Original Approval Date: September 5, 2009 **Most Recent Approval Date:** July 13, 2012

Last Edited: December 11, 2017

Parent Policy: Administrative Information Systems Security Policy

Administrative Information System Access and Maintenance Procedure

Office of Administrative Responsibility:	Administrative Information Systems
Approver:	Information Technology Security Committee
Scope:	Compliance with this University-wide procedure extends to all members of the University community

Overview

The University's Administrative Information Systems (AIS) unit is responsible for managing the institution's administrative (Human Capital Management, Financial and Campus Solutions) systems. The systems are primarily PeopleSoft applications. The University meets its system operating and development needs through on-going working collaborations with select external service providers, currently IBM Global Services and Tata Consultancy Services (TCS). AIS manages the work of these service providers and co-ordinates with central departments and users of these systems.

The University's Academic Information and Communication Technologies (AICT) unit holds the authority to issue Campus Computing ID's (CCID) which grants user access to the University's computing systems and facilities. The CCID along with a user-unique password are both critical aspects of maintaining the integrity of the University's computing environment. In turn administrative system security is a function of limiting user access according to an employee's position-specific related duties and responsibilities. This is achieved through the appropriate assignment of security access through PeopleSoft roles to the CCID's.

The security and integrity of AIS applications can only be assured through the appropriate due diligence of all involved in maintaining, supporting and using these applications. Thus system security is a shared responsibility.

Purpose

To inform eligible Users of AIS applications how to obtain PeopleSoft security roles.

To identify those having roles related to the security of AIS applications and clearly state these responsibilities.

PROCEDURE

1. How To Obtain Access To Peoplesoft Applications:

   a. User must have a CCID and a defined relationship to institution before they can be given access to PeopleSoft applications. A CCID is created on the earliest start date of a user's relationships with the University. A CCID will expire when all of their multiple, simultaneous relationships have ended.
   b. User completes the appropriate Request for Administrative Information Systems Access Form indicating desired Operator **Role Name**. There are six forms:
      - Request for Administrative Application Access – Ad Astra
      - Request for Administrative Applications Access – PeopleSoft Financials
      - Request for Administrative Applications Access – PeopleSoft eTRAC
      - Request for Administrative Applications Access – PeopleSoft Campus Solutions
      - Request for Administrative Applications Access – PeopleSoft Human Capital Management (HCM)
      - Travel & Expenses Independent Reviewer Security Request

      These forms are stored in the Administrative Information Systems Forms Cabinet.

HCM access can also be granted using the online Security Smart Form available to Authorized Approvers in PeopleSoft HCM. A link to the PeopleSoft HCM database is available on the AIS website.

2. The unit's Authorized Approver must sign the Form, approving system access consistent with the Security Roles indicated. An Authorized Approver cannot delegate this authority to another. A list of Authorized Approvers is located on the AIS Website by signing into the AIS Support Site. Contact the AICT Helpdesk (helpdesk@ualberta.ca or 780.492.9400) to request the username and password for the AIS Support Site.
3. The appropriate Project Holder (Principle Investigator) must sign the eTRAC form, approving access to their research grant information.
4. Submit the Form to AIS Security Forms (aissecurityforms@ais.ualberta.ca) using the email or fax number indicated on form.
5. As needed for certain specified Security Roles, TCS will conduct 'call back' validations. That is, they will call the central unit responsible for the business area and confirm that the Security Role can be assigned to the User.
6. Request is processed by TCS, who retains the forms on file. TCS will check to ensure the User has at least one relationship to institution that is active and appropriate for the Security Role being requested.
7. TCS notifies User and Authorized Approver that security roles have been granted.
8. All Users must consent to an on-line confidentiality agreement before any sign-on to PeopleSoft systems will be allowed. If the User has not yet consented to the terms in the on-line confidentiality agreement, they will be prompted at sign-on for the consent, and once the consent has been given, the sign-on can proceed.

How To Maintain User Access to AIS Applications (withdraw 'PeopleSoft ID or change roles)

In the event of any change relevant to a User's administrative system access (i.e. change in employment status, department transfer, change in responsibility), the Authorized Approver should submit a revised Request for Administrative Information Systems Access Form in a timely fashion. If the security change relates to a single or a limited set of applications, then the forms described in step 1b should be used. If the User is to be removed from all PeopleSoft databases, then the form intended to delete the User from all databases should be used:

- Request for Administrative Applications Access – PeopleSoft Delete

A listing of administrative system Users will be distributed annually from AIS to the Authorized Approvers, so they can review and ensure that all PeopleSoft security access is appropriate to each User's duties and responsibilities. This practice is intended to catch oversights and is not to be relied upon as the only means to maintain appropriate User access to the University's administrative systems.

Dynamic Roles

There are several Dynamic Security Roles that are assigned based on a person's Relationship to the Institution and/or are based on data within PeopleSoft, such as being a member of a Project Team. These Security Roles are created and expired through automated processes.

- Bear Tracks Employee
- Bear Tracks Applicant
- Bear Tracks Student
- Bear Tracks Prospect
- Bear Tracks Instructor
- Bear Tracks Continuing Education Student
- Travel and Expense Self-Entry
- Purchasing Requester Entry
- Financials Approver (Travel & Expenses and Purchase Requisitions)
- Financials Department Manager Inquiry and Reporting
- Financials Delegated Approver (Travel & Expenses and Purchase Requisitions
- eTRAC Project Team Members
- Researcher Home Page
- Authorized Approvers
- Dean, Director, Chair (DDC)
- ePAF smart form project manager approval
- ePAF smart form project manager approval delegation authority

Administrative System Application Access Security Related Responsibilities

Administrative Information Systems (AIS)

To ensure access to AIS applications is only attained through an established procedure that affords an appropriate degree of control.

To ensure those involved in this procedure have a clear understanding of their related responsibilities.

Tata Consultancy Services (TCS)

TCS is the University's application service provider in maintaining and supporting certain aspects of the University's computing systems. TCS is responsible to execute their role in providing access to these systems in a procedure compliant, timely and careful matter. TCS retains files of access requests, and approvals.

User

To support the integrity of the University's computing system through procedure compliance and safeguarding their CCID's and passwords.

Faculty/Department/Unit

To identify and provide signature verifications for their Authorized Approvers and ensure these persons comprehend the significance of their role in managing access to the University's administrative computing.

To advise AIS, on an on-going basis, of changes in their Authorized Approvers and respond upon request from AIS, to confirm their list of Authorized Approvers and the security access of their approved users.

Authorized Approvers

To support the integrity of the University's computing system through procedure compliance and ensuring their approvals reflect an appropriate degree of due diligence.

To advise TCS on an on-going basis of any user related change (i.e. employment status, transfers) that will impact their security access.

No less than annually, review the appropriateness of the unit's entire system access, being careful to ensure that each User's security is consistent with their position-specific duties and responsibilities.

DEFINITIONS

Any definitions listed in the following table apply to this document only with no implied or intended institution-wide use. [▲Top]

Security Role Name	For each AIS application (i.e. HCM, Campus Solutions or Financials), the Security Role Name denotes a specific user profile that outlines a unique set of processes that users, set up under that Role Name, are given access/allowed to do.
Authorized Approvers	Employee(s) within a faculty/department/unit who have been authorized by their Dean, Director or Chair and identified to AIS as having the authority to approve user access to the University's AIS applications and decide what processes that user is to be allowed to do. Only employees of the University of Alberta can be Authorized Approvers.

FORMS

Should a link fail, please contact uappol@ualberta.ca. [▲Top]

Administrative Information Systems Forms Cabinet

RELATED LINKS

Should a link fail, please contact uappol@ualberta.ca. [▲Top]

Administrative Information Systems (University of Alberta)

Information Technology Use and Management Policy (University of Alberta)