Prepared by the Office of the VP for Planning and Policy
This is a <u>NEW</u> Procedure

A7.023   <u>Security Guidelines and Procedures:</u>
           <u>Student Information Management System (SIMS)</u>

1.   <u>Purpose</u>

     To implement the security objectives of the SIMS Data
     Administration Policy as set forth in Executive Policy
     E7.104.

2.   <u>Objectives</u>

     a.   To ensure the security and privacy of student
          records maintained in the University of Hawai'i's
          (UH) SIMS database.

     b.   To set forth guidelines and standards for
          responsible and acceptable use of SIMS.

     c.   To supplement existing UH policies/agreements and
          state and federal laws/regulations.

3.   <u>Policy Statement</u>

     Access to SIMS data is to be granted only to UH regular
     employees who demonstrate that in the course of
     exercising their officially assigned responsibilities,
     they have a need for specific information. With
     special permission, a student researcher may be granted
     access. Restrictions will apply to all SIMS data
     stored on the UH administrative mainframe and SIMS
     downloaded data stored in mini-computers and micro-
     computers.

4.   <u>Definitions</u>

     a.   Executive Policy E7.104——Establishes a Student
          Information Management System (SIMS) for

University administration; establishes uniform data standards that ensures consistency, comparability, accuracy and integrity of SIMS information; and ensures security and privacy of student records maintained in the SIMS database.

b. SIMS——a Student Information Management System that is intended to serve the UH as a whole, not only individual campuses. It provides the UH administration with a technically current, online accessible, central repository of system-wide student information needed for planning, policy making, and decision support. At designated key points in the semester, each campus will upload a "snapshot" of their student database to the central repository for system-wide consolidation, reporting and management information. Since SIMS contains only the latest "snapshots" sent by campuses, it is not intended to service the daily operational needs of individual campuses or to replace existing campus-based student registration systems.

c. SIMS Data Administration——An executive level functional responsibility, which includes the total management of the University's SIMS data resource.

d. SIMS Data Administrator——An executive who is responsible for SIMS data administration at the University of Hawai'i and reports directly to the President. The Vice President for Planning and Policy, or a designated representative, serves as the SIMS Data Administrator.

e. Access Capability——Authority granted to an individual which allows viewing of data residing in a computer system file. Access capability is generally managed through assignment of a user ID and password.

f. User ID——A character string which identifies an individual to a computer system and enables access.

g.   Read Only Access——Users who are able to view, but
      not update, information in the SIMS database.

h.   Family Educational Rights and Privacy Act(FERPA) —
      Federal rules and regulations that set out
      requirements for protection of the privacy of
      parents and students under section 438 of the
      General Education Provisions Act, as amended. It
      affords students certain rights with respect to
      their educational records.

5.   Security Administration

     The SIMS Data Administrator, or designee, is
     responsible for the data residing in SIMS. The
     responsibilities of the SIMS Data Administrator are to:

     a.   ensure proper operating controls to maintain a
           secure processing environment;

     b.   ensure accuracy and quality of data;

     c.   approve all requests for access; and

     d.   ensure that system issues impacting the quality of
           data are reported and adequately resolved.

6.   Computing Security Procedures

     a.   SIMS Database Security.

           Information Technology Services (ITS) will be
           responsible for the security of the SIMS database
           and will provide appropriate security measures to
           control access to the SIMS database.

     b.   Establishing Backup and Recovery Procedures.

           SIMS backup and recovery procedures should be part
           of the ITS overall backup and recovery procedures

for administrative computing systems and databases.

c. Protecting and Managing Passwords.

Passwords are a critical component to any computer security program. To properly control passwords and maintain their integrity, the guidelines below are established.

(1) Users should never give out or share their personal passwords with anyone.

(2) Passwords will automatically expire at least once a year.

d. Employee Turnover.

When an employee who is an authorized user of SIMS changes assignments or terminates employment with a unit or the University, the guidelines below are followed.

(1) The employee or employee's supervisor immediately notifies the SIMS Data Administrator of termination so appropriate actions can be initiated to change or terminate access to SIMS and any associated files. This standard practice serves to protect the employee and the University in the event of problems arising from subsequent unauthorized access.

(2) Reemployment and reinstatement of authorized access will require submitting a new request for access (see item #7) and, upon approval, establishing a new user ID.

7. Requests For Access

a. **UH Faculty/Staff:** Complete and submit the *SIMS Request for Access Form* (Attachment 1) and *SIMS Security/Non-Disclosure Agreement* (Attachment 2) to the SIMS Data Administrator. Database access will be restricted to **read only**.

b.   **Students:** Personally identifiable information from
      student educational records maintained in SIMS is
      restricted to read only and may be accessed by
      University students conducting research in
      fulfillment of academic requirements provided all
      the following conditions are met.

   (1)   The student researcher is a classified
         student who has acquired basic research and
         statistical skills as an upper-division
         baccalaureate or graduate student.

   (2)   The student researcher has obtained the
         approval of the dean of his or her school or
         college based on submission to the dean of
         the following information: (Attachment 3)

      (a)   A description of the research project
            including certification by the
            supervising faculty member that the
            research topic is of legitimate
            educational interest or value to the
            University and that the research design
            meets academic requirements;

      (b)   The specific data needed;

      (c)   A statement of the method to be used in
            protecting the confidentiality of
            personally identifiable information;

      (d)   A statement of how the results of the
            research will be used and by whom;

      (e)   The period of time for which access is
            requested;

      (f)   A signed statement by the supervising
            faculty member accepting responsibility
            for the supervision of the student
            researcher for the use and protection of
            any personally identifiable data and for

the appropriate dissemination of the results; and

(g) Two copies of the **SIMS Access Request Form** and **Security/Non-Disclosure Agreement**, one completed and signed by the student and the other completed and signed by the supervising faculty member.

c. All requests for access must be authorized by the applicable Dean, Director, Provost, Chancellor or Vice President and submitted to the SIMS Data Administrator for action.

d. The SIMS Data Administrator, or designee, receives all requests for access and may consult and coordinate with campus data custodians prior to approving/disapproving access or determining the specific data access privileges, such as which campus, files, and data elements.

e. If approved, the SIMS Data Administrator, or designee, will complete and submit the **Administrative Systems Sign On Request Form** (Attachment 4) to the Office of Information Technology Services for implementation.

8. <u>User Responsibilities</u>

a. Users are responsible for safeguarding their identification (ID) codes and passwords, and for using them for the period of time allowed and for stated purposes only. Each authorized user is responsible for all transactions made under the authorization of his or her ID, and for all network activity originating from his or her data jack.

b. Users are responsible for determining what data are appropriate for distribution, the audience for distribution, and the methods and timing of distribution. In all cases, the provisions of FERPA apply.

c. Every user shall ensure compliance with any
    regulatory requirement or UH policy and provide
    necessary assurances that the provisions of FERPA
    are observed. Requirements relating to the
    maintenance of FERPA are contained in 34 C.R.F.,
    section 99.1-99.67; Chapter 20-20, Hawai'i
    Administrative Rules; and University of Hawai'i
    Administrative Procedure A7.022. Failure to abide
    by these provisions will, at a minimum, result in
    termination of access and denial of further access
    to the SIMS database.

d. Users will not engage in the following activities.
    Information and/or evidence to the contrary will,
    at a minimum, result in termination of access and
    denial of further access to the SIMS database:

    (1) Disrupt or interfere with the access or
         administration of SIMS.

    (2) Use SIMS for commercial or profit-making
         purposes without written authorization from
         the University.

    (3) Allow access to SIMS by unauthorized users.

    (4) Use SIMS for illegal activities. Criminal
         and illegal use may include threats,
         harassment, theft, and unauthorized access.

9. Enforcement

a. Suspected or known violations of any provision of
    the administrative procedure should be reported
    immediately to the computing unit of the
    respective UH campus, the SIMS Data Administrator
    and the applicable Dean, Director, Provost,
    Chancellor or Vice President who authorized access
    to SIMS. All actions necessary to secure the SIMS
    database will be taken.

b. Violations will result in: suspension or
    revocation of current and future access privileges
    and associated computer resources; faculty, staff
    or student disciplinary action; and/or legal
    action.

UNIVERSITY OF HAWAI'I
Student Information Management System (SIMS)
Access Request Form

I. Requestor			
Name of User (Last, First) ☐ Permanent ☐ Temporary ☐ Student		SSN	Date
Campus	Department/Office	Position	
Campus Address	Electronic Mail Address		Campus Phone
Existing administrative user of mainframe computer on Manoa Campus? ☐ Yes User ID (RACF) _____ ☐ No			
Description of Intended Use (include campus, data elements and semester/year needed and duration of project). Attach separate sheet if necessary.			
Authorization: Dean/Director/Provost/Chancellor/Vice President Name _____ Signature _____ (Print or Type)			Date

Send Access Request Form, Security/Non-Disclosure Agreement and, if applicable, Student Researcher Form to: Office of the Vice President for Planning and Policy
2444 Dole Street, Bachman 110
Honolulu, Hawaii 96822

II. For OVPPP Use Only	
Consulted with campus data custodian(s)? ☐ Yes ☐ No Comments:	

☐ Access Approved
   Duration:
   Campus(es):
   File(s):
   Data Elements:	

☐ Access Disapproved Reason:	
SIMS Data Administrator or Designee Name_____ Signature _____ (Print or Type)	Date

UNIVERSITY OF HAWAI‘I
Student Information Management System (SIMS)
Security/Non-Disclosure Agreement

Access to personally identifiable information from student education records maintained as part of the University of Hawai‘i's Student Information Management System is subject to the requirements of the Family Education Rights and Privacy Act (codified in 20 U.S.C., section 1232g), as amended; federal regulations as adopted by the U.S. Department of Education to implement this act (codified in 34 C.F.R., section 99.1-99.67), as amended; Chapter 20-20, Hawai‘i Administrative Rules, entitled "Protection of Educational Rights and Privacy of Students;" and UH Administrative Procedure A7.022. Information related to student academic performance may be accessed by approved users of the University of Hawai‘i's Student Information Management System in accordance with the following stipulations:

1. This information will be used solely for curriculum analysis and educational improvement.

2. Personally identifiable information may not be re-disclosed to any other person except authorized education officials with a legitimate educational interest. (See UH Administrative Procedure A7.022 for the definition of *authorized education officials*.)

3. The mention of any personally identifiable information in all written reports, proceedings, memoranda, and minutes is prohibited.

4. Personally identifiable information contained in printed form shall be stored in a secure location.

5. When personally identifiable information is no longer needed, it shall be destroyed in a manner that is consistent with the confidential nature of its content.

6. Each user is responsible for maintaining the integrity and security of his or her individually assigned account, ID/password, or other user identifier. Such individually assigned identifiers shall not be communicated by any means to any other person and should be deleted upon termination of employment with the University of Hawai‘i or completion of time-specific research projects.

I agree to the above stipulations and understand that any unauthorized disclosure of student information may subject me to legal action and University of Hawai‘i sanctions including immediate termination of access and denial of future access.

_____   _____
                Print Name   Signature

_____   _____
                   Title   Date

UNIVERSITY OF HAWAI'I
Student Information Management System (SIMS)
Student Research Form

I. Student Researcher		
Name of Student (Last, First)	SSN	Date
Description of Research Project (attach separate sheet if necessary)		
Specific Data Needed (include campus, semester/year, data elements, cohort)		
Method Used to Protect Confidentiality of Personally Identifiable Information		
How Results of Research Will Be Used and by Whom		

II. Supervising Faculty Member	
Name (Print or Type)	Campus
College	Department

As the supervising faculty member, I certify that: the student researcher is a classified student who has acquired basic research and statistical skills as an upper-division baccalaureate or graduate student; the research topic is of legitimate educational interest or value to the University of Hawai'i; and the research design meets academic requirements. Furthermore, I accept responsibility for the supervision of the student researcher, for the use and protection of any personally indentifiable data, and for the appropriate dissemination of the results.

Signature _____   Date _____

III. Dean	
☐ Approved ☐ Disapproved Name _____ Signature_____ (Print or Type)	Date

Attach two copies of the *Access Request Form* and the *Security/Non-Disclosure Agreement*   one completed and signed by the student and the other completed and signed by the supervising faculty member   and send to: Office of the Vice President of Planning and Policy, 2444 Dole Street, Bachman 110, Honolulu, HI 96822.

ADMINISTRATIVE SYSTEMS SIGN ON REQUEST FORM

I. TO MIS APPLICATION MANAGER

01. Name of System Coordinator	02. Date
a. Print _____	a. Current Date _____
b. Signature _____	b. Effective Date _____

03. Name of User (Last, First) ☐ Regular ☐ Student/Casual ☐ Other	04. SSN

05. Department

06. Campus Address (if non-regular employee)

07. Existing Administrative User?	08. Is Employee Terminating From the UH?
☐ Yes ☐ No User ID (RACF) _____	

09. Action (check desired action)

☐ Add Activities	See Back of Form	
☐ Delete Activities	See Back of Form	
☐ Change Name	Old Name	Check if Want New User ID Created ☐
☐ Change Department/Address	New Department/Address (if non-regular employee)	
☐ Correct SSN	SSN	

II. For MIS Use Only

RACF User ID	Initial/Date	Natural Group
Created	| | | |	
Deleted	Top Menu	RACF Group
RACF Password	Comments	

MSO Form-425

UH ADMINISTRATIVE SYSTEMS LIST

BUDGET SYSTEM

Add	Delete	
☐	☐	BJ Summary Worksheet-36
☐	☐	BJ System-35
☐	☐	BJ Code Table-70
☐	☐	BJ Security Table-70
☐	☐	BJ Batch Submission-70

STUDENT SYSTEMS

Add	Delete	
☐	☐	CAPIS
☐	☐	Codeset Update/Retrieval
☐	☐	FUTURE Project (DARS)
☐	☐	Natural (FUTURE)
☐	☐	ISIS
☐	☐	Student Aid Information System
☐	☐	Student Loan Maintenance (60,151)
☐	☐	Student Loan Access (60,152)
☐	☐	Student Loan Table Maintenance(60,153)
☐	☐	Student Loan Table Access (60,154)
☐	☐	Student Loan User Maintenance (60,155)

HUMAN RESOURCES INFORMATION SYSTEMS

Add	Delete	
☐	☐	HRIS

FISCAL SYSTEMS (Accounting)

Add	Delete	
☐	☐	Account Master Access (27)
☐	☐	Account Master Update (28)
☐	☐	Customer Master Access (3)
☐	☐	Customer Master Update (4)
☐	☐	Fis Tran Retrieval (9)
☐	☐	Fiscal Transaction Access (45)
☐	☐	Fiscal Transaction Update (44)
☐	☐	Object Symbol Access Menu (60,102)
☐	☐	Object Symbol Update Menu (60,101)
☐	☐	Weekly Cash Balance Maintenance(60,103)

FISCAL SYSTEMS (Disbursing)

Add	Delete	
☐	☐	Foreign Vendor Master Maintenance (60,141)
☐	☐	Foreign Vendor Master Access (60,142)
☐	☐	Vendor Master Access (1)
☐	☐	Vendor Master Update (2)

CONTRACTS AND GRANTS

Add	Delete	
☐	☐	CGIS Account Master Maintenance (60,130)
☐	☐	CGIS Account Master Access (60, 131)
☐	☐	CGIS RTBSR Master Access (60,132)
☐	☐	FREDI Trans File Maintenance (60,133)
☐	☐	LOC Code Maintenance (60,134)
☐	☐	LOC Code Access (60,135)

EQUIPMENT INVENTORY

Add	Delete	
☐	☐	Equipment Description Table Update (41)
☐	☐	Equipment Master Update (5)

SCOPIS

Add	Delete	
☐	☐	SCOPIS Master File Maintenance Menu(60,111)
☐	☐	SCOPIS Master File Access Menu (60,112)
☐	☐	SCOPIS Code Table Maintenance (60,113)
☐	☐	SCOPIS Code Table Access Menu (60,114)
☐	☐	SCOPIS Payment Input Menu (60,115)
☐	☐	SCOPIS Auto Payment Input Menu (60,116)
☐	☐	SCOPIS Scan Sheet Printing Menu (60,117)

DATA WAREHOUSE

Add	Delete	
☐	☐	HRIS (Indicate valid area/orgs in comments box)

COMMENTS:

For Fiscal Transaction Update

Batch From	Range To	Enc (01)	Paymt (02)	Treas Dep (03)	JV/AR (04)	Allot LV4 (05)	Allot LV5/6 (06)
_____	_____	☐	☐	☐	☐	☐	☐
_____	_____	☐	☐	☐	☐	☐	☐
_____	_____	☐	☐	☐	☐	☐	☐

MSO Form - 425