UAR NUMBER: 310.04

TITLE: Administrative Data Responsibility

ORIGINATOR(S):

Assistant Vice President for Technology

INITIAL ADOPTION: 6/14/1993

REVISION DATE(S): 4/30/2010; 10/01/2016; 07/09/2018

AUDIENCE: (SELECT ALL THAT APPLY)

✓ FACULTY ✓ STAFF ✓ STUDENTS VENDORS OTHER (SPECIFY):

PURPOSE:

To ensure all University administrative data resources are properly utilized and maintained to effectively address the service mission of Morehead State University.

SCOPE:

All faculty, staff, and student workers.

DESCRIPTION (INCLUDE DEFINITIONS):

RESPONSIBILITY:

The following statements will function as the official guidelines of Morehead State University as it relates to the use and security of all administrative data. The Office of Information Technology shall have the responsibility for the development of the regulations and procedures by which the University faculty, staff and students will operate to ensure the quality and security of all University administrative data located on University enterprise servers, departmental servers, desktop computers, mobile devices or other electronic storage devices. This includes student-, financial-, alumni-, employee-, library-, policy-, and budget-related data.

PURPOSE:

The University maintains data which are essential to performing business. These data are to be viewed as valued resources over which the University has both rights and obligations to manage, secure, protect, and control. This policy addresses data issues such as the rights and responsibilities of authorized persons in the handling of, as well as, the security and protection of University data accessible by employees in their official University capacities.

OBJECTIVE:

To identify proper procedures and regulations for handling and securing University administrative data. While these data may reside in different data base management systems and on different machines, these data aggregate may be thought of as forming a logical data base, which will be herein called the Administrative University Data Base (AUDB). This terminology is not intended to imply that these data now or in the future should reside in a single physical data base. Rather, it is a recognition that regardless of where these data reside, there are some general principles of data management that should be applied in order to maintain the value and guarantee effective use of information resources.

APPLICABILITY:

This regulation applies to all Morehead State University full-time and part-time faculty, staff and student workers that access administrative data. The following statements will function as the official guidelines of Morehead State University as it relates to the use and security of all administrative data.

DATA SYSTEMS:

University data is maintained on a variety of computer data bases. The following table outlines some, but not all, of the current major systems/networks. The Office of Information Technology maintains a current

APPROVED BY:

VICE PRESIDENT: Chris Howes DATE: 7-9-18

APPROPRIATE INSTITUTIONAL REVIEW: _____ DATE: _____

PRESIDENT: Jay D. Vroegan DATE: 7-9-18

310.04 Continuation

DATA SYSTEMS:

University data is maintained on a variety of computer data bases. The following table outlines some, but not all, of the current major systems/networks. The Office of Information Technology maintains a current, complete listing of all systems.

DATA BASE	SYSTEM	DESCRIPTION OF APPLICATION
Ellucian Colleague	IBM Power S814	Ellucian Colleague Enterprise Resource Planning (ERP) System provides an integrated administrative system for admissions, student records, finances and accounting, student accounts, Financial aid, human resources and other administrative functions.
Ex Libris Alma	Hosted by the Kentucky Virtual Library	The library system houses the catalog system for the resources available in the Camden-Carroll library. Also maintained in this system is patron information.
University File Servers	Various Windows File Servers available via the University LAN and WAN	The University maintains a system of file servers available for storage of documents created and maintained by offices within the University.
Phone System	CBTS Hosted Cisco Unified Collaboration System	Contains University telephone data and call track-ing, instant messaging and voice mail information.
Electronic Mail System	Microsoft Exchange	Email messages of faculty and staff.
Departmental	Desktop and mobile computers	Various administrative data maintained on desktop and mobile computer equipment.

OWNERSHIP OF ADMINISTRATIVE DATA:

In order to control access and update capabilities, an individual residing in the user area responsible for the specific application is designated the data custodian. This individual performs in a supervisory or managerial capacity and is responsible for the data residing in the designated application. The responsibilities of the data custodian are to:

- Ensure proper operating controls over the application in order to maintain a secure processing environment;
- Ensure accuracy and quality of data residing in the application;
- Approve all requests for access to and update capability for the specific application;
- Ensure system issues impacting the quality of data within the system are properly reported and adequately resolved;
- Ensure data elements maintained are consistent with official university reporting requirements;
- Respond to requests for ad-hoc (QUERY) reports for data residing in the application.

A list of data custodians and the applications in which they manage data is maintained by the Director of Information Technology Applications Services.

PASSWORDS:

Passwords are a critical component to the computer system's security. To property control passwords and maintain their integrity, the guidelines below should be followed by every data user:

- Users must never give out their personal password to anyone; sharing of passwords is a violation of this policy. Granting of a password to a user extends responsibility to that user to maintain confidentiality of restricted data without exception.
- Account access will be terminated upon notification of an employee's termination or suspended for employment transfer until request for access has been made.

ADMINISTRATIVE DATA RESPONSIBILITY COMPLIANCE:

Users are reminded of their responsibility to protect University data at the time of login. When faculty, staff, or student logs into MyMoreheadState Portal or Blackboard, they acknowledges compliance with the following statement:

"Morehead State University (MSU) maintains administrative, technical, and physical safeguards to protect the security and confidentiality of students, staff, faculty, and sensitive University information: specifically, information managed and maintained through information technology resources. Furthermore, MSU guards against unauthorized access to data, information, and resources that could result in substantial harm or nuisance to any customer. By logging in, you are agreeing to abide by the safeguards put in place at MSU and to follow the rules for acceptable use of technology resources and FERPA guidelines as stated in PG-55, the student and faculty handbooks, and the undergraduate and graduate catalogs."

REQUEST FOR ACCESS:

Access capabilities for an individual employee or authorized user must be approved by the supervisor and appropriate data custodian assigned to the data application. (See OWNERSHIP OF ADMINISTRATIVE DATA).

DATA ACCURACY:

The accuracy of each data element within the AUDB must be maintained at all times. The following guidelines should be followed to ensure data accuracy:

- Applications that capture and update data should incorporate edit and validation checks where possible to assure the accuracy of data.
- Each data user has the responsibility of questioning any data elements that do not agree with hardcopy or other validating documents. The data user must provide as much detailed information of the suspected problem to the data custodian and assist with correction as soon as possible.
- The data custodian is responsible for responding to data element questions and working the Office of Information Technology if necessary to correct any inconsistencies.

Upon notification of erroneous data, corrective measures should be taken by the Office of Information Technology and the data custodian to:

- Correct the cause of the erroneous data.
- Correct the data base elements involved.
- Notify users who may have accessed erroneous data.

NOTE: Problems with data on the Ex Libris Alma library system should be reported to and handled by the Camden Carroll Library Staff.

DISTRIBUTING ADMINISTRATIVE INFORMATION:

Just as caution must be exercised in granting access capabilities to administrative data, such caution must also be extended to the distribution of administrative information. Each user must follow the guidelines below when distributing information:

- Ensure that the information distributed is in compliance with any regulatory requirements (e.g. Buckley amendment) or university policy.
- Ensure that distribution methods (paper, diskette, or electronic transfer) are appropriate and provide adequate security over the information contained on the particular media.
- Maintain confidentiality of restricted data.
- Ensure that authorization for releasing data has been received from the data custodian.

DATA SECURITY BREACHES:

If any user becomes aware of possible breaches in administrative data/computer security, that user is responsible for reporting the occurrence(s) to the Office of Information Technology, the data custodian, or any member of the Technology Resources Committee. Such reports will be held in strict confidence.