Access Procedures and Guidelines for Information Technology (IT) Telecommunications (Telecom) Closets

A Mandatory Reference for ADS Chapter 545

Partial Revision Date: 09/14/2017
Responsible Office: M/CIO/IA
File Name: 545max_091417

Information System Security
Access Procedures and Guidelines
for Users, Help Desk Staff, System Administrators, System Owners and Information System Security Officers

1. Introduction

This document defines the processes for controlling access to USAID Information Technology Telecom closets that store and/or house information technology (IT) equipment (e.g., server rooms, network switches). This document does not apply to "restricted spaces" where end user classified processing is authorized and occurs.

2. Restricted Information Technology (IT) Closets

Any facility, room, or space that houses a USAID information system is a restricted IT closet. Any such area that houses infrastructure components (e.g., servers, network equipment, core telecommunications equipment, etc.) is referred to as a “restricted access IT closet.” The Bureau for Management, Office of the Chief Information Officer, Information Technology Operations (M/CIO/ITO) and the Bureau for Management, Office of the Chief Information Officer, Information Assurance Division (M/CIO/IA) have overall responsibility for authorizing access to the restricted IT spaces that contain their information systems.

3. Authorized Access List

M/CIO/ITO and M/CIO/IA must work with the Office of Security, AIDNet, or ClassNet Information System Security Officers (ISSOs) to ensure that they develop and maintain a list, referred to as an “authorized access list,” of the personnel authorized to have unescorted physical access to restricted IT spaces. There must be an authorized access list posted at every restricted IT closet.

ISSOs must post the authorized access list at the entrances to computer rooms, server rooms, and other restricted IT spaces. Each authorized access list must include personnel who are allowed authorized access, and personnel who must be contacted in an emergency. Only individuals on the authorized access list or escorted by staff on the authorized access list will be admitted to a restricted IT space.

The ISSO must review and update the access list as authorized personnel changes occur. At a minimum, the list must be reviewed annually and personnel who no longer require access must be removed from the authorized access list.

4. Visitor Logs

Visitor access logs are required where restricted IT closets exist. Visitor logs must record all persons entering the restricted IT space who do not have authorized access. For restricted IT closets housed in USAID facilities, such as the Continuity of Operations (COOP) center and the Ronald Reagan Building (RRB), the Office of Security (SEC) is responsible for maintaining these visitor logs. For information systems hosted outside of USAID facilities where restricted IT closets exist, System Owners (SOs) must check with SEC to find out who is responsible for maintaining the visitor logs. If SEC does not maintain logs for their facility, SOs must ensure, via contract language, that this task is performed.

The visitor log should include fields such as:

- Visitor's name;
- Visitor's signature;
- Visitor's company;
- Purpose of visit;
- If the restricted IT space visited is a computer room, you must include the name of the person who escorted the visitor to the room;
- Date and time of entry; and
- Date and time of exit.

5. Admitting Personnel

Personnel on the authorized access list may enter restricted IT spaces unescorted. Personnel with authorized access must make sure that visitors and maintenance personnel (escorted personnel) adhere to the following guidelines while in restricted IT spaces:

- **Visitors**: Visitors must have a valid purpose for entering a restricted IT space. All visitors must sign the visitor log prior to entering a restricted space. After signing, the visitor is assigned an escort who is related to the purpose of the visit. The escort admits the visitor to the restricted IT space. A staff member on the authorized access list must keep all visitors under continual visual observation while they are in the restricted IT space. Visitors must sign out upon leaving the restricted IT space.

- **Maintenance Personnel**: Maintenance personnel must follow the same admission procedures as visitors for restricted IT space. A staff member on the authorized access list must keep all maintenance personnel under continual visual observation while they are in the restricted IT space.

Only staff on the authorized access list for the restricted IT space may escort visitors. Personnel with authorized access are required to verify that personnel in restricted IT spaces who do not display proper credentials, or who are unescorted, are authorized for the space. Authorized personnel are responsible for escorting their visitors while the visitors are in restricted IT space.

545max_091417