Original Approval Date: December 10, 2010
Most Recent Approval: December 10, 2010
Editorial Amendments: December 12, 2025

Parent Policy: Information Technology Security Policy

Administrative Information System Access and Maintenance Procedure

Office of Administrative Responsibility:	Administrative Information Systems (AIS)
Approving Authority:	Technology Strategy Oversight Committee (TSOC)

Purpose

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.

The purpose of this policy document is to inform eligible users of AIS applications how to obtain PeopleSoft security roles, and to identify those having roles related to the security of AIS applications and clearly state these responsibilities.

Definitions

The attached definitions table outlines the terms used in this policy document and any specific rules of interpretation that apply.

Scope

This policy document applies to the University Community.

Procedure

1. HOW TO OBTAIN ACCESS TO PEOPLESOFT APPLICATIONS:

    a. User must have a CCID and a defined relationship to the 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:

        i. Request for Administrative Application Access – Ad Astra

        ii. Request for Administrative Applications Access – PeopleSoft Financials

        iii. Request for Administrative Applications Access – PeopleSoft eTRAC

        iv. Request for Administrative Applications Access – PeopleSoft Campus Solutions

        v. Request for Administrative Applications Access – PeopleSoft Human Capital Management (HCM)

        vi. 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.

    c. 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.

    d. The appropriate Project Holder (Principal Investigator) must sign the eTRAC form, approving access to their research grant information.

    e. Submit the Form to AIS Security Forms (aissecurityforms@ais.ualberta.ca).

f. 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.

g. Request is processed by TCS, who retains the forms on file. TCS will check to ensure the user has at least one relationship to the institution that is active and appropriate for the Security Role being requested.

h. TCS notifies user and Authorized Approver that security roles have been granted.

i. 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.

2. 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:

a. 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.

3. 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.

a. Bear Tracks Employee

b. Bear Tracks Applicant

c. Bear Tracks Student

d. Bear Tracks Prospect

e. Bear Tracks Instructor

f. Bear Tracks Continuing Education Student

g. Travel and Expense Self-Entry

h. Purchasing Requester Entry

i. Financials Approver (Travel & Expenses and Purchase Requisitions)

j. Financials Department Manager Inquiry and Reporting

k. Financials Delegated Approver (Travel & Expenses and Purchase Requisitions

l. eTRAC Project Team Members

m. Researcher Home Page

n. Authorized Approvers

o. Dean, Director, Chair (DDC)

p. ePAF smart form project manager approval

q. ePAF smart form project manager approval delegation authority

4. ADMINISTRATIVE SYSTEM APPLICATION ACCESS SECURITY RELATED RESPONSIBILITIES

a. Administrative Information Systems (AIS)

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

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

b. Tata Consultancy Services (TCS)

i. 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 manner. TCS retains files of access requests, and approvals.

c. User

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

d. Faculty/Department/Unit

i. 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.

ii. 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.

e. Authorized Approvers

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

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

iii. 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 Table

Any definitions listed here apply to this policy document only with no implied or intended institution-wide use. For clarity, defined terms listed here include grammatical variations thereof.	
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 and/or 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

- Security Forms and Information
- Enterprise Applications Forms Cabinet

Parent Policy Suite

- Information Technology Security Policy
- Accounts and Access Procedure
- Administrative Information System Access and Maintenance Procedure
- Encryption Procedure
- Requesting Variance to IT Security Procedure
- Remote Access Procedure
- University Campus Network Procedure

Related Policy Documents

- Information Technology Use and Management Policy

Related Links

- Information Services and Technology (IST)
- Technology Governance

History

- September 9, 2009 Approved.
- July 13, 2012 Approved.
- May 8, 2025 Editorial amendment. Formatting, office name and links.
- December 12, 2025 Editorial amendment. Formatting and links (previously approved under the *Administrative Information Systems Security Policy*, rescinded).

For questions surrounding policy document interpretation or implementation, please contact the Office of Administrative Responsibility.

The official version of this document may be obtained from https://www.ualberta.ca/policies-procedures/index.html