VIRGINIA MILITARY INSTITUTE
Lexington, Virginia

GENERAL ORDER)
NUMBER 63) 28 June 2011

Access Card Control Policy

1. **Purpose**

The purpose of this policy is to provide guidance for obtaining and controlling access cards. The scope of this policy covers Access Cards only; metallic keys are addressed in General Order 56 (Key Policy). General ID card policies and procedures are covered in General Order 39 (ID Card Policy).

2. **Terms and Definitions**

a. VMI Access Card – serial-numbered, plastic access card issued to employees, cadets, and/or visitors. The VMI Access Card serves as the individual's "key" to the proximity (electric) locks the individual is granted access to. There are two types of access cards: a Picture ID access card that has a picture of the individual, and a Visitor Access Card that has no picture. Note: Any individual that has a picture ID VMI Access Card must also have a Colleague ID.

b. Keypad Locks – these locks are activated by a chip embedded in many VMI Access Cards. They have a keypad, a metallic lock, and may be proximity-enabled. These locks are not wired to a central computer database.

c. Computer Managed (CM) Locks –these locks are proximity-enabled, do not have a key pad or a metallic key lock, and are wired to a central computer database.

d. Electric Lock Coordinator – each building equipped with proximity (electric) locks has an Electric Lock Coordinator who is trained in the use of the proprietary software that controls the proximity locks at VMI.

e. Biometric Hand Reader – device that measures the physiological characteristics of an individual's hand and unlocks door(s) after making an automated comparison to a database of authorized personnel access.

f. Employees – For purposes of this policy, an employee is defined as any faculty, staff, or classified employee of VMI employed on a full- or part-time basis.

3. **Access Control**

a. Employees – Department Heads coordinate access for individuals they supervise through the Electric Lock Coordinator in the building(s) whre access is needed.

b. Cadets – at the beginning of each semester, faculty shall provide a by-name and by-class-section list of those cadets who require access to their Department Heads. Any access granted to cadets is temporary and must be reviewed no less than once a semester.

c. Visitors – in instances where a visitor will be on Post long enough for it to be advantageous to VMI for the visitor to be granted limited access to areas deemed essential, a Visitor Access Card may be issued.

4. **Lost or Stolen VMI Access Cards**

If a VMI Access Card is lost or stolen, the individual should immediately notify the VMI IT Help Desk to have the card deactivated. As with any theft, the VMI Police should also be notified.

5. **Recovery of VMI Access Cards from Departing Individuals**

a. Employee – the employee's immediate supervisor shall recover the VMI Access Cards from employees who are departing VMI and turn them over to their Department Head.

b. Cadets – The Commandant's Office shall recover the VMI Access Cards from cadets graduating or departing in the middle of a semester.

c. Visitor Access – The Building Coordinator shall recover the VMI Visitor Access Card from each visitor prior to that visitor's permanent departure from the VMI Post.

FOR THE SUPERINTENDENT:

Jeffrey H. Curtis
Colonel, USAF (Ret.)
Chief of Staff

OPR: IT
DIST: E

Attachment – Procedures

PROCEDURES

1. Areas of Responsibility and Issuing Office

- VMI Physical Plant -- Responsible for issuing all metallic keys. Keys shall only be issued after a Request for Key Issuance form is submitted in accordance with General Order 56 (General Key Policy). The VMI Physical Plant is responsible for maintenance of all access hardware not maintained by outside vendors.

- Human Resources Office -- Responsible for issuing Access Cards to everyone except cadets and visitors. Prior to issuing a Picture ID Access Card to an individual, the Human Resource Office shall update the ID Works and Colleague databases. Human Resources shall issue a maximum of ten (10) serial numbered Visitor Access Cards each to those Building Coordinators who have facilities with proximity locks.

- Office of Cadet Life – Responsible for issuing Access Cards to cadets. The ID Works database is automatically updated with the cadets' information when the card is printed.

- Department of Information Technology – Responsible for administering the Security Management System access software as well as the maintenance of cardholder information and credentials.

- Electronic Lock Coordinators – The Electric Lock Coordinator works for the Building Coordinator; however, he/she grants or restricts access to proximity locks and/or Biometric Hand Readers based on information provided by Department Heads.

  Additionally, the Electronic Lock Coordinator shall set the expiration date for the Access Card to match the date printed on the Access Card, with the exception of Visitor Access Cards. The Electronic Lock Coordinators shall also update the keypad locks. Electronic Lock Coordinators are not authorized to add, delete, or edit any cardholder or credential data. Electronic Lock Coordinators shall also work with the access system administrator to configure area definitions and schedules. Electronic Lock Coordinators shall conduct biannual inventories of access.

- Building Coordinators -- shall be issued a maximum of ten (10) Visitor's Access Cards and shall be responsible for activating and setting expiration dates on these cards. These cards shall be issued to the Building Coordinators by the Human Resources Office. Each Building Coordinator shall also be responsible for tracking their cards and performing periodic inventories of the cards. The Building Coordinator may exercise supervisory responsibility of the building and resolve any issues with access control in their building.

2. Access Control Permissions

- Employees – After receiving the Picture ID Access Card from Human Resources, the employee shall conduct a face-to-face meeting with the Electric Lock Coordinator where

the system is explained and access to authorized areas is enabled.

- Cadets – Obtain Access Card from the Office of Cadet Life.

- Visitors – The visitor shall conduct a face-to-face meeting with the Electric Lock Coordinator where the system is explained and access to authorized areas is enabled.

3. Lost or Stolen VMI Access Cards

- Employee -- report lost or stolen Access Cards to the VMI IT Help Desk as soon as possible, and no later than 24 hours after the incident. As with any theft, the VMI Police should be also notified.

- VMI IT Help Desk – after a report has been received, the VMI IT Help Desk will have the card deactivated.

4. Recovery of VMI Access Cards from Departing Card Holders

- Supervisor – Immediate supervisors shall recover VMI Access Cards from employees who are permanently departing VMI and turn them over to their Department Head.

- Human Resources – As a person is out processed by Human Resources, the card will automatically be deactivated in accordance with General Order 35 (Personnel Clearance Procedure).

- Office of Cadet Life – After receiving a card from a cadet or the Commandant's Office, the Office of Cadet Life shall notify all Electric Lock Coordinators by e-mail, including the cadet's name and card number, by the close of business the day the card is received so that access capabilities can be suspended. The card shall then be destroyed.

- Building Coordinators – Each Building Coordinator shall recover the VMI Visitor Access Card from each visitor prior to that visitor's permanent departure from VMI.

5. Physical Access Problems

- Should an individual experience any type of physical access problem, they should contact the Information Technology Help Desk, who will direct the individual to the party that can resolve the issue. Depending upon the circumstance, the Help Desk may refer the individual to Physical Plant, Human Resources Office, Office of Cadet Life, Information Technology, the Electronic Lock Coordinator, or Building Coordinator.