

## Account Privilege Policy

Applies To:	All	Policy Number:	ITS-0008
Issued By:	AVP for IT	Policy Version Number:	1.2
Date Issued:	March 1, 2005	Last Review Date:	December 1, 2016
		Last Revised Date:	December 1, 2016

### Policy

The University provides accounts to systems as needed to support academic and administrative work at the University.

Account credentials are individually provided for access to email, self-service, online resources, enterprise systems and other solutions as needed.

Access to accounts is considered a privilege that may be temporarily or permanently removed.

### Student Accounts

All student accounts are automatically generated from admissions information during the admissions process. This information is sometimes initially routed through the Financial Aid (FASFA) process or the transfer process.

Email accounts remain active for current students but will be systematically inactivated after 12 months of inactivity. Inactive accounts will be automatically removed and the information stored within the accounts will not be retrievable.

Self-service accounts remain active for current students but will be systematically inactivated after 12 months of inactivity. If permitted, inactive accounts will require revalidation prior to reactivation.

If storage has been granted, storage will be automatically removed and the information stored will not be retrievable.

### Applicant Accounts

Account access granted during the application process to prospective students will remain active for one term. If the applicant has not enrolled as a student, the account will be removed.

## **Employee Accounts**

Employee accounts may be requested by supervisors completing an ITS Account Application form and submitting it to Information Technology Services.

Students or alumni who become professional employees of the University will be governed by the terms for employee accounts and will sacrifice the rights and privileges received from student status. Work-study and non-workstudy positions are not considered professional employment.

All employees must review and sign the University FERPA policy as well as the University's Acceptable Use policy. Failure to do so will result in denial of the account applications.

Information Technology Services will verify all information on the form prior to granting access. Please note, other administrative areas have autonomy in granting access to the solutions they manage such as the Registrar, Human Resources, Finance and Advancement.

## **Employee Accounts at Time of Separation**

At the time an employee has separated from the University whether voluntarily, involuntarily, through resignation, contract completion, retirement, death or for any other reason from the University, access to University accounts will be removed.

This action protects the University, the separated employee and our students by ensuring University compliance with FERPA, HIPAA and other regulations.

Employees should take the previous statement seriously and avoid using their University accounts, specifically their University email account, for personal business matters, such as the point of contact for personal legal matters, utility bills, credit card bills and other private or time-sensitive communications. At the time of separation, access to current and future communications through the employee's account will cease to exist and not be retrievable.

In limited circumstances where high-profile activity passes through an account, such as Admissions employees, Advancement employees, Athletic employees, personal counsellors, wellness center employees and Title IX coordinators, the University may temporarily keep the account online to intercept business related communications and route those to the appropriate office. This ensures continuity of operations. The University maintains the right to forward business related incoming mail of a separated user to the appropriate office.

If individual storage has been granted, storage will be automatically removed and the information stored will not be retrievable.

Employees who have signed up for electronic W2's will receive a paper copy of their W2 from the Human Resources office.

In all cases, the separated employee is required to work through the appropriate contact in the Human Resources department. The Information Technology Services department will only respond to separated employee matters as provided from the Human Resources department. The Human Resources department will coordinate communication from and to the separated employee.

### **Employees with Academic History**

To ensure the security of University information that may be accessible from a separated employee's account, the employee's account will be immediately closed down. A separated employee who has need to access their academic information may request their information through the Registrar's Office.

### **Retirees or Employees who Return as Employees**

In cases where a retiree or separated employee returns to the University for official work, the supervisor is required to submit new account application paperwork with the prior TitanConnect number and prior user name.

If the returning employee's account is still active, the account will be cleansed and the employee will start with an empty account.

### **Employees or Retirees who Separate Employment from the University but are Current Students**

In cases where an employee has separated from the University and is actively enrolled in University courses, the University may grant a new account to the separated employee/student, cleanse the existing account of all University business related items and/or, intercept business related communications and route those to the appropriate office. It is critical that the separated employee take prior action to preserve any academic materials they wish to retain prior to their separation, since those prior materials will be removed from the account at time of separation and will not be retrievable. When a new account has been issued or Information Technology Services has completed cleansing the account, Information Technology Services will provide the necessary details to the Human Resources department for communication to the separated employee.

### **Employees or Retirees who Separate Employment from the University but Return as Students**

In cases where an employee has separated from the University and returns as a student and the account has yet to be removed from the University's domain, the University may grant a new account to the separated employee/student, cleanse the existing account of all University business related items and/or, intercept business related communications and route those to the appropriate office. It is critical that the separated employee take prior action to preserve any academic materials they wish to retain prior to their separation, since those prior materials will be removed from the account at time of separation and will not be retrievable. When a new account has been issued or Information Technology Services has completed the cleansing of the account, Information Technology Services will provide the necessary details to the Human Resources department for communication to the separated employee.

In cases where an employee has separated from the University and returns as a student and the account previously used has been removed, a new account will be created and fall under the terms in the Student Accounts section of this policy.

### **Vendors, Contractors, Student Employees, Temporary Employees, Volunteers, Visiting Guests, Religious Members of our Community and other Special Categories**

Accounts may be requested by supervisors completing an ITS Account Application form and submitting it to Information Technology Services.

For roles where access to University records may be required, the applicant must review and sign the University FERPA policy as well as the University's Acceptable Use policy. Failure to do so will result in denial of the account application.

Information Technology Services will verify all information on the form prior to granting access. Please note, other administrative areas have autonomy in granting access such as the Registrar, Human Resources, Finance and Advancement, amongst others.

At time of separation, the account will be handled as if it were an employee account.

**Special Circumstances**

For circumstances not defined within this policy, please consult the AVP for IT.