Section 3: Controls and Security

The following establishes responsibility and minimum requirements for the protection of University data and describes the control and functional features necessary to maintain data security.

Control Responsibility

The System Manager is responsible for determining the control features of a system. The appropriate IS staff member who oversees management of the given system is responsible for implementing control and audit features in accordance with the requirements as stated by the System Manager.

Auditability Requirements

System audit requirements will include: System logging to create a transaction audit trail for online systems; and verification/comparison checks to validate the accuracy and integrity of programs and data.

Access Authorization

A System Manager is responsible for authorizing/restricting access to data within a system except for himself/herself. Access/privileges, to include any changes in access/privileges, for System Managers must be authorized by the supervisor of the System Manager. All NSU information systems will operate on the principle of "least privilege", as follows:

- users will be assigned the minimum privileges needed to perform their tasks
- applications will be assigned the minimum privileges to perform their tasks

Request for such access shall be made in writing using the File Access Request form.

Damage Prevention

Data security shall be designed to prevent both accidental as well as deliberate destruction and unauthorized alteration of data.

Sensitive Data

Sensitive data is that which through loss, unauthorized access, or modification could adversely affect the operation of the university or the privacy of individuals (which is protected under the Privacy Act).

All files with sensitive data must be made secure against unauthorized access.

User Identification and Access Permission

Access Restriction

Access to system applications will be authenticated at logon and job initiation, based on valid user identification and authorization.

Restriction Scope

Access restrictions shall apply to sensitive system resources such as commands, transactions, or data.

Separate Systems

Development and test systems shall be kept separate from live or production systems. Data stored in live systems must be properly maintained and protected from unauthorized access. Testing of new or modified programs will be accomplished only on the test system – live data will not be used for testing purposes unless required to validate real-time reports.

Faculty and Staff Password Standards
The following standards apply to faculty and staff passwords:

- Passwords shall remain confidential – Passwords must not be shared with anyone for any reason
- No one may use the username and password of another individual
- Passwords shall not be kept on paper or stored in plain text format.
- A password will be changed anytime the user suspects that the password may have been compromised.
- If it is suspected that the system may have been compromised, then the System Security Officer/System Administrator will cause all passwords to be changed at the next login.
- Passwords must not be hard coded into software.
- Passwords must not be stored in dial-up communications utilities or browsers.
- Passwords must not be recorded in a system log unless the password is encrypted.
- Passwords must be a minimum of eight (8) characters. Passwords greater than 15 characters should not be used. Passwords greater than 15 characters will result in access to the PLUS servers being denied.
- Imbedded blanks or spaces are not allowed in passwords.
- Passwords must contain at least 3 of the 4 categories:
    - English uppercase characters (A-Z)

    - English lowercase characters (a-z)
    - Base 10 digits (0-9)
    - Non-alphanumeric (special) characters (%, &, !, etc.).
- Passwords must be changed at least every 120 days.
- Systems prompting users for passwords shall not display the password as it is being entered.
- Password history configuration will prevent reutilization of the last 24 passwords when technically possible.

Student Password Standards
The following standards apply to student passwords:

- Passwords must be a minimum of six characters.
- Accounts are disabled after 50 invalid login attempts.
- Passwords should be changed immediately after the student account is created.
- Passwords should be changed at least every 120 days.

Access Monitoring

Systems will be monitored for unauthorized access attempts and will restrict repetitive attempts to gain access in order to forestall unauthorized entry.

Authentication

A valid user name and password are required for access to an information system other than web pages available to the general public.

System Interfaces

Each point where data transfers from one system to another must be secure and the transmission media must be protected from unauthorized access.

Data Backup

Information Systems is responsible for backing up all system data on a routine basis. Data backups will be stored at an offsite location.

Backup and Recovery from Interruptions

Backup Files

All critical data files will be backed-up nightly to facilitate recovery in case of data loss. All source program files, faculty/staff, and student files must be backed up weekly. All backup files must be secured as originals. Any file backup must be in compliance with the "NSU Backup and Restoration Procedures" maintained by Information Systems.

Offsite Storage

At least one backup should be maintained offsite, for all essential applications.

Restoration of Data

In the event of data loss, files must be restored from the latest backup. All data restoration must comply with the "NSU Backup and Restoration Procedures" maintained by Information Systems.

Recovery Process

A disaster recovery process should be in place for all essential systems in order to ensure the ability of the institution to survive business interruptions and to function adequately after an interruption.

Security Administration Procedures

The System Manager shall be responsible for approving requests for system access and privileges. The System Custodian's Representative shall be responsible for implementing these approved requests.

Correcting Errors

System resource use, security variances, and delegation activity should be regularly monitored by the System Manager to trigger timely and appropriate corrective action whenever necessary.

Securing Hardware/Software

All administrative system computing equipment, programs, files, logs, and documents should be kept in physically secure areas in order to provide protection from unauthorized access and acts that would cause hardware or program malfunction.

When a PC is disposed of as surplus property or transferred to a new budget unit, the original budget unit must request the User Support section of Information Systems to inspect the PC and "sanitize" the hard drive(s) on the PC before it is transferred. Support may be requested by calling the helpdesk line @ 4090.

If the PC is being disposed of as surplus property, then the User Support section of Information Systems will perform the following:

- Remove CMOS password, if any.
- Document hardware problems the PC may have before it is sent to surplus.
- Use appropriate software to "sanitize" the PC hard drive(s). If a PC will not function to allow the hard drive(s) to be sanitized, the hard drive(s) will be placed in a functioning PC to be sanitized.
- Affix a sticker to the PC attesting to the above.
- Forward the PC and all necessary paperwork to the warehouse.

The Warehouse will not accept PCs for disposal without the sticker affixed by Information Systems.