WESTERN MICHIGAN UNIVERSITY

Administrative Data and Systems Policy – PeopleSoft Applications

It is the policy of Western Michigan University to implement controls to secure and limit vulnerability of administrative data and applications stored in/and accessible by University owned computing systems and by University employees.

Access to administrative data and applications residing on any University owned computing system or application will be granted to employees of WMU only. Access to data and applications will be granted only to the extent necessary for employees to exercise the responsibilities of their employment.

Students and contract workers who are employees of the University, with supervisor permission, may access administrative data and applications to the extent necessary to perform the responsibilities of their employment.

Administrative Data and Systems Definitions

Access Capability - Authority granted to an individual which allows viewing of Administrative data residing on any administrative systems or applications file. Access capability is generally managed through assignments of a login name and password

Administrative Data - *Any data related to the administration of WMU. This includes data used by both the central administration and the administrative units of the various departments of the University.*

Administrative Systems and Application - *Any computer system/application or program which supports administrative activities of the University. This includes systems or applications supporting both central administration and the administrative units of the various departments of the University.*

Maintaining Confidentiality of Restricted Data

The Data Steward is responsible for determining:

- What administrative data within administrative systems and applications are appropriate for distribution.
- The audience for distribution.
- The methods and timing of distribution.

The Data Steward must ensure that all individuals with access to administrative data are aware of the confidential nature of the information and the limitations, in terms of disclosure, that apply to the data.

When accessing restricted information, employees are responsible for maintaining its confidentiality. The granting of a user login name and password requires that employees will always maintain confidentiality over appropriate information.

Updated and Approved by PS Security Committee on March 24, 2010

The release of administrative data without the express approval of the Data Steward or outside the established guidelines for such administrative data will not be tolerated.

University enterprise-level administrative data are assets owned by Western Michigan University and must be protected accordingly. For continuity and consistency with University policies and procedures set by the Office of Information Technology, this policy serves as a foundation of acceptable administrative use of the University's PeopleSoft applications. Reference to the other related acceptable use and security policies are indicated below:

http://www.wmich.edu/security

- Confidential Information Policy for Employees of Western Michigan University
- Family Education Rights and Privacy Act (FERPA)
- Social Security Number protection policy
- Health Insurance Portability and Accountability Act (HIPAA)
- Freedom of Information Act (FOIA)
- Identity Theft Prevention