

**Financial Policy & Procedure Instructions Manual  
FPI E-3 Online Access**

- I. PURPOSE
  - II. POLICY
  - III. GENERAL
  - IV. PROCEDURES
- 

**I. PURPOSE**

To describe policies and procedures for authorizing and monitoring on-line access to the University's core computer systems, including the Campus Information System (CIS), CASHNet, Financial Records System (FRS), Human Resource Management System (HRS), Integrated Student Information System (ISIS), and Student Accounts Receivable System (SARS).

**II. POLICY**

On-line access to the above systems is restricted to those individuals who have obtained written approval from the responsible department head, the organization responsible for the system, and the Information Systems department. Authorization should be obtained through the use of the access application for each system:

CASHNet - <http://www.colostate.edu/Depts/BusFin/fpicash.html>

FRS - <http://www.colostate.edu/Depts/BusFin/fm.html>

HRS - <http://www.hrs.colostate.edu/datasys/index.html>

ISIS - <http://www.casa.colostate.edu/advising/facman/chapter5/ISIS.cfm#access>

SARS - <http://wsprod.colostate.edu/cwis329/forms/staff/sarsform.pdf>

Once approval has been obtained, access will be limited to data and functions for which the individual has responsibility. Unique passwords will be assigned to the individual user. Initiating a change to a password is the responsibility of the user and should be done whenever security has been violated. It is standard practice for security packages to require users to change their passwords periodically. The purpose is to limit risk associated with unauthorized persons using someone else's password to access the system.

Users granted access understand that information retrieved, processed or communicated through the University computer systems is sensitive and/or confidential. Unauthorized release of such information or release of access codes at any time during or after employment with Colorado State University is a violation of University policy and state law. Violations may be reported to the Larimer County District Attorney and/or Colorado Attorney General. Access will be used for authorized purposes as related to the user's assigned duties. Personal use of systems' information is not authorized.

Use of on-line access will be monitored by the security coordinator of each system to reduce the risk of security violations and to identify weaknesses in the security system.

**Financial Policy & Procedure Instructions Manual**  
**FPI E-3 Online Access**

**III. GENERAL**

Responsibilities associated with on-line systems access involve different individuals or organizations.

- A. Information Systems provides administrative computing services to academic and administrative offices through management of institutional level core computer systems. Information Systems is responsible for the design, implementation, enhancement, maintenance, and production services of the core computer systems. An IBM mainframe computer (IBM 9672 R21) is used to support core computer systems.
- B. The security coordinator in Information Systems coordinates the establishment and maintenance of user IDs and passwords to ensure that access is restricted to authorized users.
- C. Business & Financial Services-Bursar's Office specifies and approves the parameters for access to the CASHNet System.
- D. Business & Financial Services-Systems Management Office specifies and approves the parameters for access to the FRS, Travel Manager, the FRS modules of the Campus Information System, and Delphi.
- E. Human Resource Services-Data Systems Office specifies and approves the parameters for access to the HRS, and the HRS modules of Delphi.
- F. Enrollment Services-Systems Support specifies and approves the parameters for access to the ISIS, the ISIS modules of the Campus Information System, and Delphi.
- G. Student Accounts Receivable specifies and approves the parameters for access to the SARS and the SARS modules of Delphi.
- H. Users are responsible for the appropriate use of the University computer systems and to ensure that password security is maintained.
- I. User departments are responsible to ensure that they approve access to appropriate users.

**IV. PROCEDURES**

System access request forms must be completed and approved before access will be granted. These steps should be taken in obtaining approval for system access:

- A. Confirm that you have a compatible PC and that it is connected to the University IBM mainframe computer. (Contact your departmental LAN manager with questions.)
- B. Complete an access application for each system you are requesting access for and submit it to the appropriate security coordinator. The access application must be signed by the individual requesting access and the department head.
- C. Information Systems will assign you a unique accessor ID (ACID) & password. Logon instructions will be provided to you.
- D. The security coordinator for each system that you request access for will contact you with specific instructions related to that particular system.