X-15.21- ADMINISTRATIVE COMPUTER SECURITY

I. PURPOSE:

To ensure that the creation or “building” of computer accounts and the access privileges given to each user will be properly authorized and documented. To set forth the procedures and guidelines to be followed in creating, using and closing computer accounts.

II. APPLICABILITY

A. Scope:

1. The computer system and information contained therein are essential to the daily operations of Bowie State University. The computer systems serving BSU support various business functions and are used to manage proprietary information.
2. It is the responsibility of BSU management and each of its department managers to protect proprietary information.
3. Proprietary information is any data or software BSU does not wish to freely disclose or lose control of, or which is governed by copyright and/or trade regulations. The term also includes the computer resources and information about others that is in the possession of BSU which is subject to restrictions on its use or further disclosure.
4. Critical business applications are those programs, functions, activities, and data performed by or contained on the University's administrative computer system which, if lost, interrupted, or misused, would have a significant adverse impact on the services provided by BSU and/or would materially impair the University in carrying out its mission.
5. The primary objective in protecting proprietary information is to prevent, contain, and recover from man-made and/or natural harms to University computer resources.
6. It is the policy of BSU to protect its proprietary information and allow the use, access and disclosure of such information only in accordance with the University's interests and the Annotated Code of Maryland, Crimes & Punishments, Article 27, §45A and §146.
7. The Bowie State University Administrative Computer Center is charged with the responsibility to know and to comply with the usage and access controls required by proprietary data and/or software over which the University has control as specified by the owner/originator.
8. Each employee as the originator, custodian and/or user of data, must ensure that University data under his/her direction and/or control is properly identified and safeguarded according to its sensitivity , proprietary and/or critical nature.

9. As users of University data, each employee must strictly adhere to the specific security measures and controls that have been established (See Section E). Any unauthorized use of the University's computer resources for personal purposes, or any other purpose not related to the University, is strictly forbidden. Employees are permitted to use only the computer resources and information for which they are authorized. Employees must be granted use of the computer system only in accordance with the procedures contained in Section E of this policy.
10. Violations or suspected violations of computer security measures or controls must be reported immediately to the Department Head/Supervisor and/or The Administrative Computer Center.

B. Responsibility: The Administrative Computer Center of Bowie State University is the unit charged with maintaining computerized records in a variety of areas including student information, personnel records, and fiscal accounts. This information is sensitive and must be protected against unauthorized access, alteration, or use. For this reason the University has established policies on computer security and access to information.

III. VIOLATIONS:

A. Using another user's computer ID for fraudulent purposes such as copying that user's files or giving yourself access to his/her files is prohibited.

B. Any action which would intentionally jeopardize the availability or integrity of the system is forbidden.

C. Attempting to defeat the computer's security system or to use system management facilities without authorization is prohibited.

D. Altering or copying software licensed to Bowie State University without authorization is prohibited. This includes Mainframe and Microcomputer software.

E. Unauthorized manipulation of data using computer resources is prohibited.

F. Use of any User ID other than your own is a serious violation.

G. Any other act that is inconsistent with this policy.

IV. PENALTIES:

Violators of these rules are subject to punishment under the Annotated Code of

Maryland, Crimes & Punishments, Article 27, §§45A, 146.

V. GUIDELINES:

A. Each application (i.e., Student Information System) has only one Application User Coordinator with the authority to approve and request the creation of Application Accounts and their associated access. In order to have an Application Account, a Virtual Management Operating System Account (VMS: the operating/management system software for the administrative computer) must be created. The VMS account type will be determined by the VMS Security Manager.

B. Administrative Computer Center VMS/Application/Function Request Forms are to be filled out for every request and signed by the User, the Unit Account Authorization Designee, the Department Head/Supervisor, and the Departmental Application User Coordinator.

C. The completed request forms are to be sent to the appropriate Computer Center Security Officer (VMS or Application, see Section D).

D. The Security Officer will, after receiving the request, check it for validity, discuss with the Department Application User Coordinator any questions or concerns the Security Officer may have about the request. After all questions have been answered to the satisfaction of the Security Officer, the request will be filled.

1. When the request is for an access modification to an existing account, the form will be given directly to the Application Security Officer for the modification.
2. When the request is for a new Application account creation or function it will:

a) Go to the VMS Security Officer who will create the VMS portion of the account, fill out and sign a VMS Issuance of New Operator Account Form and place the assigned VMS password in a sealed envelope and forward the package to the Application Security Officer.

b) The Application Security Officer will add the application related access specified in the request. The Application Security Officer will fill out an Application Issuance of New Operator Account Form, record the name, username, operator number and current date in the “password log” and forward the package to the Administrative Computer Center Office Automation Specialist Trainee.

c) The Administrative Computer Center Office Automation Specialist Trainee will forward the copies to the Department Application User Coordinator and file the original forms in the Administrative Computer Center Account History file.

d) The bottom portions of both the VMS and Application Issuance of New Operator Account Forms (Receipt Acknowledgement) are to be signed by the user receiving the account and returned within ten days to the Application Security Officers in order for the user to receive the password for their account.

e) The Application Security Officer is responsible for obtaining the user's signed receipt acknowledgement, and recording the receipt date in the "password log."

E. When an employee gives notice that he or she is leaving the employment of Bowie State University, and has an account(s) on the Administrative Computer, the resigning employee's Department Head/Supervisor will notify the Administrative Computer Center VMS and Application Security Officers in writing:

1. Written notification should include the following:
   a) The VMS Username(s) and Operator ID(s).
   b) The employee's last day of active employment.
   c) A statement signed by the Department Head/Supervisor and the Departmental Application User Coordinator(s) allowing the employee continued access to the account(s) until his/her last day of active employment.
2. If the notification does not include the signed statement allowing the employee continued access to the system, the account(s) and ID(s) will immediately be deleted.
3. If the notification does include the signed statement allowing the employee continued access, the account(s) and ID(s) will be deleted on the employee's last day of active employment.

F. After the decision has been made to layoff an employee and this employee has an account(s) on the Administrative Computer, the employee's Department Head/Supervisor will notify the appropriate Computer Center Security Officer in writing that he or she is being laid-off.

1. Written notification to the Computer Center Should include:
   a) The VMS Username(s) and Operator ID(s).
   b) The employee's last day of active employment.
   c) A statement signed by the Department Head/Supervisor and Departmental Application User Coordinator(s) allowing the

employee continued (inquiry only) access to the account(s) until his/her last day of active employment.

2. If the notification does not include the signed statement allowing the employee continued (inquiry only) access to the system, the employee's account(s) and ID(s) will immediately be deleted.
3. If the notification does include the signed statement allowing continued (inquiry only) access to the system the following steps will be taken:
   a) Any update access in the employee's application account will immediately be changed to inquiry only access.
   b) If the employee has a non-captive account (open to the VMS System), the account will immediately be disusered (made nonfunctional).
   c) Any other functions within the application menu that allow for updating or changing of data will immediately be disabled.
   d) The account(s) and ID(s) will be deleted on the employee's last day of active employment.

G. When an employee with an account(s) on the Administrative Computer is dismissed by the institution, the employee's Department Head/Supervisor will immediately notify in writing, the appropriate Computer Center Security Officers. All account(s) and ID(s) assigned to the employee will be deleted immediately upon receipt of written notification.

Effective Date: 05/23/1995