Capital
University
Ask. Think. Lead.

Policy Number: 500-1

Section: Information Technology

Title: User Account Policy

Effective Date: July 1, 2020

Date Issued: June 3, 2008

Revised Date: June 22, 2020

Review Date: Annual review

Attachments:

Responsible University Officer: Vice President for Business & Finance

Responsible Office: Department of Information Technology

Applies to: Capital University Employees, Students, Contractors, and Guests

I. Overview

Informational resources and assets owned by Capital University are protected by means of user account management processes that include standards for authorizing and revoking access. Employees, students, contractors, emeriti and guests in good standing are granted access once their relationship and role with the University have been properly vetted.

All users must conform to all current University policies and procedures. Access to University resources and assets is a privilege, not a right, imposes certain responsibilities and obligations, and is subject to University policies, local, state, and federal laws.

II. Purpose

The purpose of this policy is to establish a standard for effective account management procedures that promote security and integrity of University information systems and assets. This includes user account creation, administration, usage, and deactivation. University resources and assets are to be used by authorized individuals for legitimate educational, research, academic, and administrative purposes.

III. Scope

This policy applies to all information systems, data, identities, computer/network assets and accounts that are used to access University-owned or leased resources on premise or hosted by a cloud service provider. This includes, but is not limited to, shared informational resources such as iLearn, WebAdvisor, myCap or Colleague, and computer/network systems. The policy covers departmental accounts as well as those responsible for the management of accounts.

IV. Account Management

1. Eligibility

All current Capital University employees, students, contractors, emeriti, and approved guests in good standing are eligible to have one Capital University account and email address based on role. Alumni may be able to obtain account services through the Capital Alumni Online Community, or other Alumni offered systems, managed by the Alumni Relations Office.

The Department of Information Technology will create network, e-mail, and other accounts on request after authenticating the identity of a user and validating their role and relationship with the University. Responsibility and role of users within the University will determine the request and account creation process.

All user accounts are subject to the Capital University Acceptable Use Policy (AUP). Use of an account indicates your acceptance of Capital University's Acceptable Use Policy and all other account related policies.

2. Managing Accounts

All accounts will periodically be reviewed to ensure that access and account privileges are commensurate with job function, need-to-know, and University status. Accounts may be revoked, locked or deactivated for users who no longer meet eligibility criteria. Accounts can be disabled for security risks, intrusions or acts that obstruct or disrupt system resources.

3. Account Duration

Employee accounts will remain active as long as the individual’s status with the University is in good standing.

Student accounts remain active while the student remains registered for courses with the University or is on approved leave of absence through the Office of the Registrar, and for one year after graduation.

Emeriti accounts are issued after an individual’s official employment with the University has terminated.

Exceptions must be approved by the University and arranged by the Department of Information Technology in advance.

4. Account Deactivation

Employee accounts will be deactivated immediately upon departure or termination from University employment, unless a prior special exemption is granted by Human Resources or the Provost’s Office

Upon graduation, student email accounts and myCap services will remain active for one year. Exceptions to this standard must be approved by the University. For students who have not graduated and (1) have not gone on official leave of absence; (2) have not registered for a course within one academic semester; or (3) do not have a prior special exception, their student email accounts and myCap services will be terminated after one year.

All other accounts will be deactivated when the account holder's status with the University is no longer active or no longer in good standing.

5. Account Deletion

The Department of Information Technology will periodically audit the University's information systems to determine which accounts, and the associated data, should be removed from the various systems. Timeframes for purging systems and data vary based on the type of account and the role of the user with the University.

V. Compliance

Capital University and/or the Department of Information Technology reserves the right to deny, limit, restrict, or extend privileges and access to any user accounts.

VI. Miscellaneous

Capital University through appropriate review and amendment, reserves the right to amend this policy at any time and without prior notice in order to provide better information and technology access to faculty, staff, students, contractors or any other individual using these accounts.

VII. CONTACTS

Capital University
Department of Information Technology
1 College and Main
Columbus, Ohio 43209
Email: helpdesk@capital.edu
Phone: 614-236-6508
Website: www.capital.edu/IT

VIII. HISTORY

Originally issued: June 3, 2008 approved by President's Cabinet
Revised: May 1, 2019 and June 22, 2020