Effective: February 4, 2014

Administrative Policy
COMPUTER SECURITY

Approved: February 4, 2014
President's Cabinet

All administrative information stored within Administrative Software Systems is considered a resource and the property of Millersville 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.

Individuals must keep passwords confidential. Information Technology will require individuals to change their passwords on a regular basis in compliance with our password policy.

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 Account Request form.

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

Information Technology 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.

Access to any data must be approved by the data owner in charge of that area.

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

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

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

Any change in employment status, that would affect an individual's administrative computer access, should be reported to Information Technology so that the appropriate security measures may be enacted.

Any breach of security should immediately be reported to Information Technology.

Definitions

Administrative Software System – These systems are core to university business, and contain data related to students or university employees. Examples: Financial, Alumni, Student, Human Resources, Learning Instruction, Health Services, etc.

Data Owner – Individual who has the ultimate responsibility for the data integrity, accuracy and legitimacy at Millersville University.

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

Area of Responsibility	**Officer**
Admissions	VP for Student Affairs
Alumni/Development	VP for Advancement
Financial Aid	Director of Financial Aid
Financial Records	Accounting and Budget Director
Human Resources	Executive Director for Human Resources
Payroll	Director of Payroll
Purchasing	Director of Purchasing
Budget	Accounting and Budget Director
Financials	Director of Student Accounts
Student Records	Registrar

Data Steward – Designees based on position that can change / update data information and are responsible for the data integrity, accuracy and legitimacy at Millersville University.

Data Users - Those people who have a legitimate need for access to administrative data stored within the Administrative Software Systems at Millersville University.

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 are the shared responsibility of Data Owners, Data Stewards, Data Users and Information Technology.

Data Owners shall:

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

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

Data Owners can assign the responsibility to approve access to an additional staff member in each area. The Data Owner may grant this responsibility by sending a letter to the Director of Information Systems Support.

Data Users shall:

Have the 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:

1. Obtain approval from the appropriate Data Owner in charge of the area where access is requested before update or view capability of any software module is granted.

2. 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 Information Systems Support, Assistant Vice President for Information Systems Services and the Assistant Vice President of Information Technology.

3. Maintain password confidentiality.

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

5. Report suspected misuse of administrative data or the computing resources of Information Technology to the director of that office.