5.8.16 Administrative System Access Control Program

Chapter 5 - Information Technology	Original Effective Date: June 2002
Section: 5.8 Information Security	Date Last Reviewed: August 2022
Responsible Entity: Chief Information Security Officer	Date Last Revised: August 2022

I. Purpose

UT Health San Antonio administrative business systems contain information that is critical to operations, confidential in nature, strategic in decision support, and in many cases protected by UT System policy with accompanying audit requirements. This policy outlines the requirements, responsibilities, appointment, and resources for Access Control Executives (ACEs). Each aspect of this policy is to provide assurance that administrative business systems are protected, that effective business processes are in place and enforced, that the resulting transactional data assets of the institution are preserved, and that each aspect complies as held accountable by audit.

II. Scope

The policy applies to all faculty, staff, students, residents, healthcare providers, researchers, contractors, or any other third party entities who have direct or indirect access to data created, held, or maintained by any UT Health San Antonio controlled affiliate, including, but not limited to its clinics, hospitals, and research operations.

III. Policy

Individuals are granted access control roles from the highest appropriate level with subsequent ascending review and approval through the vice president and chief financial officer (VP/CFO). The service center director appoints the service center administrator (SC Admin). The department/unit chief, chair, or director appoints the departmental access control executive (ACE).

For the remainder of this document, both SC Admins and ACEs will be referred to as “ACE” unless the policy and procedure differ for their respective responsibilities. The ACE will grant user privileges either within an application or via the Personal Security Access Request (PSAR), a limited access service request.

A. Requirements

1. All UT Health San Antonio departments are required to have a designated ACE and each administrative service center is required to have a designated SC Admin to authorize and manage user access to institutional administrative business systems. See Institutional Handbook of Operating Policies (IHOP) policy 6.1.11, PeopleSoft E-Procurement Requisition (REQ) Purchases and Payments.

2. In order to designate a new or replacement Access Control Executive or Service Center Admin, the current ACE must complete a Access Control Designation Form, secure approvals from dean, chair, or director, and the Office of the Vice President and Chief Financial Officer (VP/CFO), then submit the form as a service request via a link on the My UT Health ACE page. This service request link requires elevated access and is only accessible to current ACEs. The My Service Center request is then processed by the Application Security Team. If no dean, chair, or director exists for a department or unit, only the VP/CFO can appoint the ACE.

B. Responsibilities

1. UT Health IT - Business Support Services (BSS)

   Administrative system access control is the custodial responsibility of UT Health IT BSS. The delegation of access management is accomplished through policy, implemented in two roles, the first at the administrative service center level for transactions, and the second at the department level for operational activity and reporting.

2. Access Control Executive (ACE)

   The "Guide to Access Control" documents the ACE responsibilities and procedural compliance requirements. In summary, it is the responsibility of the ACE to:

   a. Understand university policies and procedures, internal controls, and the department's business processes and organizational structure.

   b. Assign appropriate security access to all application systems. Departmental users should be assigned access privileges based on job duties, or on a “need-to-know” basis.

   c. Ensure approval cycles support appropriate separation-of-duties and good internal controls. If the ACE reconciles departmental accounts, there must be a documented review of the reconciliations at a higher management level.

   d. Manage departmental user access including both in-app activity and the submission of service requests to immediately disable access for users that transfer, terminate, or no longer have a need to access administrative business systems.

e. Ensure all departmental users of administrative business systems receive both formal systems training, and training related to departmental procedures and accounts.

f. Ensure all departmental computers accessing administrative business systems are appropriately secured.

g. Attend access control training on a routine basis as systems, procedures, or polices are changed.

h. Manage the electronic administrative mailbox, which is established for internal control of routine departmental business; and,

i. Serve as a liaison between user communities, administrative departments, and IT in the use of UT Health SA administrative business systems.

3. Department/Unit-level Leadership

The dean, chair, or director of a department/unit is responsible for ensuring the ACE attends appropriate training and reviews user security access to administrative systems on at least an annual basis. To document the completion of this requirement, the ACE will participate in an annual system user audit with records maintained by UT Health IT-Business Support Services (BSS).

IV. Definitions

There are no defined terms used in this policy.

V. Related References

The My UT Health Business Application User Support ACE page contains links to guides, job aids, references, and service requests related to administrative access controls.

VI. Review and Approval History

A. The approving authority of this policy is the University Executive Committee.

B. The review frequency cycle is set for three years following the last review date, a time period that is not mandated by regulatory, accreditation, or other authority.

Effective Date	Action Taken	Approved By	Date Approved
06/2002	Policy Origination		
05/2018	Policy Revision		
08/2022	Policy Revision, discretionary edits	CISO/ICPO	08/29/22