Access to Electronic Records Held in Accounts Subsequent to Termination, Departure or Death Protocol

ITS Protocol

Pursuant to the University at Albany Information Security Policy, this protocol is established as part of the Access Control Security Domain.

Security Domain

The Access Control Security Domain establishes that access to University Business Information is governed by the principle of “least privilege” and employs industry-accepted access control and authorization frameworks to ensure that external and internal computer applications and persons have only such access as is appropriate to information resources, and to facilities and devices containing and displaying information.

Objective

This protocol establishes that a formal process be developed for requesting and granting access to electronic records held in University at Albany personal accounts subsequent to the termination, transfer, departure, or death of the faculty member, student, or employee to whom the account was issued.

Background

Numerous laws and regulations apply to the release and disclosure of certain types of business and personal records created, collected, stored, and used by the employees and students at the University at Albany in the course of business, research, and academic activities. Information subject to these laws and regulations may be held in accounts that are issued by the University to specific individuals (Personal Accounts) for the purpose of conducting its daily operations, e.g., email accounts, Active Directory accounts, Unix accounts. In the event of an employee or student's termination, transfer, departure, or death, the University may be subject to internal and external requests from various parties for electronic records contained in a Personal Account. Therefore, the University has formulated this protocol to establish standards and procedures to properly manage requests for business records and personal information under these circumstances.

Scope

This protocol applies to all University at Albany employees and students.

Roles and Responsibilities

All requests for access to the electronic records of terminated, transferred, departed, or deceased employees and students must be reviewed and approved, in writing, by the University’s Office of Legal Counsel prior to releasing the records, all such requests being subject to any and all applicable laws.

Office of Legal Counsel

It is the responsibility of the Office of Legal Counsel to draw up and publish procedures for submitting requests for access to a terminated, transferred, departed, or deceased employee or student’s computing account(s). The Office of Legal Counsel shall also publish guidelines informing the campus community of the types of information whose release is governed by law and the applicable statutes.

Information Technology Services (ITS)

ITS shall assist in the formulation of procedures requesting the release of account information and shall provide the proper access controls to ensure that access is in compliance with the Office of Legal Counsel's conditions.

ITS shall also assist the Office of Legal Counsel in ascertaining the nature of material stored in the account for the purpose of determining whether or not the information is subject to legal regulations.

Other Campus Providers of Electronic Accounts and Storage

Account services and storage are provided by many independent entities across campus. The individuals or offices responsible for managing these account assignments and access controls, independent of central IT services, are responsible for assisting the Office of Legal Counsel in ascertaining the nature of material stored in the account for the purpose of determining an appropriate response to a request for access, as well as assuring compliance with the terms and conditions of account access established by the Office of Legal Counsel.

Individuals or Offices Seeking Account Access
Individuals or offices seeking access to information stored in the accounts of terminated, transferred, departed, or deceased employees or students are required to follow the procedures published by the Office of Legal Counsel for this purpose.

Upon receipt of written authorization from the Office of Legal Counsel to access the specified information, individuals or offices seeking access shall comply with the stipulations and limits as set forth by the Office of Legal Counsel in the written authorization.

Compliance

All parties are bound by the terms and conditions of the written authorization for access. The service providers who manage the account in question shall take what measures are appropriate to ensure that access is in compliance with the terms and conditions of the written authorization.

Review

This protocol and all related published documents will be reviewed no less than once every three years.

Related Documents

Request for Access to a University at Albany Personal Account Subsequent to Termination, Departure, Transfer, or Death
SUNY Procedure #6608: Information Security Guidelines, Part 1: Campus Programs & Preserving Confidentiality
Federal Educational Rights and Privacy Act
Health Insurance Portability and Accountability Act
Gramm Leach Bliley Act
Freedom of Information Law
NYS Surrogates Court Procedures Act
NYS Information Security Breach & Notification Law
NYS Business Law and Technology Law
NYS Governmental Accountability, Audit & Internal Control Act
NYS Information Security Policy P03-003
SUNY Policies of the Board of Trustees

Need more help? Contact the ITS Service Desk.