2 Staff should be trained in security and emergency procedures.

18.2.1.1.2.1 A policy of nonresistance should be established and given top priority.

18.2.1.1.2.2 Employee training should include but not be limited to the following:

(1)* What to do before, during, and after a robbery
(2) How to be an effective witness through observation and reporting of details, events, and descriptions
(3) Proper use of security equipment, especially holdup alarm systems
(4) Procedures to follow in detaining or arresting shoplifters
(5) Check cashing procedures
(6) Credit card acceptance procedures
(7) Detection of counterfeit currency

18.2.1.1.3* Employee theft should be managed by using procedures and devices, including but not limited to the following:

(1) Arranging work flow and task assignments so that the work of one employee acts as a control on that of another employee
(2)* Dividing responsibilities and functions so that no one employee has control over all facets of a transaction
(3) Reducing the exposure of inventory to pilferage by keeping storage areas clean and unobstructed
(4) Implementing a program of regular and random (surprise) inventory checks, audits, and petty cash counts
(5) Using devices such as video surveillance to control theft
(6) Securing expensive items to limit opportunity for theft

18.2.1.2 Customers.

18.2.1.2.1* Shoplifting Prevention. A program against shoplifting in retail establishments should consist of procedural controls and policies consistent with laws and ordinances.

18.2.1.2.2 Check Fraud.

18.2.1.2.2.1* For those retail establishments that accept checks, a check acceptance policy should be established.

18.2.1.2.2.2 Elements of a check acceptance policy should include but not be limited to the following:

(1) Requiring two forms of identification
(2) Listing identification on the back of the check
(3)* Not accepting third-party checks
(4) Using an electronic check verification system

18.2.1.2.3* Credit Card Fraud. Retail establishments should establish a credit card payment policy.

18.2.1.2.4 Counterfeit Currency. Retail businesses should have equipment used to detect counterfeit currency.

18.2.1.3* Contractors and Vendors. Access by contractors and vendors should be monitored by management.

18.2.1.4 Security Personnel.

18.2.1.4.1* The decision to provide security personnel should be based on the SVA.

18.2.1.4.2 Security personnel should comply with 6.2.4.

18.2.1.4.3* Security patrols should be conducted in accordance with the security plan.

18.2.1.4.4 Patrols should be conspicuous, since the emphasis is on deterrence rather than apprehension.

18.2.2 Material Receiving. The receipt of materials should comply with Section 6.3.

18.2.3 Information and Data Security. (Reserved)

18.2.4* Workplace Violence. Retail establishments should have a workplace violence prevention program in accordance with Section 6.5.

18.3 Security Perimeters.

18.3.1 Area Designations.

18.3.1.1 Areas identified in the SVA should be classified in accordance with Sections 7.1 and 7.2.

18.3.1.2 Access to employee-only areas should be controlled.

Documents 2023 Edition Document Sharing Hub
Full document details: NFPA 730 2023

18.3.2* Exterior. Garbage areas should be located to enhance the safety of employees who use them.

18.4 Crime Prevention Through Environmental Design (CPTED).

18.4.1 Crime and Loss Prevention.

18.4.1.1* Cash on the premises should be kept at the lowest possible amount required to conduct business.

18.4.1.2* Means to mitigate loss from burglary or theft should include but not be limited to the following:

(1) Physical security devices
(2) Burglary-resistant safes
(3) Intrusion detection systems

18.4.1.3* Cash should be secured during non-business hours in a burglary-resistant safe, vault, or other means as determined by the SVA.

18.4.2 Human Behavior. (Reserved)

18.4.3* Lighting. Lighting should comply with Section 8.4.

18.4.4* Landscaping. Foliage and shrubbery should be trimmed and maintained.

18.4.5* Aesthetics. Product displays, posters, and advertisements in windows should not obstruct visibility into or out of the store.

18.5 Security Systems. The installation of electronic premises security systems should be in accordance with Section 9.4.

18.5.1 Contraband Detection. (Reserved)

18.5.2 Personnel Safety Alerting Systems. (Reserved)

18.5.3 Property Protection Monitoring Systems.

18.5.3.1 Asset Tracking. (Reserved)

18.5.3.2* Intrusion Detection Systems. When an intrusion detection system is installed, it should also protect the safe, security closet, or security cage.

18.5.3.3* Video Surveillance.

18.6* Accessory Property, Parking. Parking should comply with Section 10.2.

Chapter 19 Office Buildings

19.1 General.

19.1.1* Scope.

19.1.1.1 This chapter addresses measures to mitigate security vulnerabilities in office buildings.

19.1.1.2* Buildings operated by federal, state, or local government that have tenants, including law enforcement agencies, court-related agencies and functions, or government records and archives, or that have tenants that perform functions critical to national security are not within the scope of this chapter.

19.1.2 Security Plan.

19.1.2.1* Office buildings should have a security management plan.

19.1.2.2 A security vulnerability assessment (SVA) should be conducted as part of the security plan.

19.1.2.2.1 The SVA should evaluate the potential security risks posed by the physical and operational environment of the office building to all assets in the building.

19.1.2.2.2 The office building management should implement procedures and controls in accordance with the risks identified by the SVA.

19.1.2.2.3 Regardless of the measures utilized, security should not conflict with fire or life safety code requirements.

19.1.2.3 The security plan should synchronize with emergency response, disaster, and business recovery plans.

19.1.3 Responsible Person.

19.1.3.1 A person(s) should be appointed by the management of the office building property to be responsible for security management activities.

19.1.3.2 The duties of the responsible person(s) should include but not be limited to the following:

(1) Establishing security measures for exterior areas, common interior areas, and parking areas
(2) Implementing access control at basement-, ground-, and street-level entrances and exits
(3) Implementing a key/credential control program
(4) Setting up training and supervision of security personnel
(5) Carrying out employee background checks and drug testing
(6)* Reviewing local neighborhood crime trends

19.2* Administrative Controls. Emergency telephone numbers and building management contact information should be posted.

19.2.1 People Management.

19.2.1.1 Employees and Tenants.

19.2.1.1.1 Employee practices should comply with 6.2.1.

19.2.1.1.2* Employees and tenants should be instructed how to exercise reasonable care in protecting personal property.

19.2.1.1.3* Employees and tenants should receive training on their roles in the security plan.

19.2.1.1.4* Tenants should be notified of significant security-related incidents.

19.2.1.1.5 Where identification badges are provided, tenants should display identification badges as recommended in 6.2.1.2 for employees.

19.2.1.2 Visitors.

19.2.1.2.1* When an office building, or portion thereof, is a secure area as designated in the security plan, visitors should enter through a monitored and designated visitor entrance(s) and identify the person they are visiting.

19.2.1.2.2 Visitors should be issued a visitor badge.

19.2.1.2.2.1 To be issued a visitor badge, visitors should be required to show government-issued, photo identification to a staff member.

AVA Documents Document Sharing Hub
Full document details: NFPA 730 2023