

00712 Building Security

Part 1: General

- 1.01 The following guideline discusses security features and arrangements that are recommended for campus buildings and facilities.
- 1.02 During the design process for new NC State buildings and assessment phase of proposed renovations of existing facilities, the designer, the Facilities Planning and Design Project manager, and the primary occupants shall review security needs with the Campus Police Crime Prevention Officer and consider installation of a security infrastructure to control access of persons, vehicles, and movable assets. This infrastructure may employ various technologies such as card access, closed circuit television or other means as outlined below in the design guideline sections. Recognizing the cost associated with implementing many of these technologies, the design team and building occupants must balance the issue of cost versus the need for enhanced security. It is the joint responsibility of the occupants represented by the building committee, Deans, and Department Heads to make recommendations about the level of security required. These decisions should be reached through consultation and deliberation with Campus Police.

Part 2: Design Guidelines – Security Infrastructure

2.01 **Basic Security Measures for Specified Types of Facilities/Areas**

Types of NC State Facilities/Areas:

Category One - Remote Campus Facilities

Category Two – Core Campus (North, Central, South, Centennial, and West Precincts)

Category Three - General Administrative Offices, Academic Buildings, Athletic Facilities

Category Four - Maintenance and Support Facilities, Information and Technology Areas, Security Areas, Mail Facilities, Telecommunication areas

Category Five - Student Housing, Executive Offices, Pulstar Reactor, Laboratory and Chemical Storage Areas

2.02 **Category One - Remote Campus Facilities**

Category One is classified as a site that is owned by the University but is not patrolled by Campus Police. The following measures are recommended:

Perimeter

- Some type of natural or structural barrier may be in place at the site such as a controlled access gate.
- The site must be clearly posted as an NC State University facility and appropriately posted to prevent trespassing or unauthorized site access.

Building/Structure

- A monitored Intrusion Detection System electronic alarm system containing magnetic contacts on exterior/perimeter doors and/or office areas and motion detection or detectors strategically placed inside should be considered. Access to the alarm system control panel must be secured in such a manner that the panel and wiring are protected from viewing and tampering by unauthorized personnel. This system should be activated at the end of normal business hours and de-activated at the start of normal business hours.
- Installation of adequate locks for exterior doors to buildings and doors to office areas in multi-tenant facilities.
- A minimum light level of 0.5 foot-candles in all outside areas utilized by faculty and students. Facility entrances require 10.0 ft. candles.
- Signage in accordance with the Campus Signage Manual installed at all entrances to facilities and buildings.

Parking Lots/Areas

- A minimum light level of 0.5-foot candles in all outside areas utilized by faculty and students.
- Landscaping selected and placed so that opportunities for concealment are minimized.
- Signage in accordance with the Campus Exterior Signage Manual installed at entrances to the property.

2.03 Category Two – Core Campus (North, Central, South, Centennial, and West Precincts)

Category Two is classified as the General Grounds of the core campus that is patrolled by Campus Police. The Security measures recommended for consideration include those from Category One plus the following:

- A CCTV system designed to monitor strategic areas of parking lots, all exterior building card access doors 24-hours per day, and primary assembly or perimeter areas.
- Parking facilities should have “Blue Light” emergency telephones located at intervals of approximately 300 feet. They should be located at avenues of approach and egress from major facilities.

2.04 Category Three - General Administrative Offices, Academic Buildings, Athletic Facilities

Category Three is classified as General Administrative Offices, Academic Buildings and Athletic Facilities. The Security measures recommended include Categories One and Two plus the following:

- A card access system containing magnetic contacts on exterior/perimeter doors to buildings and/or office areas should be installed. Access shall be initiated by magnetic stripe or proximity card and cards shall be treated the same as keys. Access to the alarm system control panel must be secured in such a manner that the panel and wiring are protected from viewing and tampering by unauthorized personnel.
- A telephone or intercom system should be installed on the outside of certain exterior card access door locations in close proximity to the card access reader. This system may be used to contact building occupants in the event exterior doors are locked.
- A card access control should be placed on the access door to all data/telecom rooms within these facilities.
- The facility should be sited and arranged so that the main building entrance should be easily identifiable from roads, pathways, and parking areas that service the facility.
- Buildings should have one primary entrance. All other entrances should be considered secondary entrances.
- If secondary entrances are required, they should be configured to move persons to the main entrance through public spaces. Secondary entrances should not allow access to private interior spaces, other than through the main entrance lobby.
- Building main entrances should contain a lobby or other area that may accommodate a security checkpoint.
- Required ground level emergency egress doors should be labeled “emergency exit only” and secured against building entry.
- Building lobby spaces should be designed so that there is a clear delineation between public and private spaces. Public spaces include restrooms, shared conference rooms, 110 classrooms or vending spaces. Private spaces include elevators, offices, stairs or research laboratories. Access to private spaces must be through a securable portal.
- From the designated lobby security checkpoint, there should be a clear line of sight to elevators, lobby restroom access, stair access, building entrance, and access points to private areas.
- Building interiors should be compartmentalized so that public and private spaces may be easily secured and maintained separate from each other.
- Building elevators and stairwells must be securable to limit access to sensitive area or building floors.

2.05 Category Four – Maintenance and Support Facilities, Information and Technology Areas, Security Areas, Mail Facilities, Telecommunication Areas

Category Four is classified as Maintenance and Support Facilities, Information Technology Areas, Mail Facilities, Telecom Areas and Security Areas. The security measures recommended for these types of facilities include all categories listed prior to this plus the following.

- A duress button (s) connected to the alarm system should be placed in high-risk areas.
- CCTV monitoring of areas handling cash transactions should be considered.
- CCTV should be considered to monitor critical interior card access doors.

2.06 Category Five – Student Housing, Executive Areas, Nuclear Reactor, Laboratories

Category Five is classified as student housing, executive areas, the Nuclear Reactor, laboratory and chemical storage areas, and other critical areas. In addition to Categories One, Two, Three and Four, the following security measures should be taken.

- Card Access readers should be placed on these areas. These areas should be monitored with a CCTV system and permission levels for these areas should be kept to a minimum.

2.07 Summary :

Category	Type	Security Measures
One	<ul style="list-style-type: none"> ▪ Remote Campus Facilities (facilities too far from main campus for security patrols) 	<ul style="list-style-type: none"> ▪ Perimeter barriers (natural and structural) ▪ Lighting ▪ Intrusive Detection System
Two	<ul style="list-style-type: none"> ▪ General Grounds – Core Campus 	<ul style="list-style-type: none"> ▪ Includes Category One ▪ CCTV monitoring of areas of assembly ▪ Emergency Call Phones
Three	<ul style="list-style-type: none"> ▪ General Administrative Offices ▪ Academic Buildings ▪ Athletic Facilities 	<ul style="list-style-type: none"> ▪ Includes Category One and Two ▪ Electronic Access Control ▪ Exterior door locks ▪ Visitor Control Points ▪ Telecom Protection ▪ Intercoms for Exterior access doors ▪ CCTV Monitor of parking lots and card access doors
Four	<ul style="list-style-type: none"> ▪ Maintenance and Support Facilities ▪ Information Technology areas ▪ Mail Facilities, Telecom areas ▪ Security areas 	<ul style="list-style-type: none"> ▪ Includes Categories One, Two and Three ▪ Duress button(s) in high risk areas ▪ CCTV monitoring of duress button area ▪ Card access on Telecom areas, including hub rooms
Five	<ul style="list-style-type: none"> ▪ Student Housing ▪ Executive Offices ▪ Nuclear Reactor ▪ Laboratory Areas ▪ Other critical areas 	<ul style="list-style-type: none"> ▪ Includes Categories One, Two, Three, and Four ▪ Limited Card Access with CCTV monitoring of doors