Public Comment No. 1-NFPA 730-2018 [Chapter 11]

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.

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

(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.

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

Statement of Problem and Substantiation for Public Comment

We support committee action to retain the present location of Chapter 11 content for education facility guidance NFPA 730. We believe that the broad principles contained in Chapter 11 should be enforceable; NOT spun off to an annex in NFPA 731 where they are NOT enforceable. The education industry -- where we have tenure as an authoritative voice -- is an industry that is dealing with significant security risks. (We do not see substantiation by the submitter for making this change, either).

Related Item

• Public Input No. 27-NFPA 730-2018 [Chapter 11]

Submitter Information Verification

Submitter Full Name: Michael Anthony
Organization: Standards Michigan
Affiliation: STANDARDSMICHIGAN.COM
Street Address:
City:
State:
Zip:
Submittal Date: Thu Nov 15 14:06:47 EST 2018
Committee: PMM-AAA

Committee Statement

Committee Action: Rejected
Resolution: The Technical Committee retains the text of Chapter 11 in NFPA 730.

Public Comment No. 2-NFPA 730-2018 [Chapter 12]

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

(4) Providing security at alternative care sites or vacated facilities

(5) Controlling vehicular traffic control on the facility property

(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 non identified 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

(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.

Statement of Problem and Substantiation for Public Comment

We support committee action to retain the present location of Chapter 12 content for education facility guidance NFPA 730. We believe that the broad principles contained in Chapter 12 should be enforceable; NOT spun off to an annex in NFPA 731 where they are NOT enforceable. The education industry -- where we have many university affiliated healthcare systems and tenure as an authoritative voice -- is an industry that is dealing with significant security risks. (We do not see substantiation by the submitter for making this change, either).

Related Item

• Public Input No. 28-NFPA 730-2018

Submitter Information Verification

Submitter Full Name: Michael Anthony
Organization: Standards Michigan
Affiliation: WWW.STANDARDSMICHIGAN.COM
Street Address:

City:
State:
Zip:
Submittal Date: Thu Nov 15 14:23:04 EST 2018
Committee: PMM-AAA

Committee Statement

Committee Action: Rejected
Resolution: The Technical Committee retains the text of Chapter 12 in NFPA 730.