3.5 SECURITY AND LIFE SAFETY STANDARDS

3.5.1 DESIGN FOR SECURITY

3.5.1.1 General

References:

- Crime Prevention through Environmental Design (CPTED) Guidebook: http://www.ncpc.gov.sg/pdf/CPTED%20Guidebook.pdf

It is a priority for George Mason University to create a safe and secure environment for its users. The guidelines below shall be followed:

- Adhere to the Crime Prevention through Environmental Design (CPTED) principles in all designs in accordance with the Crime Prevention through Environmental Design Guidebook, October 2003 edition.
- Increase security and crime prevention through the use of environmental controls. These controls include natural surveillance, natural access control, territorial reinforcement and maintenance as outlined below:
    - Natural Surveillance: Maximize visibility with strategic placement of architecture and physical elements.
    - Natural Access Control: Place entrances, exits, fencing, landscaping and lighting to control movement of people and vehicles.
    - Maintenance: Maintain landscaping, buildings, lighting, etc. in order to maintain visibility, preserve pride in ownership and continue declaration of ownership.
- In planning for security and crime prevention, the following design principles must be addressed (see the CPTED Guidebook for more information):
    - Natural Surveillance
    - Natural Access Control
    - Territorial Reinforcement
    - Maintenance and Management
- Within these principles, the following strategies must be evaluated and employed:
    - Sight Lines: Provide clear sightlines that allow unobstructed views to the maximum degree possible. Minimize dead space and blind spots. Carefully consider camera angles to maximize the coverage area for each camera.
    - Lighting: Lighting shall support a safe and secure campus environment. Address areas of deep shadowing, but avoid over-lighting and consider energy use.

- Concealed or Isolated Routes: These are to be minimized. If they are required for specific design reasons, provide these areas with appropriate lighting and camera coverage.
- Entrapment Areas: All designs shall avoid these areas.
- Isolation: Areas that are isolated from the rest of the campus environment shall be carefully designed to provide an adequate secure environment within and from/to these spaces. Isolated spaces should otherwise be avoided.
- Land Use Mix: Planning of the campus shall evaluate the location of various functions and encourage mixed land uses.
- Activity Generators: Entrances to buildings and areas that encourage people to gather should be spaced and adjoin other outdoor spaces in order to create active pathways and avoid unintended isolated areas.
- Ownership, Maintenance and Management: It must be clear who has oversight and responsibility for all spaces and security measures in any facility or area of the campus.
- Signs and Information: Signage and wayfinding must indicate safe zones and locations to get help when needed.

- Other factors to be considered include:
  - Vehicular barriers to prevent easy access to areas not intended for vehicles.
  - The impact of landscape design on the security of spaces in and around buildings.
  - The location and security of parking areas. Underground parking is to be designed carefully and should include best practices for perimeter control and structural considerations. Parking near a building is subject to scrutiny.

3.5.1.2 Building Access

- Refer to Part 4, Division 08 70 00 – Hardware.
- All lockable doors on campus are required to have a key bypass
- The Architect is responsible for specifying the lock core (per University system); the University is responsible for keying
- The card key system must be coordinated with the University Security Systems Manager.
- Best Cores are employed University-wide, Access control Access IT Universal are employed University-wide for card access.
- Electronic card access is generally preferred
- All buildings that contain laboratories, scene shops or art studios, or maintenance buildings where chemicals are used, must be equipped with electronic access.
- All hazardous waste and hazardous substance bulk/stock storage rooms must be keyed to the Environmental Health and Safety (EHS) Hazardous Waste Key.

- Security closets and telecom (inclusive of server spaces) rooms should have electronic card access
- Low use spaces, that are normally locked, are good candidates for wireless locking systems; conversely, high volume spaces are not well suited for wireless locks
- Access card closet must comply with UL Listings, and accommodate a 4x8 plywood area for install.
- All access systems need to have backup power and battery available.
- All doors must allow unrestricted egress at all times. Requirements for specific access points include:
    - Primary Entrances
        - Allows egress at all times
        - Card access reader
        - Electronic locking hardware
        - Door position switch
        - Request-to-exit detector
    - Secondary Entrances
        - Electronic locking hardware
        - Door position switch
        - Request-to-exit detector
        - Local alarm sounder, only as designated by University
    - "Exit only" doors
        - Door position switch
        - Local alarm sounder, only as designated by the university
        - Integrated Request-to-exit detector
- Magnetic locks are not permitted
- Padlocks a must be able to accept a George Mason University standard core.
- Building entrances shall be numbered. A street address shall be provided on the building in a visible location.

3.5.1.3 Surveillance Camera Systems

- Within building interiors, provide a camera every 2,700 square feet, as determined by George Mason University for precise locations.

- For exterior space, provide camera surveillance at every entrance, every lot (as determined by Mason), and all garages.

3.5.1.4 Building Systems Security

RESERVED

3.5.1.5 Emergency Notification System

- Electronic message boards
- Emergency telephones

3.5.1.6 Parking

- Parking has separate gate security requirements

3.5.2 DESIGN FOR LIFE SAFETY

3.5.2.1 General

References:

- CPSM: http://dgs.virginia.gov/DivisionofEngineeringandBuildings/BCOM/CPSM/tabid/402/Default.aspx

3.5.2.2 Fire Safety and Emergency Preparedness

3.5.2.2.1 Mass Notification Sign Infrastructure

- The lobby entrance should have at least one Ethernet port supplied with power (power over Ethernet) and at least one 120 Volt electrical outlet installed for future mass notification signage. The Ethernet and electrical boxes should be installed at least eight feet high in the building lobby where users can see the sign. The associated wall system should be reinforced with wood blocking that will be capable of supporting mass notification sign and/or a large screen 52 inch LCD television set.

3.5.2.2.2 Commercial Cooking Hood Systems

- There should be a hose bib with hot water, and power connection on the same level as the exhaust fans for the hood exhaust system.
- All electrical shunts, gas shutoff valves, and other associated shut off devices should be labeled.
- All Type I hoods should be protected by a wet-chemical suppression system.

3.5.2.2.3 Pitched Roofs

- Fire detection or suppression equipment that is located on a pitched roof must have the appropriate tie-offs and guide rails to facilitate a safe ascent to and descent from the equipment. Fall protection such as tie-offs and guide rails shall be in accordance with OSHA standards.