

AFMC makes important changes to CAC PIN policy

by Peter Kaye, public affairs specialist

7/14/2008 — **KIRTLAND AIR FORCE BASE, NEW MEXICO** (AFPN) — Air Force Materiel Command (AFMC) has released new policies designed to improve security on the AFMC networks and better protect our Air Force warfighters.

Phase 1 introduces a system where the personal identification number (PIN) on the Common Access Card (CAC) will be prompted to change based on the Information Operations Condition (INFOCON).

At INFOCON 5, the lowest INFOCON level, CAC PINs will not be prompted to change. AFMC network users are encouraged to change their PIN at least every six months, and especially if they feel there is a chance the PIN may have been compromised.

At INFOCON 4, CAC PINs will need to be changed every 90 days. At INFOCON 3, CAC PINs will need to be changed every 60 days. At INFOCON 2, CAC PINs will need to be changed every 30 days.

At INFOCON 1, the highest INFOCON level, CAC PINs will need to be changed every week.

Also, at INFOCON levels above 3, AFMC will randomly declare "Reset Days" where all users must reset the CAC PIN. At all levels, users will not be able to log into the AFMC networks when their CAC PIN is due to be reset.

Resetting the CAC PIN will require the network user to find a nearby CAC PIN Reset machine (CPR). These machines are located at the base Military Personnel Flight (MPF) and at helpdesks for the Client Support Administrators (CSAs) and Functional System Administrators (FSAs). To reset your CAC PIN, you will need a second form of photo ID (state driver's licenses, firearm permits, and Costco memberships are acceptable) and you will need to submit your fingerprint for personal identity verification. The process itself usually takes only 2-3 minutes. Wait times at MPF can be significantly higher depending on demand.

The virtual MPF (vMPF) website will not be available for CAC PIN resets.

Phase 2 involves changes to passwords for accounts that are excluded from CAC logon requirements. Those accounts, commonly used by CSAs and FSAs, will need to have their passwords changed at the same frequency as CAC PINs as introduced in phase 1. The password requirements will be:

Search

[Advanced Search](#)
[Week In Photos: 11/24/06](#)

[Featured AF Links](#)

- [AF 60th Anniversary](#)
- [AF Bandstand Player](#)
- [AF Posture Statement](#)
- [AF Media Center](#)
- [AF Mission](#)
- [AF Senior Leadership](#)
- [AF Symbol](#)
- [Airman Magazine](#)
- [Biographies](#)
- [BRAC 2005](#)
- [Deployed Newspapers](#)
- [Fact Sheets](#)
- [Senior Viewpoints](#)
- [Senior Leader](#)
- [Soundbites](#)
- [Week in Photos Gallery](#)
- [Why I Serve](#)

[Specials](#)

[Blue Summit Videos](#)

- 4 upper case letters (A,B,C)
- 4 lower case letters (a,b,c)
- 4 numbers (1,2,3)
- 4 special characters (!,@,#)
- Length must be between 16-20 digits
- May not contain words of more than three letters in any of the following languages: English, Spanish, French, German, Italian, Farsi, Russian, Chinese, Japanese, Portuguese, Arabic, Polish, Norwegian, Hindi, Lenape, Lakota, Pacific Islander dialects, Inuit, Swahili and Esperanto
- May not contain keyboard patterns (1QAZ, QWERTY, XDCFDV)
- Must be at least 75% different from your previous six passwords.

AFMC has stated that these changes will go very far towards protecting our modern warfighter, in the field as well as here at home, from threats on our Information Infrastructure.



Other Links

- [AAFES](#)
- [AF Crossroads](#)
- [AF Personnel Center](#)
- [AF Portal](#)
- [Air Force OneSource](#)
- [Army](#)
- [Citizen Airman](#)
- [DECA](#)
- [Defense Link](#)
- [Employer Support to the Guard and Reserve](#)
- [Freedom of Information Act \(FOIA\)](#)
- [Join the Air Force](#)
- [Marine Corps](#)
- [Multi-National Force - Iraq](#)
- [Navy](#)
- [No Fear Data](#)