SECURITY SCREENING PROCEDURES

Directive: 12 – 110

Date of Issue: March 2017 Amends/Cancels: 12-110, July 2013

I. PURPOSE

The purpose of this Directive is to provide guidance to members of the Department of General Services, Maryland Capitol Police (MCP) in regards to checking the Security Cards of employees and identification of visitors entering Department of General Services Facilities.

II. POLICY

All members of MCP will strictly adhere to procedures outlined within this Directive. This will be done in order to preserve the safety and security of those who work at or visit DGS managed facilities.

It is important that all personnel conduct the screening process in the directed manner at all times. To do otherwise creates confusion among those entering our facilities leading to questioning of our staff as to the method employed. All members of MCP will conduct themselves in the most courteous and professional manner when dealing with the public as well as tenants.

III. DEFINITIONS

A. VISITOR MANAGEMENT SYSTEM - The Visitor Management System, consisting of Desktop Computer, and ID Scanner, is a tool that was implemented in order for the Department to provide adequate security for our facilities which do not have standard screening equipment, i.e., x-ray machines and walk-through-scanner. It allows the person's information to be checked against our internal database for persons that have been banned from entering our facilities for security reasons.

B. VALID FORMS OF IDENTIFICATION – Valid identification is defined as either:

1. A State Security Card issued by DGS, or

2. A Valid Government Issued Photo Identification, which would include the following:

   a. US Passport or Passport Card;

   b. Foreign Passport w/ supporting documents;

   c. US Certificate of Naturalization;

d. US Certificate of US Citizenship;

e. US Citizens Card;
f. Permanent Resident Card;

g. Federal Employment Authorization Document Card that contains a photo(Form I-766);

h. Out of State US photo driver's license, learner's permit, or identification card;

i. US Territory or Canadian photo driver's license, learner's permit or identification card;

j. Maryland issued non-driver identification card, driver's license or learner's permit;

k. US Military ID or dependent card with photo; and

l. Federal, State or local Law Enforcement Identification.

IV. PROCEDURES

A. GENERAL PROCEDURES AND RESPONSIBILITIES

1. Once the building is opened all pedestrian traffic will enter by way of the main entrance. The MCP employee posted at the door will check the Security Cards or valid photo identification of those entering the building.

2. MCP personnel will examine Security Cards and photo identification cards closely enough to be able to positively identify the photo as being that of the person presenting the card in question. If the photo is of such poor quality that a positive identification is not possible, the identification card will not be accepted.

3. Exceptions:

    a. The four constitutional officers for Maryland (Governor, Lieutenant Governor, Comptroller and Attorney General) and their immediate family will be granted unchallenged entry.

    b. Those being escorted by MSP executive protection or Legislative Services Security are presumed to have been pre-screened for any potential security risk.

4. Those refusing to stop and display the required identification should be considered a security risk.

    a. Supervision and additional units should be notified if the subject is unknown to the screening personnel.

b. Employees should not abandon their screening posts to chase those not displaying identification unless there is a clear and present danger to do so.

5. If an individual attempts to enter a building without showing their Security Card or valid photo identification they are to be stopped and access denied until such a time as they produce the proper identification and it is verified.

6. If access to a controlled area is limited to authorized personnel, only those authorized employees may be permitted to enter the area after proper identification has been confirmed.

B. SECURITY CARDS

1. State employees must wear the Security Card at all times while inside DGS owned or managed property.

2. State employees and contractors without a Security Card or valid photo identification will not be granted access without the verification of employment by their supervisor.

3. State employees are required to wear their State Security Cards on their outer garment in order to distinguish between visitors and employees.

4. When on State property employees must display the Security Card:

   a. In the area of the upper chest between waist and shoulders;

   b. So as to be visible at all times; and

   c. Produce the Security Card upon demand by a member of MCP.

5. Security Cards will not be:

   a. Placed in a holder or cover that impacts the viewing and examination of the Card;

   b. Loaned or allowed to be used by another individual for any reason; or

   c. Altered, copied, photographed, or reproduced; or

6. If MCP personnel observe the wearing of a Security Card in a manner inconsistent with this Directive, they will direct the card holder to display the card in the proper manner.

7. If a Security Card is damaged, worn, or the photography cannot be used to identify the bearer, the card holder should be advised to obtain a new Security Card.

8. Generally, access to buildings is restricted between 1700 hrs and 0730 hrs Monday through Friday and on weekends and holidays. State employees needing access during these hours must have early/late prox privileges on their Security Card or have special arrangements made with MCP three days in advance.

C. VIOLATIONS OF THE SECURITY CARD POLICY

1. MCP personnel who observe a card holder attempting to circumvent the screening process or violating this policy will report the incident to their supervisor.

2. An incident report will be completed detailing:

    a. The date, time and place of the incident;

    b. Identity of the card holder; and

    c. A copy will be forwarded to the building coordinator or supervisor authorizing the card holder to possess the Security Card.

3. Serious or repeat violations will result in the confiscation of the security card and loss of card access privileges.

D. EXPIRED SECURITY CARDS:

1. Expired Security Cards will be confiscated on the spot and the Shift Supervisor will be immediately notified;

2. An incident report will be generated, capturing the following:

    a. A copy of the Security Card will be attached; and

    b. The name of the company or department the Security Card was issued to will be listed.

3. The confiscated card will be turned in to the Security Card Processing Center personnel.

4. Unless it is determined that there will be a follow-up investigation, the individual who presented the confiscated Security Card will be required to produce other acceptable photo identification and be allowed entry as a visitor.

E. VISITOR SCREENING

1. Visitors without valid photo identification will not be granted access.

2. The government issued identifications listed in III, B. above will be accepted a valid identification.

3. If a visitor presents a form of valid identification, other than those delineated in III, B. above, the employee should notify their supervisor, who will inspect the identification and make a determination whether to grant or deny access.

4. Certain posts are equipped with a Visitor Management System (VMS). Visitor Identification from driver's licenses can be captured via scanner and compared to existing BOLO list. At these posts, the following procedures will be adhered to:

    a. Visitors will be asked to produce a valid identification as defined above.

    b. If presented with a driver's license, MCP personnel will scan the visitor identification into the VMS software. (Note: The scanner is designed to scan all 50 state's drivers licenses, however, with continuous changes to driver's license security features there may be errors when the information is captured during the scan).

    c. Once scanned to computer, MCP personnel will ensure that displayed visitor information matches that on driver's license. If there are any corrections required, MCP employee will manually correct visitor information.

    d. If scanner does not recognize driver's license data, or other Valid ID is presented; MCP personnel will manually enter visitor information.

    e. If scanner software alerts to a BOLO "hit"; MCP personnel will notify their supervisor of alert. Supervisor will respond to post and verify BOLO "hit" through dispatch/CAD/RMS records.

F. VISITOR PASSES

1. Visitor passes will be generated by the VMS.

2. The visitor pass will be worn on the outermost garment. MCP staff will ensure this procedure is followed before the visitor leaves the desk. Visitors will not be allowed or encouraged to place the pass on books, folders, brief cases etc., nor will they be allowed to just hold them.

2. MCP personnel will attempt to retrieve the pass prior to the visitor leaving for the day. This includes employees who were processed as visitors.

3. Persons who have been issued visitors passes including employees will be expected to show a valid photo identification card when navigating between State buildings this includes exiting and entering the same building for any reason.

4. MCP personnel are reminded that visitors' passes are easily transferable. Those looking to breach security could easily do so unless we are vigilant in checking our screening process.