



## UNIFORMED SERVICES UNIVERSITY OF THE HEALTH SCIENCES

4301 JONES BRIDGE ROAD  
BETHESDA, MARYLAND 20814-4712  
<http://www.usuhs.mil>



Office of the President  
PPM-015-2011 (CIO)

JAN 19 2012

### **SUBJECT: Implementation of Visitor Access Control and Common Access Card (CAC) Inspection Program**

**Purpose:** In accordance with the provisions of DoD Information Assurance Certification and Accreditation Process (DIACAP), this Presidential Policy Memorandum (PPM) establishes policies and procedures for monitoring visitor access throughout the campus and protection of network access utilities such as CAC.

**References:** (a) DoD Instruction 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP), November 28, 2007.  
(b) USU-CIO Memorandum, DIACAP Traditional Security Review, July 22, 2011.

**Applicability:** This memorandum applies to all USUHS students and employees (military and civilian).

**Policy:** This memorandum establishes the policies and procedures as follows:

1. Common Access Card (CAC) Audit:
  - a. Per ref (a), CACs must not be left unattended at any workstation to prevent security breaches.
  - b. The Information Assurance (IA) Division of the Network Operations and Communications (NOC) and Security Department (SEC) will conduct joint monthly inspections to monitor compliance. Violations will be dealt with using a 3-tiered response as follows:
    1. First violation: The IA team leaves a reminder card informing the user that his/her CAC was left unsecured along with a copy of the inspection memorandum.
    2. Second violation: The IA team takes the CAC and leaves a note informing the user that the CAC had been turned in to SEC. IA and SEC will maintain a record of all CACs that have been turned in and claimed by respective owners.
    3. Third violation: Same response as for the second violation, including supervisor notification for appropriate action.
  - c. CAC compliance issues will be included as an agenda item for Faculty Orientation briefings and Administrative Officers (AO), and Faculty Senate meetings (AO), and Faculty Senate meetings and Faculty Orientation briefings.


2. Visitor access control and monitoring:

- a. Sponsoring departments must escort visitors to SEC for badge issue and ensure an escort remains with the visitor while on campus.
- b. Visitors must prominently display their badges for the duration of their visit.
- c. Visitor sign in/out and badge turn-in process must be strictly enforced.
- d. Staff members are encouraged to politely request visitors to show their badges if they are not visible.
- e. Visitors requiring access to areas controlled by swipe card locks should be assisted by their sponsors to coordinate their visits with the respective departments. Visitors shall remain escorted during visits to such controlled areas.

**Responsibilities:**

1. The Chief, Information Assurance shall ensure that a monthly CAC audit is conducted randomly. Reports shall be furnished to the Chief Information Officer (CIO) within three days of audit completion.
2. The Director for Security shall:
  - a. Maintain custody and responsibility for the CACs recovered during the audit. Logs will be maintained to account for CAC turn-in and retrieval by users.
  - b. Ensure enforcement of the visitor access control and monitoring and provide reports to the chain of command, as necessary.

**Effective Date:** This PPM shall be effective from the date of signature.

  
Charles L. Rice, M.D.  
President