MISSOURI SOUTHERN STATE UNIVERSITY POLICY

Policy #:	02-0021				
Name of Policy:	Data Standards and Integrity				
Date of Last Revision:	May 2022	Initial Date of Approval:	Unknown	Initial Effective Date:	Unknown
Policy Owner	Chief Security Officer				
Policy/Chapter Sections	Definitions Data Integrity Administrative Responsibility Access to Data Secured Access to Data User ID Passwords Data Custodians Area of Responsibility of Data Custodian Data Change Rules				
Date of Next Review:	May 2025				

1.0 PURPOSE

This policy provides guidance for establishing university data standards and guidelines for data integrity. This policy outlines the responsibilities for data owners and users who input and access data.

2.0 SCOPE

This policy applies to all individuals who utilize university data systems such as Ellucian Banner and any other system with the capability to access/add/update/remove records.

3.0 POLICY

Definitions

Data Custodian - A Data Custodian is the director of a Missouri Southern State University office or department. The Data Custodian may make forms (data screens) in their charge available to others for the use and support of the office or department's functions.

Data User – A Data User is an individual who has direct responsibility for entering and/or using data as part of their daily tasks. The Data User includes but is not limited to employees, student workers, interns, teaching assistants, and third-party vendors.

Data Integrity

Administrative Responsibility
By law, certain data is confidential and may not be released without proper authorization. Users must adhere to any applicable federal and state laws as well as Missouri Southern State University policies and

procedures concerning storage, retention, use, release, and destruction of data (refer to the Annual Family Education and Privacy Act (FERPA) Notifications as well as the MSSU Employee Handbook).

Data is a vital asset owned by the University. All Missouri Southern State University data, whether maintained in the central database or copied into other data systems (e.g. personal computers) remains the property of Missouri Southern State University. Access to data should not be approved for use outside a user's official University responsibility. Data will be used only for legitimate Missouri Southern State University business.

As a general principle of access, University data (regardless of who collects or maintains it) will be shared among those Data Users whose work can be done more effectively by knowledge of such information. Although the University must protect the security and confidentiality of data, the procedures that allow access to data must not unduly interfere with the efficient conduct of University business.

Division/department heads will ensure, for their areas of accountability, each Data User is trained regarding user responsibilities. As part of that training, each user will read, understand, and agree to abide by the stipulations in this document.

Division/department heads will ensure a secure office environment for all Missouri Southern State University data systems. Division/department heads will determine the data access requirements of their Data Users as it pertains to their job functions before submitting a request for access to the IT Help Desk.

All procedures and data systems owned and operated by Missouri Southern State University will be constructed to ensure:

1. All data is input accurately.
2. Accuracy and completeness of all data is maintained.
3. System capabilities can be re-established after loss or damage by accident, malfunction, breach of security, or natural disaster.
4. Breaches of security can be controlled and promptly detected.

Access to Data

Data Users are responsible for making sure they understand all data elements to be used. If a user does not understand the meaning of a data element, the user should consult their supervisor or the appropriate Data Custodian (see the Data Custodian section). Users must protect all University data files from unauthorized use, disclosure, alteration, or destruction. Users are responsible for the security, privacy, and control of data in their control. Every user is responsible for all transactions occurring during the use of their log-in identification (ID) and password. Users are not to loan or share access codes with anyone. If it is discovered a user inappropriately loans or shares their access codes, they will be subject to disciplinary action, up to and including termination.

Division/department heads must request access authorization for every Data User under their supervision by submitting a request for access to the IT Help Desk (See Secured Access to Data Section). Generally, temporary or part-time employee access will be limited to display (inquiry/query) only on selected data screens. A Data User will be given update capability only after being carefully considered and approved by the division/department head and the Data Custodian. When a Data User updates information in the data system, these changes will be tracked by user ID.

Secured Access to Data

Data system access will be established based on job functions such as clerical, faculty, cashier, etc. and this will be referred to as role. Specific access will be assigned to each role. For example, the registration clerk might have update access to registration, but only display access to academic history. Each user will

be assigned a role, or possibly several roles, depending on their needs as established by their division/department head and approved by the Data Custodian(s).

User ID

- Data User ID's are generated automatically for new employees and students. For new Data Users the division/department head and/or Data Custodian(s) determine the appropriate roles the user is to be assigned and requests roles by submitting a support ticket to the MSSU Help Desk.
- The Data User will participate in data training provided by the employee's direct supervisor or designee, which will also include password protection (see Password Section below).
- Change requests for ID security may also be made by calling the Help Desk. All Data Users must not leave their workstations while logged into university systems. Windows logo key + L provides a mechanism to lock a workstation. To unlock a workstation, a password must be entered.

Division/department heads will determine the data access requirements of their Data Users, as it pertains to their job functions before submitting a request for access to the IT Help Desk.

- It is the responsibility of the supervisor/HR to notify IT when a Data User changes positions/roles which necessitates different access.
- It is the responsibility of the division/department head to notify IT immediately when a Data User has or will be terminating their employment/engagement at MSSU.

ALL DATA USERS <u>MUST</u> LOG OUT AT THE END OF THE DAY.

Passwords

Access will be granted using a Lion Login. Upon first entry into the system, the Data User should change their password. Additionally, all information access systems used campus wide will require a password that complies with the university guidelines.

Please use the guidelines noted below to ensure passwords will stay secure and be difficult to breach.

- Passwords should be more than 8 characters as recommended by best practices.
- Passwords should be unique from other passwords used for other accounts (personal email, online banking, etc.).
- Passwords should not be easily guessable (first name, last name, nickname, child or spouse's name, birth, anniversary dates, semester and year, month and year, season, etc.).
- Do not write down and store passwords in an easily accessible location, such as a desk drawer, monitor screen, keyboard shelf, etc.
- If a Data User forgets their password, they must contact IT Help Desk in person, bearing a photo ID.
- Data Users are not allowed to share their User ID or password with any other person. Data Users are responsible for the activity on their accounts.

Data Custodians

A Data Custodian (see list below) is the director of a Missouri Southern State University office or department. The Data Custodian may make forms (data screens) in their charge available to others for the use and support of the office or department's functions.

Before granting access to forms (data screens), the Data Custodian must be satisfied that all protection requirements have been implemented and a "need to know" is clearly demonstrated. By approving user

access, the Data Custodian consents to the use of that data in the normal business functions of administrative and academic offices or departments.

Data Custodians are responsible for the accuracy and completeness of data files in their areas. Misuse or inappropriate use by individuals will result in revocation of the user's access privileges. Data Custodians are also responsible for the maintenance and control of data system validation and rules tables. These tables, and the processes related to their use, define how business is conducted at the University.

Area of Responsibility of Data Custodian

Category	Area of Responsibility	Data Custodian
Student	Faculty/Catalog/Room Scheduling	Provost
Student	Registration/Academic Records/ Transfer Articulation	Registrar
Student	Prospects/Applications/Admits	Dean of Admissions
Student	Residential Life	Director of Res Life
Student	Student Accounts Receivable	Bursar
Student	Co-curricular Records	VP of Student Affairs/Provost/Director of Athletics
Student	Advising/Early Alert	Director of ACTS
Student	Medical	Health Center
Student	Counseling	Lead Mental Health Counselor
Student	Athletics	Director of Athletics
Student	Conduct	Director of Conduct
Student	Financial Aid	Director of Financial Aid
Finance		Treasurer
Human Resources		Chief Officer of Human Resources
Advancement	Alumni Association	AVP of Development
Advancement	Foundation	Executive VP

Area of Responsibility of Data Custodian may be revised, edited, changed, or removed at any time with or without notice.

Data Change Rules

The following rules govern which office makes name, identification number, address, and/or telephone number changes to student, employee, financial aid recipient, or vendor, in the integrated data system.

For Prospective Students

Prospective student or applicant	The Office of Admissions will make the change with the appropriate documentation.

Financial aid applicant only	The Financial Aid Office will make the change with appropriate documentation.

For Matriculated Students

Matriculated student	Registrar will make the change with appropriate documentation.
Matriculated student and financial aid recipient	Registrar will make the change with appropriate documentation and with notification to the Financial Aid Office.
Matriculated student and vendor and/or financial aid recipient.	Registrar will make the change with appropriate documentation and with notification to Accounts Payable and the Financial Aid Office.
Matriculated student and employee	All employees who are also students will be required to submit changes through the HR office, this includes help and work-study students.

For Employees

Employee or employment applicant only	HR will make the change with appropriate documentation.
Employee and vendor	HR will make the change with appropriate documentation with notification to Accounts Payable.

For Vendors

Vendor only	Purchasing or Accounts Payable will make the change with the appropriate documentation.

4.0 HISTORY

This policy may be revised, edited, changed or removed at any time with or without notice to applicable individuals.

5.0 RELATED DOCUMENTS

None