FERRIS STATE UNIVERSITY

BUSINESS POLICY

Computing Account and Access Management Policy

Effective Date:	11/01/2017
Policy Number:	2018: 01
Policy Owner:	Chief Technology Officer, Information Technology Services
Supersedes:	Campus Computing Access and ID Creation 2005:02

SCOPE

This policy applies to employees, student employees, students, affiliates, contractors, vendors, guests, emeriti, retirees, and others, who need an account or access to University systems and networks. This policy also covers system and departmental accounts for use in special situations.

POLICY STATEMENT

Accounts and related access to information resources require prudent oversight to ensure the security of University data and systems. Use of University information technology resources and data is controlled through the timely creation, management, and removal of accounts/access.

Account Lifecycle

Account Creation

Users are required to keep authentication information confidential and secure, ensuring that it is not shared with others.

1. The Enterprise Resource Planning (ERP) system is the authoritative source for generating IDs.
2. For systems that are not using the University's Account Management System, the person acting as the system administrator or individual responsible for the resource will issue a unique account for each individual and follow the University's password standards, where technically feasible.
3. Security is assigned based on minimum access required per job, role, or task and must be approved by the Data Owner or Privacy Owner.
4. Account creation date recorded by audit log or captured electronically in the IT Service Management application.
5. All guest or Third Party (Vendor) accounts (for those who are not official members of the University community) with access to University computing resources must contain an expiration date, where technically feasible. An appropriate member of the department managing the resource must authorize all guest accounts.
6. Users working with confidential or restricted data will be required to sign a Confidential Data Security Agreement.
7. Users requiring elevated (privileged) access require special account(s) based on job functions.
8. Only those authorized to create accounts may do so. University policies and procedures must be followed when creating accounts.
9. Application administrators who grant access must also audit those accounts at least annually.

Account Modifications

Ferris Computing Account ID changes will be made on an exception basis. For more information, see the Contacts section of this policy.

Account Termination/Removal

Email and system account(s) are removed, revoked, suspended, and/or deleted based on the individual's relationship with the University and their role as determined by Human Resources and General Counsel. When a role change is initiated by Human Resources or General Counsel, email and system accounts will be disabled immediately and removed after 60 days; unless the user account is placed on Legal Hold. Application System accounts will be removed immediately as part of the separation process. Some individuals may keep access to email and ancillary systems based on other agreements (Emeriti, Retirees, Adjunct Faculty, etc.) that determine role requirements with the University. Vendor accounts will be removed at the end of the contract through the work order system.

Access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract, or agreement, or adjusted upon role change.

- Separated Employee(s), Deceased Employee(s): Disable system/email account and maintain availability for 60 days. After 60 days, the account will be removed.
- Terminated Employee(s), Urgent Separation: Disable system/email account and place account in Legal Hold status. Account will be maintained until General Council authorizes removal. ITS will provide a list of Legal Hold accounts quarterly to General Council to review. The account will be removed when General Council determines the account is no longer needed.
- Suspended Student(s): Disable system/email account. Account is maintained and re-enabled when the student returns to "Active Student" status. Suspended accounts will be removed after 1 year. Students returning after this time will be issued a new account.
- Dismissed Student(s): Disable system/email account and maintain availability for 60 days. After 60 days, the account will be removed.

Access

Data Owners approve access to their respective data (e.g., the Registrar will determine who is granted access to registration data, and what access each user will have). A basic set of rights/access to IT resources will be granted based on the role of the individual. Additional access will be granted as authorized by the supervisor and Data Owner. When someone transfers positions, access is removed for the old role, granted new access based on the new role, and documented in IT Service management application. Application Programmers should not be given update access in production environments, where technically feasible.

Roles

A person's relationship(s) with the University determines the access based on the assigned role(s). If more than one role applies in the list below, the role with the lowest number takes precedence:

1. Employee
2. Emeriti
3. Retiree
4. Current Student
5. Affiliate/Volunteer
6. Former/Alumni Student

Examples:

- If the individual is an employee and a current student, the employee role takes precedence.
- If the individual is a current student and an affiliate of the University, the current student role takes precedence.

Departmental Accounts

In some situations, an account to support the functionality of a process, system, application, or device (such as computers) may be granted with proper documented authorization and justification.

Each of these departmental accounts must have a designated owner who is responsible for the management of access to that account. The owner is also responsible for the documentation, which should include a list of individuals who have access to the account.

Passwords for these accounts must change at least annually and/or when users with knowledge of the account change status.

Personal Use of Account(s)

University services may be used for incidental personal purposes if such use does not:

- Directly, or indirectly interfere with University business;
- Interfere with the Users employment or other obligations to the University; or
- Violate this policy, or any applicable policy or law.

Personal usage of your account(s) will be subject to access consistent with this policy or applicable law.

Violations/Sanctions

Suspected or known violations of this policy or applicable laws must be reported to Technology Assistance Center (TAC), and if applicable, an employee's supervisor. Suspension of access to Ferris IT resources may occur while investigating a suspected violation. Any person found to have violated this policy will be subject to appropriate disciplinary action as defined by current University policy, student code of conduct, and/or collective bargaining agreements. When appropriate, University authorities and/or law enforcement agencies may conduct an investigation into the incident.

DEFINITIONS

Employee

New Hire: An employee that has never worked at the University.

Re-Hire: Employee who has worked at the University before, but does not have a current assignment (this does not include previous student employment).

Examples:

- An employee re-hired after any break in employment.
- Adjunct faculty that hired on a semester-by-semester basis for each new semester assignment.

Extension

The extension of a part-time or full-time temporary employee's current assignment.

Transfer

The transfer of an employee with a current assignment to another primary assignment without a break in employment dates.

Examples:

- A part-time employee with a current assignment who attains a full-time position.
- Employee with an active primary assignment in one department and then moves to a primary assignment in a different department.

Student

- Current Student – Has the status of Active Status (AS) in Banner.
- Enrolled Student – A student who registered for a class.
- Active Enrolled Student – Both an Active Status and registered for a class.
- Alumni/Former Student – Has taken at least one class.

Affiliate (Volunteer)

An individual that requires access to a University system, but is not a current employee or student employee.

Emeriti

A retired employee that qualifies and meets Board of Trustees policy for Emeritus status.

Retiree

A retired employee that qualifies and meets Board of Trustees policy for Retiree status.

Guest

Members of the public that are visiting and do not have another role at the University who usually only require Wi-Fi use in the Library or other public spaces.

Data

Information collected, stored, transferred, or reported for any purpose, whether electronically or hard copy.

Data Owner and Privacy Owner

An individual or their designee with primary authority and accountability for specified information (e.g., a specific business function) or type of data. They have the ability to authorize or deny access to certain data. This individual is responsible for delegating responsibility to appropriate users.

Departmental Account

An account used by one or more users that is for University business.

Vendor

Vendor, consultant, contractor, or other third party, paid to do business with the University. They may also be considered an Affiliate if they require an ID to access University systems..

RESPONSIBILITIES

The following lists of responsibilities are not an exhaustive list.

- Protecting your University accounts from any unauthorized access.
- Do not share your ID or password with others.
- Store passwords in a secure location or memorize them.

PROCEDURES

https://ferris.edu/HTMLS/administration/adminandfinance/human/Employment/starting/index.htm#Access
https://ferris.edu/it/service-catalog/securityandaccounts-accountmgmt.htm

CONTACTS

If you have any questions, contact:

Technology Assistance Center, (231) 591-4822 or toll-free (877) 779-4822

ID Changes
Student ID Changes are approved by Admissions and Records.
Employee ID Changes are approved by Human Resources

RELATED INFORMATION/FORMS/INSTRUCTIONS

Proper Use of University Technology Resources

Use of University Email Policy

Information Security Guidelines (ISO A9.2. A9.3)

Data Classification Policy (ISO A9.1)

Confidential Data Security Agreement (ISO A9.1, A9.3)