

Southern University at New Orleans

Information Technology Security Policy

STANDARDS AND GUIDELINES FOR STRATEGIC SYSTEMS

TABLE OF CONTENTS

1. Strategic System Platforms
 - 1.1 Definition of 'Strategic'
 - 1.2 Management of Strategic Systems
 - 1.3 Physical Security
 - 1.4 Physical Access
 - 1.5 User Access
 - 1.5.1 New Users
 - 1.5.2 Terminating Users
 - 1.5.3 Screen Access & Report Generation
 - 1.5.4 Guidelines on Passwords
 - 1.6 Fire Detection and Control
 - 1.7 Data Integrity
 - 1.8 Password Aging
 - 1.9 Documentation
2. Software Change Control
 - 2.1 Definition
 - 2.2 General Obligations
 - 2.3 Change Control Responsibilities
 - 2.4 Change Control Environment
 - 2.5 Documentation
3. Communications
 - 3.1 Campus Local Area Networks
 - 3.1.1 Physical Security
 - 3.1.2 Physical Access
 - 3.1.3 Data Integrity
 - 3.2 Regional and Wide Area Networks

1. **Strategic System Platforms.**

1.1 Definition of 'Strategic'

A strategic system is one that meets several of the following criteria specified in the University Information Technology Project Inception Form:

- 1.1.1 Is critical to the mission of the University.
- 1.1.2 Affects large parts of the University.
- 1.1.3 Yields university-wide benefits.
- 1.1.4 Is large.
- 1.1.5 Is expensive.

1.2 Management of Strategic Systems

The following policies apply in the management of strategic systems:

- 1.2.1 Strategic platforms will be managed and operated by the Information Technology Center.
- 1.2.2 Strategic Applications/Specific Application functions will be managed by the designated custodian of the application or specific application function.
- 1.2.3 These platforms and Strategic Application/Functions are identified in the general outline "Information Technology Security Policy " document.

1.3 Physical Security

The following standards of physical security of strategic platforms must be met:

- Premises must be physically strong and free from unacceptable risk from flooding, vibration, dust, etc.
- Air temperature and humidity must be controlled to within acceptable limits.
- Platforms must be electrically powered via UPS to provide the following:
 - Minimum of 15 minutes' operation in the event of a power blackout.
 - Adequate protection from surges and sags.
 - Trigger an orderly system shutdown when deemed necessary.

1.4 Physical Access

- Premises will be staffed and controlled by designated Information Technology Center or unit area staff.
- External doors will remain locked, preferably with electronic locks.
- There will be security screens on all external windows and doors.

1.5 User Access

1.5.1 New Users (Faculty, Staff, Workstudy Students)

New User ID's & Operator ID's will be handled as follows:

- Written application must be submitted on a Security Access Form.
- Someone must sign the application form in authority (e.g. Dean, Department/Unit Head).
- The Security Access Form will be kept indefinitely by the Information Technology Center.
- The new User ID and password will be given to the applicant and applicant only, unless special delivery has been authorized due to special circumstances (e.g. applicant is overseas or out of state).
- If the Operating System supports a password aging facility then it must be set to force password change on the first login.
- The system and screen level access will be no higher than required as approved by the Custodian of that function or system.
- Must complete all steps in the Security Access Form Procedure.

1.5.2 Terminating Users.

The User ID's and Operator Numbers of persons leaving the University or transferring to another department must be disabled. The Security Access Form Procedure must be completed during the checkout process. Users transferring to and from departments must have their access rights removed from the old area and re-established in the new area via the Security Access Form Procedure. All files will be referred to the System Administrator for disposal.

1.5.3 Screen Access & Report Generation

- Custodians of Strategic Applications/Functions must approve all Screen Access to System Users for application specific screens via the **"Security Access Form" procedure** with the exception of Auditors.
- Any System User who requires reports, and/or files from Custodian maintained databases will require Custodian written approval via the **"Production Work Order Request" procedure** with the exception of Auditors.

1.5.3 Screen Access & Report Generation continued

- Custodians must identify in writing to the Information Technology Center any System User who **DOES NOT** require Custodian approval for all or specific reports and/or files **only** that is to be used by the System User for reporting purposes.
- Custodians must identify to the Information Technology Center in writing those person(s) whom have signatory approval authority in their absence.

System Users can refer to the **Custodian Screen Access List** and **Reporting Systems Custodian Access List** to determine the corresponding Custodian for screen and report approvals.

1.5.4 Guidelines on Passwords.

1.5.4.1 Password Management.

- Passwords should be memorized - never written down.
- Passwords belong to individuals and must never be shared with anyone else. Except in the case of an Academic Computing Lab environment.
- Passwords should be changed immediately upon issuance.
- Password should be changed, at a minimum, at least once a year.

1.5.4.2 Password Administration.

- New or changed passwords must be given in writing only to the identified user never over the telephone or via email.

1.5.4.3 Password Construction.

Password security isn't just a matter of thinking up a nice word and keeping it to yourself. You must choose a password, which will be difficult for someone else to guess or crack.

We often have a tendency to forget passwords, so we choose something that has particular relevance to ourselves (the name of a loved one, our favorite car, sport, or ice cream, etc.). Anyone knowing a little about us can make a list of these words and easily crack the password. All-digit passwords usually fall into this category - birth dates, phone numbers. Observe the following guidelines when choosing your password:

1.5.4.3 Password Construction continued.

- A password should be at least 6 characters long.
- NEVER make your password a name or something familiar, like your pet, your children, or partner. Favorite authors and foods are also guessable.
- NEVER, under any circumstances, should your password be the same as your username or your real name.
- DON'T use words that can be associated with you.
- Do not have a password consisting of a word from a dictionary. Most basic cracking programs contain over 80000 words, and plenty of variations.
- Try to have a password with a number or mixed case letters. Simple substitutions like a '1' for an 'i', and '0' for an 'O' are easily guessed.
- Choose something you can remember, that can be typed quickly and accurately and includes characters other than lowercase letters.
- Don't reuse your current password for SIS/PLUS, FRS, ADS passwords. ZSS security will retain the last 3 created passwords.
- After 3 unsuccessful attempts ZSS Mainframe Security will force you off the system.
Examples:
 - Made-up "words" - chok-bel (can be "pronounced", has a punctuation character)
 - Personal acronyms - ihc, alt (I Hate Coffee, And Love Tea)
 - Invert syllables - sick.sea (instead of 'seasick')

1.6 Fire Detection and Control.

- There should be smoke and thermal detectors on the premises.
- Under-floor areas should have smoke and water detectors.

1.7 Data Integrity

- Security backups of all Strategic Application data will be made daily.
- Full Image backups of all Mainframe disks are required to be done on a weekly basis on a two-week rotation schedule.

1.7 Data Integrity continued.

- Strategic Network system component backups are required on a nightly basis on an incremental accumulative format.
- Full image backups of critical Strategic Network components must be performed on a weekly basis on four-week rotation or monthly retention period.
- The backup regime must meet the following criteria:
 - Enable recovery to at least the start of business on any weekday of a failure.
 - Provide at least one more level of backup to a previous time, to cover the case of the failure of the primary backup media.
 - There must be offsite storage of security backup media to enable a full data recovery to no earlier than one working week.
 - There must be a validation of security backup media at least once every 12 months.

1.8 Password Aging

If the Operating System or Application System provides the facility, automatic Password Aging will be enforced. Where applicable, the life of a password should be no more than 12 months.

1.9 Documentation

Procedures reflecting these policies must be documented the ITC Computer Operations Instructions.

2. **Software Change Control.**

2.1 Definition

Software Change Control covers the control of all aspects of strategic systems software including the operating system, its associated packages (DBMS etc.) and utilities, third party and university-developed applications, together with any command procedures and documentation to support and run them.

2.2 General Obligations

When changes are required to systems software, associated packages and utilities, applications software, command procedures, or documentation, it is essential that the changes be:

- Appropriately authorized and approved.
- Thoroughly tested.

2.2 General Obligations continued.

- Sufficiently documented.
- Implemented at an appropriate time.

Any change must only be transferred into the production environment when approved by the appropriate System Custodian.

2.3 Change Control Responsibilities.

Specific personnel will be given the responsibility for the implementation of changes by undertaking appropriate testing in the test environment and subject to the appropriate approvals, moving the changes to the production environment. All elements of the system will be subject to the Software Change Control Policy.

There should be a separation of responsibilities in the transfer of software from test into the production environment.

2.4 Change Control Environment.

Where possible, three separate environments should be maintained for each strategic system:

- Development
- Testing
- Production

Migration of software between environments should only be undertaken after obtaining the appropriate sign-off as specified in the Technical Service Request and Programming Documentation Procedures.

New software and changes to existing software should be prepared in the Development Environment by appropriately authorized development or applications support staff. Applications should be specified, designed and coded according to the Users specifications as indicated on the Technical Service Request (TSR) and supporting Programming Documentation Procedures.

Once assessed as satisfactory, the new or modified software should be transferred to the Testing Environment for systems and acceptance testing by an appropriate testing agent. Changes to software are not permitted in the testing environment.

Following successful completion of testing and approval by the appropriate systems custodian, the new or modified software should be transferred to the Production Environment for implementation under the control of the Information Technology Center Computer Operation's staff.

2.5 Documentation

- Software Change Control Policy
- Technical Service Request

No software change is to be undertaken without an appropriately authorized Technical Service Request (TSR) and Programming Documentation Form (PDF). The TSR and the PDF serve as the principal documentation to be completed for the software change management process.

3. **Communications.**

Network access can be categorized into five major areas:

1. Campus Local Area Network
2. External Access via Modem link
3. Regional Networks (LaNet)
4. Wide Area Network (Internet)

The University has varying degrees of control decisions affecting security management of these areas:

1. Total control over the campus LAN Modem links, and Intercampus Network, given that University staff plans, install, manage, and maintain these systems.
2. Limited control over the Regional networks, which are managed by either a consortium of universities and LaNet.
3. No control over the Internet.

3.1 Campus Local Area Networks.

3.1.1 Physical Security

The following standards of physical security campus local area networks must be met.

- Premises housing network control equipment must be physically strong and free from unacceptable risk from flooding, vibration, dust, etc.
- Air temperature and humidity must be controlled to within equipment-defined limits.
- Network electronics must be powered via Un-interruptable Power Supplies to provide the following:
 1. Minimum of 15 minutes' operation in the event of a power blackout.
 2. Adequate protection from surges and sags.

3.1.2 Physical Access

- Access to areas housing network electronics such as wiring closets will be controlled by designated Information Technology Center staff only.
- Doors to areas housing network electronics will be locked with a unique key, the distribution of which will be determined by the Information Technology Center staff or Unit area leadership.

3.1.3 Data Integrity

3.1.3.1 Eavesdrop Protection.

With our present security strategy, users are categorized into security sub-groups (students, faculty, administrative staff, and general staff).

- SUNO Campus Local Area Networks should all be protected by a hardware level of eavesdrop protection.

3.1.3.2 Intrusion Protection

Within the boundaries of the LAN, intrusion protection is required to prevent:

1. Non-university staff or students from indiscriminately plugging laptop computers into any access port of the campus network.
2. Unauthorized access of staff and students to the Universities strategic systems.
 - Only those computers belonging to staff and students will be allowed to function when connected to the University network. Visiting personnel wishing to access the network must have authorization from a staff member, who must apply to the Information Technology Center for temporary access rights.

3.2 Regional and Wide Area Networks.

Protection from illegal entry from public Regional and Wide Area networks will be provided by network firewalls. Many of the University's customers are external to the campus and use the public networks to access university teaching, research and library material via the Internet. Also, academic staff can be highly mobile, requiring access to University services from various external locations off campus.

Because of the nature of Wide Area Networks (WAN) there are only limited security measures that can be taken. The Security Policy for Strategic Systems must rely heavily on software applications, firewalls and general computer

3.2 Regional and Wide Area Networks continued.

controls. The risks of transmitting information over the WAN must be considered when:

- Determining the nature of information to be sent over the WAN.
- Granting approval for new applications, which involve the transmission of information over the WAN.

Approved: _____
ITC Security/Internal Controls Auditor Date

Approved: _____
ITC Director Date

Approved: _____
V.C. of Administration & Finance Date

Approved: _____
Chancellor Date

Created December, 2007