FROSTBURG STATE UNIVERSITY
POLICY FOR COMPUTER SECURITY

A. P O L I C Y

1. All administrative information stored within the Administrative Software System is considered a resource and the property of the University. Implementation and adherence to the University 's security policy is necessary to protect this resource. Security standards shall be applied in the procurement, design, development, implementation, and operation of computer systems and applications.

2. Before an administrative computer account is released to an individual, the individual is required to read and sign a Certification of Security form.

3. Individuals must keep passwords confidential. The Office of Administrative Computing will force individuals to change their passwords on a regular basis.

4. Accounts must be kept active. If an account is inactive for six months or more, it will be disabled and the account owner will be required to complete an Inactive Account Notification form.

5. State and Federal laws regarding unauthorized access and disclosure of confidential information must be adhered to.

6. The Office of Administrative Computing computer facilities and administrative data support the operation of the University. Use of these facilities or data for unauthorized activity such as: to obtain personal monetary gain; to jeopardize legitimate use; to provide resources to other unauthorized persons; or to conduct illegal activities is forbidden and will be prosecuted within the scope of applicable laws. Additionally, violation of security policies or procedures can result in revocation of access and disciplinary action, including suspension or termination.

7. Access to any data must be approved by the line officer in charge of that area.

8. If a PC is going to be left unattended, the user should lock the computer.

9. Screens should be kept out of view from any other unauthorized personnel.

10. Students should not be allowed to use other individual's accounts under any circumstance.

11. Any change in employment status which would affect an individual's administrative computer access should be reported to the Office of Administrative Computing so that the appropriate security measures may be enacted.

12. Any breach of security should immediately be reported to the Office of Administrative Computing.

B. DEFINITIONS

1. Line Officers - Those people who are responsible for the application software systems at Frostburg State University. They are responsible for insuring data integrity, accuracy and legitimacy.

   Individuals in the positions listed below are currently responsible for approving access to the data in the following area:

Area of Responsibility	Officer
Admissions	Associate Director of Admissions
Alumni/Development……	Director of Annual Giving
Financial Aid……………..	Director of Financial Aid
Financial Records……….	Director of General Accounting
Human Resources……….	Director of Human Resources
Payroll……………………..	Manager of Payroll
Purchasing/Budget……….	Associate VP for Budget
Student Financials………..	Bursar
Student Records…………	Registrar

2. <u>End Users</u> - Those people who have a legitimate need for access to administrative data stored within the Administrative Software Systems at Frostburg State University.

C. RESPONSIBILITIES

The protection of the administrative data resource is inherently management's responsibility. Managers identify and protect data within their area of control. In addition, managers ensure employees understand their obligations to protect this data. Implementation of security measures is the shared responsibility of end users, line officers, and the Office of Administrative Computing.

1. End Users have a right to access information in the Application software systems as necessary to perform their assigned duties. In exercising this right to access data, they shall:

    a. Obtain approval from the appropriate line officer in charge of the area where access is requested before update or view capability of any software module is granted.

    b. Have the right to appeal for access to the Computer Security Board if denied screen access for security reasons. This board consists of the Director of Administrative Computing, the University's Internal Auditor, the Security Manager, and the Vice President of Administration and Finance.

    c. Maintain password confidentiality.

    d. Maintain the privacy and security of data and use the data and computing resources as efficiently as possible.

    e. Report suspected misuse of administrative data or the computing resources of the Office of Administrative Computing to the Director or Security Manager of that office.

2. Line officers shall:

    a. Identify the degree of protection required for their data.

    b. Establish measures which affect security within the application, if required. These measures limit users to specific portions of the application as dictated by the user's function and promote proper separation of duties.

c. If they so desire, assign the responsibility to approve access to an additional staff member in each area. The line officer may grant this responsibility by sending a letter to the Director of Administrative Computing or the Security Manager.

(Internal)