Physical/Access Security

Standard Operating Procedures

Sample

Attachment #1

.

OSAM & SERVICE'S SPECTRUM MANAGEMENT OFFICES

PHYSICAL SECURITY PROCEDURES

1. Purpose: This directive adapts the procedures established in references (a) through (e) to the environment of the collocated facility, Suite 1200, xxxx VA. It is intended to provide guidance in the discharge of individual security responsibilities and to allow open storage collateral classified storage of systems, personal computers, storage media, and printed material classified Secret or below in the facility.

2. Applicability: This directive applies to all personnel (government and contractor) within the collocated facility. All personnel with the authority to open/close the secure area will be familiar with this SOP and acknowledge such at least once a year and will comply with DoD Facility Security Procedures. Services collocated are xxx agencies.

3. References:

a. DOD 5200.1-R, Information Security Program Regulations, January 97.
b. …
e. Collocation Memorandum of Agreement, August 1998

4. Policy:

a. Additional supplementation is authorized, if needed to satisfy requirements. Supplements may expand these rules, but may not be less stringent. Such supplements must be approved through the Chief of Security (D16) and in turn by the Facility Security Manager.

b. Compliance with the provisions outlined in this Instruction and its references is mandatory. Violations are subject to administrative or judicial sanctions, or both.

c. Each Service will appoint a security manager for their

respective areas. The Service Security Manager will be responsible to coordinate security issues with the Facility Security Manager. Each service will be responsible for security within their respective areas.

5. Procedures: This instruction supplements DOD 5200.1-R and xxx by amplifying the policies contained within and by providing procedural guidance, where appropriate, for application in the collocated facility.

6. Responsibilities: The protection of classified information is the responsibility of each individual assigned to the collocated facility who possesses or has knowledge of such information regardless of how it was obtained. Security directives do not guarantee protection and cannot be written to cover all conceivable situations. Therefore, basic security principles must be applied. The collection, recording, or removal of any classified material for personal use is prohibited in the interest of national security. Each Service is responsible for the proper protection of classified material within their area.

a. Facility Security Manager

(1). Maintain facility access roster.

(2). Prepare badge form for those requiring building access badges.

(3). Maintain a list of all temporary badges controlled by the Service Security Managers.

(4). Prepare the Daily Security Checklist.

b. Service Security Manager

(1). Provide the Facility Security Manager an access roster for their service with name and SSAN. Provide additions and deletions as required.

(2). Control the issue of temporary badges to permanent occupants and visitors.

(3). Maintain a roster for closing the facility during the respective services responsibility period.

c. Individuals

(1). Perform area security checks as scheduled.

(2). Perform closing procedures as required and as scheduled.

7. OPEN Procedures:

a. Review the opening procedures in the Daily Security Checklist notebook. If assistance is needed call the cognizant office at xxx and identify them that you are opening Alarm Area #??. It is not required that they be called.

b. Open the combination lock on the main entry door, room 1201. This door must be opened first because this is the location of the security alarm control panel.

c. Run your access badge through the card reader to release the door lock.

d. Disable the security alarm. (specifics)

e. Annotate the Security Container Check Sheet (SF 702).

f. Change the OPEN/CLOSED sign on the door to OPEN.

g. Occupants of rooms xxx, xxx, and xxx will open the combination locks on those access doors as required. These doors must be opened after the door to area xxx because the security alarm must be deactivated prior to opening these doors.

h. Change the OPEN/CLOSED sign on those doors to OPEN.

8. Facility Access

a. Assigned Personnel

(1). Permanent badges

(a). The Service Security Managers will provide a list of all personnel with unescorted access to the Facility Security Manager The list will contain full name and SSAN.

(b). The Facility Security Manager will prepare DD form 2248 for each individual requiring an access badge.

(c). The Facility Security Manager will maintain the Suite xxx access roster and update access control from individual badges. If personnel no longer require access to

suite xxx their security manager will notify the Facility Security Manager and their name will be removed from the access roster, their access badge deactivated for the suite 1200 card reader.

(2). Temporary badges

Temporary badges for the facility will be issued by the Facility Security Manager, the Service Security Managers or their designates. These badges will be coded to allow access to xxx. The security manager will maintain a log of badges issued on a temporary basis. These badges will be returned at the end of the day. These badges are for those assigned personnel who have forgotten or misplaced their badges. The individual will obtain a temporary building badge from the guard's desk at the entry to xxx. They will call their section from the the reception area for entry into suite xxx. The service security manager will issue them a temporary badge that is coded for entry into suite xxx.

b. Visitors

(1). Visitors that have their security clearance on file with the service security manager will be issued a NO ESCORT badge while they are in the facility. The Facility Security Manager and Service Security Managers will issue these badges. They will gain entry to the building by calling the party they are visiting and obtain a badge from the appropriate security manager. The security manager will prepare the entry log and record the badge number issued. The badge will be returned at the end of their visit or the end of the day

(2). All other visitors will be issued an ESCORT REQUIRED badge and must be accompanied by the escort while they are in the facility. The Facility Security Manager and Service Security Managers will issue these badges and maintain an entry log of all visitors and escorts. They will gain entry by calling the party they are visiting and obtain a badge from the appropriate security manager. The badge will be returned at the end of their visit or the end of the day.

9. Control of Classified Materials

a. Classified Documents: All hard copies of classified material will be marked to the appropriate security level. All classified documents must have a coversheet and protected from casual viewing. Whenever possible documents should be secured in a safe or secure storage room. Note: Documents classified TOP

SECRET or above are not authorized for open storage and must be secured within a safe certified for TOP SECRET storage.

b. Classified Media: All classified media will be appropriately marked. Whenever possible media should be secured in a safe or secure storage room. Media will only be processed on equipment that matches its classification. Note: Media classified TOP SECRET or above are not authorized for processing within this area.

c. Classified/Unclassified Equipment: All equipment will be marked with the classification level it is approved for.

(1). COMSEC
(2). Printer
(3). FAX
(5). UNCLASSIFIED: All equipment that does not fit one of the above categories will be marked for unclassified processing.

10. Office Sanitizing Procedures

(a). The escort for uncleared visitors will notify everyone in the immediate area that there is uncleared visitors entering the work area.

(b). Cover, turn face down, or store all classified material.

(c). Activate screen savers for classified computer monitors.

(d). Don’t discuss classified information in the area.

(e). Notify everyone entering the area that an uncleared visitor is in the area.

11. Alarm Integrity Check

Follow procedures in Attachment 1.

12. Emergency Evacuation

(a). Secure classified material in a locked container.

(b). Check surrounding area for classified material.

(c). Secure all entry doors.

(d). Follow procedures in Attachment 2

13. End of Day Security Check

Each service will perform an end of day security check for their respective area. The assigned service representative will perform the following duties:

(a). Check the area to ensure there is no classified material remaining in the work area. Classified papers, removable storage devices and magnetic media will be locked in a safe, secure storage room, or cabinet.

(b). Ensure all safes and secure rooms have been locked and Security Container Check Sheets (SF 702) have been annotated. Ensure all office doors are closed and locked.

(c). Check all areas for personnel remaining late.

(d). Turn out all lights in the area being checked. Each section will have one switch that controls all lights in that section.

(e). Complete the service’s area security check sheet. If personnel are remaining in the area after the end of the duty day turn the final security check over to them and have them sign the security check sheet. The individual accepting the security check sheet will be responsible for closing that area of the facility or passing the responsibility to someone remaining later.

(f). Secure the entry door to that area of the facility. Lock the combination lock on the door and check the door to be sure the combination lock is secure by running your access badge through the card reader to release the door lock. The door should not open if the combination lock is secure. Change OPEN/CLOSED sign on the outside of the door to CLOSED. Complete Activity Security Checklist (SF 701).

14. CLOSING Procedures

The person having closing responsibilities, as established in reference (e), will perform the following procedures:

(a). Obtain the Daily Security Checklist from the reception area.

(b). Check the entry door to each section. The door should be locked, the official visit log completed, and the OPEN/CLOSED sign changed to CLOSED. If these are not completed this would indicate that someone is remaining in the section. Obtain the signature of someone remaining in the facility on the Daily Security Checklist. This will be repeated as each person signing the checklist leaves for the day. The last person remaining in the facility will complete the Activity Security Checklist for their area.

(c). Make final check for anyone remaining in the area.

(d). Turn out lights in each area as it is checked.

(e). Arm the security alarm

(f). Lock the main entry door (room 1201) combination lock and check the lock by running your access badge through the card reader to make sure the door will not open.

(g). Change OPEN/CLOSED sign to CLOSED.

(h). Complete Activity Security Checklist

(i). Complete Security Container Check Sheet

(j). Return the Daily Security Checklist to the reception area.

(k). Call security at xxx and advise them that Alarm Area #?? has been secured. Be more specific here when you find out process, include validation scheme if there is one.

Attachment 1 – Alarm Integrity Check procedures
Attachment 2 - Occupant Emergency Plan.