# SCDMV Facilities Security Plan Guide

## Purpose

Provide a strategic guide for facility compliance and to be used to improve the Security for any SCDMV facility that may receive or process a component of the DL/ID.

## Scope

Develop a check list for areas of concern for all SCDMV buildings, storage areas and other areas perceived vulnerable to theft and provide recommendations to remedy the findings.

### SCDMV FACILITIES:

A. **External structure**

1. **Physical location**

   a. Is the location of the facility in an area that could benefit from frequent night time patrols from local Law Enforcement agencies?

   **Recommendation:** For every office, contact local Law Enforcement Agencies to schedule regular night time patrols. They should also be provided a contact point within DMV in case of any irregularities.

2. **Building construction**

   a. Are the perimeter walls solid and provide adequate resistance?

   **Recommendation:** If the building is constructed of metal or wood, re-enforcements should be added to protect interior areas not covered by a motion sensor.

3. **Lighting**

   a. Is there adequate night lighting that would discourage loitering after hours?

   b. Does the lighting provide coverage for all sides of the building?

   **Recommendation:** If there is installed lighting for the building, check for adequate coverage and operation. If there is no outside lighting explore adding them. In locations that have after hours loitering the law enforcement patrols will be valuable.

4. **Landscaping**

   a. Is the shrubbery trimmed away from windows and doors to provide clear visibility from a distance?

**Recommendation:** All shrubbery should be trimmed away from doors and windows on a regular schedule. This shrubbery should be trimmed at a height that allows full visibility of all doors and window by a drive by patrol.

5. **Windows**

    a. Are the windows of a solid nature incorporated into the structure of the building?
    b. Are there wood or metal panels below the glass?
    c. Are they constructed in a manner to allow them to be opened?
    d. Do the windows have intrusion detection devices installed or adequately covered by a motion sensor?

    **Recommendation:** If the windows are solid and cannot be opened then check for easy entry via panel below the window, this panel should be reinforced or the room should be covered by a motion sensor. If the window is an aluminum crank out style or a household two panel slide up style then they should be secured by either a motion sensor or an intrusion detection device.

6. **Secure employee entrances**

    a. Is the door constructed of a material to provide resistance from a forced entry attempt?
    b. Does the door have a window?
    c. Is entry controlled by HID and PIN panel?
    d. Does this door self close and lock at all times?
    e. Is the security code or entry method changed when employees transfer or leave DMV?
    f. How many employees have the access code or key to this entrance?

    **Recommendation:** Entry into the building by employees should be a two step process, possession and knowledge. The entry door should be constructed of metal within a metal frame and have a working door closure device installed. A motion sensor should cover this door. If it is not possible to have the key pad entry should be periodically changed and especially after there have been employee changes. An inventory should be taken to determine the actual number of employees who have access to the facility and should include the mobile or floating employees. This list should be maintained by the office manager.

7. **Unsecured entrances**

    a. Are these doors constructed of a material to provide resistance from a forced entry attempt?
    b. Do these doors have a window or are they constructed of glass?
    c. Are these doors secured via a dead bolt locking system?

d. How many employees have a key to these doors?

**Recommendation:** This door should have a security door contact device installed along with a dead bolt lock and be within a few steps from a motion detector.

8. **Shared Facility**

a. Do other agencies have access to the DMV work area?
b. Is there a common outside door to all areas?
c. Does this other agency(s) operate 24 X 7?
d. Who Is in charge of overall building security and do they know of SCDMV's security requirements and security system?
e. Are the internal walls secure from intrusion?

**Recommendations:** Typically these facilities fall in to two categories, (1) DMV is located in a government building with close proximity to other agencies and most often law enforcement close by, or (2) DMV shared with non-government tenants.

In both cases caution should be taken so that the DMV area is secure from ceiling or internal wall entry and that the doors are protected by security contacts. A motion detector in the ceiling crawl space and ample motion detectors covering the doors should be explored as an option to secure DMV's area.

## B. SCDMV Internal structure

1. **Security System**

a. Is there a documented policy and plan of action when the Security system is triggered?
b. Is the Security system centrally monitored after hours to insure the alarms have been activated?
c. Does the Security system provide wireless or a dedicated communication line?
d. Does the Security system operate when there is a power loss?
e. Is the eternal audible alarm accessible so it could be easily disabled?
f. Is the audible alarm monitored by the security system?
g. Is there a Panic Button for DMV employees that tie into the Security system?

**Recommendations:** A SCDMV position paper on their current and future security requirements should be written and then compared to the current security system. A panic button should be considered for offices that are apart from other buildings and in isolated locations. This panic button should be connected to the security system to provide a silent alarm. The documented policy and plan of action would trigger the appropriate response to this alarm.

The current building security system is polled once a night to determine if the system is connected and operating, it is possible to cut the phone line and the system would not be aware of this event until it is polled from the Blue Ridge central office and then only report a data loss notification. This practice needs to be reviewed.

2. **Location of motion sensors**
    a. Are the motion sensors positioned to provide adequate coverage of all external doors and windows?

**Recommendations:** Verify that the location and the range of the motion detectors will provide total coverage of windows and doors.

3. **Security keypad**
    a. How many employees or contractors know the security code?
    b. Are the custodial companies bonded and formally notified of SCDMV security policies?

**Recommendations:** Each local DMV facility should take an inventory of employees and contractors believed to have access to the security code, key or any other method to enter the office. This inventory should then be reconciled with SCDMV facility managements list. If this cannot be accomplished then the code/ key should be changed and reissued on a need to know basic and a name log should be kept.

There should be a current review of the custodial companies under contract. Bonding and insurance information should be part of this review. The custodial company should be made aware of DMV’s security policies.

4. **Public Access to DMV secure areas**
    a. Is there easy public access to secure DMV work areas?
    b. Are the secure credentials protected from public access?

**Recommendations:** In facilities where the public restroom is located in the DMV work area, access to other DMV area should be controlled by closing and locking doors.

If the printers cannot be moved away from public access then the printer manufacture should be contacted about a cover for the output card hopper. This cover would limit direct and easy access to ID cards being printed.

C. **Secure Area**

1. **Secure storage area**
    a. Is there a designated area for secure supplies?
    b. Is there a dropped ceiling above the secure storage area?
    c. How is the access limited to this area?
    d. Is the facility safe located in this area?
    e. Is this area protected by a motion sensor?
    f. Is there a lockable and secure door to this area?
    g. Who has access to this area?

**Recommendations:** A secure storage area should be provided for each office. This area should contain the safe, be protected by a tamper resistant door and be monitored by a motion sensor. If the room has any way to gain access to it (ceiling/wall) other than through the door then the secure room needs to have a motion sensor located in the room.

D. **Secure Documents**

1. Are all secure documents locked in the safe at night?
    a. DL/ID cards, titles, other designated valuables.
2. Is the safe of adequate size to store all DL/ID cards, Titles, Laminates and currency?
3. Are the documents to be returned to Blythewood kept in the secure area and separate from employee common areas?

**Recommendations:** A new policy should be developed that requires all secure documents be kept in the safe. In conjunction with this new policy each office will need to be polled to determine if the current safe will be of adequate size to store all the secure items.

The documents that are scheduled to be returned to Blythewood for destruction should be kept out of the general work area and in the secure room until the day of the courier pick up.