

## Termination of User Access Policy

(2.22.05)

### Purpose

The principle of access control is to limit access to users who have valid reasons for accessing computers, systems, or data. Access control is a key component of information security. It is critical that access privileges be revoked in a timely manner when users terminate their relationship with the University or transfer to a job with different duties and responsibilities.

### Scope

This policy applies to all members of the University at Buffalo community (students, faculty, staff, contractors, volunteers, consultants, temporary employees, visitors) with access to UB computing or networking resources.

### Policy

Access privileges must be revoked immediately upon notification when a user no longer has a need for such access.

### Responsibilities

**Supervisors** are responsible for notifying their local department administrator (appointment person) when an employee, including a student or graduate assistant, terminates appointment or transfers to a new position with new duties and responsibilities.

**Local Department Administrators** responsibilities:

- Sending email to the alias [ub-account-term@buffalo.edu](mailto:ub-account-term@buffalo.edu), notifying those who administer central accounts (UB IT, Infosource, and mainframe accounts) that an employee has terminated appointment or transferred to a new position with new duties or responsibilities, and that access to centrally-administered accounts must be reviewed and appropriate action taken. In the case of Infosource access, the appropriate **access control administrators** will be notified that the employee has terminated appointment or transferred to a new position and that access must be reviewed and appropriate action taken.
- Consulting with the local IT support manager: notifying the manager that an employee has terminated appointment or transferred to a new position with new duties or responsibilities, and that access to department accounts and resources must be reviewed and appropriate action taken.

**Access Control Administrators** are responsible for revoking the access of users who no longer have a need for access to data.

**The CIO** is responsible for communicating, maintaining and enforcing this policy.