Limestone College Account Creation and Removal Policy

Purpose

This policy serves as guidelines for Information Technology Services to create and remove accounts for systems and services needed to serve Limestone College as a student/employee.

Scope

A Limestone College account provides access to multiple systems and technologies. Generally, eligibility for technology resources begins and ends with an active relationship with the College. Human Resources is the primary source of information determining active employees. The Student Information System is the primary source of information determining active students. Limestone College employee liaison's and College service contracts are the primary source of information determining active vendors.

Policy

Student Accounts

Student email accounts are created once the student is registered for at least one course in the default term in Jenzabar (SIS). Residential (traditional) Day students gain partial online portal access after a deposit is secured so they may complete the housing application. Students gain full access to the portal when they are registered for a course in the default term in Jenzabar (SIS). Students gain access to Blackboard two days prior to their first course. If the student is added to the course during the drop/add period they will gain access after 5pm that day.

Student email accounts will be deleted 6 months after their graduation date if they do not enroll in additional classes within the 6 months after graduation. Traditional day and MBA students who have not taken classes in a year will be deleted in January and July based on the last day of the last class taken. Evening and online students who have not taken classes in two years will be deleted in January and July based on the last day of the last class taken. Students who received an email account but did not take classes (i.e. students enrolled and dropped the classes without completing or accepted traditional day students who do not enroll in the expected semester) will be deleted 6 months after email creation date. High school students (dual enrollment) who do not start as an undergraduate Limestone student after 1 year from their HS enrollment email account will be deleted after 1 year from last HS class date.

Employee Accounts

Employee accounts are requested from supervisors via the New Employee Data and New Employee Info forms located T:\Docs\HR and submitted to Joyce Phillips, Administrative Assistant for Academic Affairs. Once the data on the new employee is entered in Jenzabar (SIS), the request is sent to the Database Administration for creation. Account is to be setup within 3 business days after form is submitted to IT. Active Directory accounts are setup for employees and information is sent to the supervisor listed on the Data Request form. Staff automatically gains access to the online portal and faculty gains access once they are assigned as an instructor to a course in the current term. Faculty members' Blackboard accounts created are upon completion of Blackboard training.

Employees are instructed upon receipt of their account credentials to reset their password and configure their account on Password Manager to manage their passwords and security questions. Password Policy can be found in the Information Technology Policies document pages 19-20.

Upon departure from active employment with Limestone College, IT is notified by Human Resources or employee supervisor to disable account. Active Directory password is changed, and group permissions are stripped. If applicable, new account password is shared with supervisor to extract information needed.

Vendor Accounts

Third-party vendor accounts and access requests are to be made to the IT department through the Limestone College liaison for said vendor.

Third-party vendor account departure notifications should come from Limestone College liaison for said vendor. Active Directory password is changed, and group permissions are stripped. If applicable, new account password is shared with supervisor to extract information needed.

Additional Access

Access to Student Information System(s) Jenzabar and PowerFAIDS are granted based on job requirements if there is a legitimate need. Supervisors are required to request access for new employee on the New Employee Info form for said system as well as what specific access the employee requires.

Users are instructed upon receipt of their SIS account credentials to reset their password as soon as possible. Users are instructed to keep credentials private and secure due to the PII they have access to in the systems.

Passwords for Jenzabar expire after 180 days and complexity requirements are as follows:

- The password does not contain the account name of the user.
- The password is at least eight characters long.
- The password contains characters from three of the following four categories:
- Latin uppercase letters (A through Z)
- Latin lowercase letters (a through z)
- Base 10 digits (0 through 9)
- Non-alphanumeric characters such as: exclamation point (!), dollar sign ($), number sign (#), or percent (%).
- Passwords can be up to 128 characters long. You should use passwords that are as long and complex as possible.

Passwords for PowerFAIDS expire after 180 days and accounts that have not logged in within 90 days will be locked. Complexity requirements are as follows:

- Be at least 10 characters long.
- Contain at least one lowercase and one uppercase letter.
- Contain at least one special character (!@#$%^&*).
- Contain at least one number.