Section 1: Introduction, Roles, and Ownership

Introduction

Scope

The standards and policies presented herein this document provide oversight for information systems, associated infrastructure, and the usage of these systems at Northwestern State University. These standards and policies also incorporate the creation, updating, processing, outputting, distribution, and other uses of electronic information at Northwestern State University. All specifications indicated are independent of system architecture and apply to all data systems, applications, networks, personal computing devices, which includes computers, tablet, smartphones and any other information technology whether developed at Northwestern or acquired from external vendors. The policies contained herein shall be reviewed periodically and supplements/changes made as needed. The University community shall be notified of such changes per the distribution procedures outlined herein.

Purpose

The primary purpose of these standards and policies is to establish roles and responsibilities and to ensure that each information and technology system meets functional requirements, is appropriately documented, is secure and controlled, has been adequately tested, is maintainable, and provides necessary audit features where applicable.

General Information

The following general information regarding this policy is provided in the following subparagraphs.

Policy Interpretation

The University's Chief Information Officer (CIO) shall be the primary contact for the interpretation, resolution of problems and conflicts with local policies, special situations, and enforcement and monitoring of this policy. Any legal issues shall be referred to the System Legal Office for advice.

Policy Enforcement

The CIO in association with the Vice President for Technology shall work with the appropriate administrative units to obtain compliance with this policy. IS administrative staff are authorized to take reasonable action in accordance with this policy to implement and enforce the usage and service policies of the system and to provide for security of the various systems and associated data.

Suspension of Privileges

Access to university electronic resources is a privilege and not a right. Privileges can and will be suspended in cases were evidence demonstrates that systems or data was placed at risk, made accessible to unauthorized individuals or organizations not approved appropriate University staff. The CIO or Deputy CIO may temporarily suspend user access privileges if he or she believes it necessary or appropriate to maintain the integrity of systems, data or network. The Vice President of Technology has ultimate authority for policy enforcement over all systems owned by or associated with Northwestern State University. After consultation with the Vice President of Technology, the CIO / Deputy CIO may permanently revoke user access for repeated or serious violations of this policy.

Inspection and Monitoring

Only the Vice President of Technology or designee can authorize the inspection of private data or monitoring of messages (including electronic mail) when there is reasonable cause to suspect improper use of computer or network resources.

Systems

For the purposes of this document, a system is comprised of people, procedures and equipment for collecting, storing, manipulating, retrieving, and reporting data. A university information system is one that is essential to conducting the business functions of the University. Once such example would be the Banner ERP System.

Roles and Responsibilities

The following paragraphs define the roles and responsibilities of the individuals and groups shown below.

- System Custodian
- System Manager
- System Custodian's Representative
- System Administrator
- Network Administrator
- System User
- User Support
- Operations Support

- Programming Support
- Vendor Support

The Office of Information Systems shall have final authority over all data processing systems, information technologies, and networks associated with the university, including the authority to access, evaluate, and/or suspend the operation of any university data processing system or network.

System Custodian

A System Custodian is a director within Information Systems. The responsibilities of a System Custodian include overall responsibility for the operations, maintenance, and security of the systems and data under the purview of Information Systems. In keeping with the roles and responsibilities as set forth in this section, a System Custodian can appoint a System Custodian's Representative for each of the systems identified in paragraph 1.5.2.

System Custodian's Representative

A System Custodian's Representative is defined as the primary point of contact between Information Systems and the System Manager. A System Custodian's Representative shall be appointed by a System Custodian for each of the systems identified in paragraph 1.5.3. The responsibilities of the System Custodian's Representative include the following:

- Serve as the primary point of contact between Information Systems and the System Manager
- Coordinate the needs of the System Manager within and among the various elements of Information Systems
- Maintain correspondence and/or documentation
- Work with software vendors as required to resolve system problems
- Participate in meetings with the System Manager
- Participate in system tests and acceptance activities
- Support the System Manager in the development of system test and acceptance criteria
- Assist the System Manager in developing and maintaining a policy statement that describes the system and identifies the key players and outlines their roles and responsibilities. The policy statement shall become a part of the EDP and, as a minimum, shall consist of the following components:
    - System Overview.
    - Key personnel and their roles and responsibilities.
    - System components and their functions.
    - System users and their roles and responsibilities.
    - Backup and restore policy.
    - Data retention policy.

- Grant access privileges as approved by the System Manager as well as creating accounts approved by the System Manager when the system does not support Active Directory authentication.

System Manager

A System Manager is defined as the individual with primary responsibility for the functional operation of a particular information system. System Managers perform functions including, but not limited to authorizing access to information, data, or applications and have overall responsibility for the integrity and accuracy of the information or data processed by that system. A System Manager shall be identified for each primary university information system. Excluded from this requirement are infrastructure systems such as e-mail, Domain Name Service, Active Directory, etc. These types of systems are managed by Information Systems. The following Systems and the associated System Manager (by job title) are shown in the table below.

System Management	
System	**System Manager**
Billing and Receivables	Bursar
Learning Management System	Vice President of Technology
Financial Aid System	Director of Student Financial Aid
Financial Records	Associate Controller
Housing Module	Director of Auxiliary Services
Human Resources System	Director of Human Resources
One-Card System	Coordinator, One Card Operations
Purchasing System	Director of Purchasing
SACS Support System	Director of University Planning, Assessment and EEO
Student Records System	Registrar
Surveillance Camera Monitoring System	Chief of University Police

Table 1-1. Key Systems and System Managers.

The responsibility of a System Manager include the following:

- Define the functions, controls, and manual office procedures features associated with the system
- Where audit features are available, specify how they are to be configured (e.g., on or off and for what data or functions)
- Request changes to the system
- Develop system test and acceptance criteria
- Testing and formally accept any change(s) to the system.
- Approve/deny user requests to change the system in conjunction with the system custodian
- Manage, control, and review user access privileges to data. This includes approve/deny user requests for system and data access. Access to the system should be granted on a “need-to-use” basis and access to data should be granted on a “need-to-know” basis
- Provide user training.

- Develop and maintain a policy statement that describe the system and identifies the key players and outlines their role and responsibility. The policy statement shall become a part of the EDP and, as a minimum, shall consist of the following components: (See paragraph 19 for an example of a completed policy.)

    - Introduction – this section should include an overview of the system
    - Purpose
    - Key personnel and their roles and responsibilities
    - System components and their functions
    - System Interfaces
    - Concept of Operation
    - System users and their roles and responsibilities
    - Backup and restore policy
    - Data retention policy

- Have meetings with those offices/individuals deemed appropriate, to include the System Custodian's Representative. The purpose of these meetings will be to review system status associated events, activities, support, or requests.
- Ensure that the system is operated in compliance with all applicable policies and procedures.
- Participate in the Continuity of Operations Plan.

System Administrator

A System Administrator is defined as the individual responsible for configuring and administering the University's enterprise system of computers and software systems. The responsibilities of the System Administrator are many. The key responsibilities of the System Administrator include the following:

- Use privileged access in an ethical manner and in accordance with this EDP.
- Take all reasonable steps to protect the privacy, security and effectiveness of the University's systems and software.
- Take all reasonable steps to ensure systems are reliable and available.
- Report any security violations to the appropriate supervisor or System Manager.
- Take immediate action in the event of a cyber-attack or security threat – this may include shutting down or deny access to systems as well as deny access to specific users believed to pose a security threat.
- Access private information on University systems only when it is necessary in the course of assigned duties by supervisor.
- Ensure that all major system changes are authorized by the System Custodian and are in accordance with this EDP.
- Ensure a proper operational environment with regard to environmental elements (e.g., moisture, dust, power fluctuations, vibration, etc.) for the data center
- Take all reasonable steps to provide a physically secure environment.
- Coordinate with the Network Administrator to ensure maximum protection of information systems and networks.
- Take all reasonable precautions against theft or damage to the system components.

- Adhere to all applicable hardware and software licensing agreements.
- Treat information about, and information stored by, the system's users in an appropriate manner, and taking precautions to protect the security of a system or network and the information contained therein.
- Monitor systems to ensure their proper function.

Additionally, the System Administrator may designate another individual to administer certain systems. This individual will be referred to as the “Designated System Administrator". The Designated System Administrator has additional responsibilities to the University as a whole for the system(s) under his/her oversight, regardless of the policies of his/her department or group, and the System Administrator has the ultimate responsibility to see that the Designated System Administrator carries out these responsibilities.

Network Administrator

A Network Administrator is defined as the individual responsible for configuring and administering the University’s information systems networks and telecommunications facilities. The responsibilities of the Network Administrator are many. The key responsibilities of the Network Administrator include the following:

- Coordinate with the System Administrator to ensure maximum protection of information systems and networks.
- Take all reasonable steps to protect the privacy, security and effectiveness of the University’s network and information systems.
- Take all reasonable precautions against theft or damage to network components.
- Adhere to all applicable hardware and software licensing agreements.
- Ensure a proper operational environment with regard to environmental elements. (e.g., moisture, dust, power fluctuations, vibration, etc.) for the data center and building telecommunications closets.
- Take all reasonable steps to provide a physically secure environment.
- Report any security violations to the appropriate supervisor.
- Take immediate action in the event of a cyber-attack or security threat – this may include shutting down or deny access to systems as well as deny access to specific users believed to pose a security threat.
- Access private information on University systems only when it is necessary in the course of assigned duties.
- Use privileged access in an ethical manner and in accordance with this EDP.
- Monitor the network to ensure its proper function.

System User

A system user is defined as an individual with an established “need-to-use” who has been granted access to a University system. The responsibilities of a system user include the following:

- Comply with the policies set forth in this EDP.

- Comply with all applicable laws and security requirements.
- Comply with all control requirements specified by the System Manager.
- Keep personal usernames/passwords confidential – usernames/passwords must not be shared with anyone and someone may not use the username/password of another individual.
- Not writing or storing passwords in plain text format.
- Logging off or locking the PC when leaving the immediate area unless the screen lock has been activated.
- Not allowing anyone to use a PC that has been signed on under another individual's username and password.
- Not making or permitting unauthorized use of any information in the computer or hard copy files.
- Not seeking personal benefit or permitting others to benefit personally by any confidential information that has come to them through their work assignment(s).
- Not displaying or divulging the contents of any record or report in any manner to any persons except in the conduct of their regular work assignment(s).
- Not knowingly or causing to be included in any record or report a false, inaccurate, or misleading entry.
- Ensure that all printed output containing personal information is shredded.
- Do not make or allow photographs to be made of any display device (e.g., computer monitor) containing personal information.
- Ensure that computer monitors are positioned in such a manner that unauthorized personnel cannot read personal or sensitive information.
- Do not aid, abet, or join in a conspiracy with any other person to violate any part of this EDP.

User Support

User support is defined as that support provided to the systems users by Information Systems staff pertaining to the installation, configuration, and maintenance of University PCs (hardware and software) and other devices used to access University systems and other systems as required for the University to conduct business.

Operations Support

Operations support is generally defined as the scheduling and execution of computer jobs and the dispersal of printed output especially as relates to batch processing related to the PLUS server. However, in practice operations support includes a wide array of actions to include scanning timesheets, bulk loading of data such as test scores, and data entry.

Programming Support

Programming support is defined as that support above and beyond the support provided by commercial systems such as Banner. Examples of programming support

are as follows: extracting, manipulating, and reporting data; providing users with a means to input and store data; providing a means for users to retrieve, format, and display data. Requests for programming support must be accomplished via a Data Request as described in paragraph 3.1.

Vendor Support

Vendor support is defined as that support provided for hardware and software under warranty and/or maintenance agreements. The specific type of support provided varies depending on the terms and conditions of the warranty and/or maintenance agreement. General examples of vendor support are as follows: the repair and replacement of hardware items; technical support for the resolution of problems; patches, fixes, upgrades, and enhancements to firmware and/or software.

Document Changes and Updates

Changes and updates to this document shall be approved by the Chief Information Officer before submission to the Vice President of Technology for final approval.

Document Distribution

This document shall be posted on the Information Systems web page. The faculty and staff shall be notified of changes/updates to this document via Messenger e-mail.