Access Management Policy

Access Management Policy

Policy Contents

I. POLICY STATEMENT
II. REASON FOR POLICY
III. SCOPE
IV. AUDIENCE
V. POLICY TEXT
VI. PROCEDURES
VII. RELATED INFORMATION
VIII. DEFINITIONS
IX. FREQUENTLY ASKED QUESTIONS
X. REVISION HISTORY
XI. COMPLIANCE
XII. POLICY EXCEPTION PROCESS
XIII. APPENDICIES

Effective Date: 03-01-2015
Last Updated: 03-06-2015

Responsible University Officer:
Opinder Bawa
Vice President, Chief Information Officer

Policy Owner:
Director, Application Services

Policy Contact:
ITS Help Desk
I. POLICY STATEMENT
   A. Access to USF Information Technology Services will be granted to members of the University community as needed. When access is no longer required, such as following the last day of employment, access is removed.

II. REASON FOR POLICY
   A. This policy is intended to ensure that changes to access are performed in a timely manner to ensure that USF ITS provides secure, reliable IT services in compliance with applicable regulations and best practices.

III. SCOPE
   A. This policy covers granting and removing access to USF IT services.

IV. AUDIENCE
   A. This policy applies to all university users who have, or are responsible for, user and system accounts in USF IT systems that store or process information.

V. POLICY TEXT
   A. Granting Access
      1. Access to University systems and services shall only be granted to members of the University community with a need for such access, based upon their role(s) and/or specific job functions.
      2. Access will be provided in advance of start date for faculty but not for staff, unless approved by HR and the hiring manager.
      3. Please note that access preservation for retired employees will be granted upon request for retirees who meet requirements set by USF Human Resources and the Provost.
   B. Removing Access
      1. Following the last day of employment, staff continue to have access to myUSF and Self Service Banner payroll records for a period of 18 months.
      2. USF email and all other services will be discontinued following the last day of employment.
      3. Supervisors must inform the ITS Help Desk of all employee separations, including projected last date of employment.
      4. Following the last teaching assignment, faculty continue to have access to all USF IT services for a period of 18 months.
5. Following degree conferral, student access is converted to alumni access. Services provided to students that are not provided to alumni are discontinued.
6. Former students who have not graduated retain access to myUSF and Self Service Banner student account records for a period of 18 months.
7. ITS must ensure timely disabling and removal of access under ITS control, and inform other departments that administer systems of the need for access disabling and removal.

VI. PROCEDURES
A. (None)

VII. RELATED INFORMATION
A. (None)

VIII. DEFINITIONS
A. (None)

IX. FREQUENTLY ASKED QUESTIONS
A. (None)

X. REVISION HISTORY
A. 06-01-2010 – First publication
B. 03-01-2015 – Updated to new template

XI. COMPLIANCE
A. Failure to follow this policy can result in disciplinary action in accordance with Human Resources Employment Handbook and Office of General Counsel employee and labor relations. Disciplinary action for not following this policy may include termination, as provided in the applicable handbook or employment guide.

XII. POLICY EXCEPTION PROCESS
A. A proposed exception request to ITS Policy requires a formal e-mail explanation related and in support of job function.
B. A proposed exception request to ITS Policy, mentioned in 'XII.A', must be approved via email by respective department or division supervisor, Dean, or VP, before submitted to ITS for review.

C. Forward approved email as stated in 'XII.B' to itshelp@usfca.edu for processing.

D. Evaluation of ITS Policy Exception will escalate internally, and as applicable may include further review by: UITC subcommittee(s), the Information Security Officer, and others as appropriate at the request of VP for IT.

XIII. APPENDICIES

A. (None)