Account Creation Policy
TEC 3.0
Office of Information Technology

Institutional Type: Operational
Applies to: Faculty, staff, students, student workers, guests, vendors, senior citizens taking classes and general/departmental network/email accounts. This also applies to accounts created for system login use and access.

POLICY DATES

Issued: 9/1/1993
Revised Last: 5/23/2023
Edited by: Tina Stuchell
Reviewed: May 22, 2023

This policy guides the creation of network, email, and system accounts. All users of the appropriate accounts must use the accounts only for academic and work-related business and must follow all policies in their use of the accounts such as the Technology Acceptable Use Policy, Information Security Policy, Remote Access Policy, etc.

This policy is reviewed on an annual basis and any necessary changes are submitted to the Policy Review Committee. Major changes to this policy are approved through VP of Business Affairs.

Definitions

Term	Definition
Email Account	Email account and email address. All Mount Union email addresses take the following format: XXXXXXXX@mountunion.edu. where XXXXXXXX is the first six characters of last name, first initial and middle initial when available. When not available a similar format is selected. The exception to this format is for student accounts. Student accounts are comprised of first six characters of last name, first initial, middle initial and current entry year. Example xxxxxxxx2023@mountunion.edu
Learning Management System	D2L/Brightspace is the institution learning management system, used by faculty & staff when teaching courses. Students also have access to this system.
Network Account	Login account that gives access to network resources.
Privileged Account	Accounts with elevated capabilities beyond regular users. Examples include Administrative Network access, System access on administrative applications/software, high level system accounts where in which the account has access to sensitive information. Accounts that install software, create new network or system accounts or edit rights of users are also privileged accounts. Privileged functionality also includes establishing system accounts, performing system integrity checks, conducting patching operations, and other key management activities.
Raider Experience	Raider Experience (also known as Ellucian Experience) is the institutional mobile app and "portal" system where on campus directory, access to forms, policies, etc. resides.
Self Service	Web application into Institution Student Information System (SIS) Ellucian's Colleague system. Self-service is used for registering, class rosters, final grades, vacation requests, pay stubs, clocking in/out, class schedule, budget reports, etc.
Student Success System	Ellucian Advise is the institution student success system, replacing Starfish in the fall of 2023.
System Account	Login account that gives access to various campus academic, administrative and server systems.
Username	This is comprised of six characters of last name, first initial, middle initial. For students it will also comprise of current entry year. Chosen name within Colleague is what is pulled from to determine username. All Active Directory (AD) accounts must contain an ID number, so the account can tie back to ERP system/legal name for user.
VPN (Virtual Private Network)	VPN is a secured private network connection. It provides a secure encrypted connection, or tunnel, over the Internet between an individual computer/device and a private network.

Applies to: Faculty, staff, students, student workers, guests, vendors, senior citizens taking classes and general/departmental network/email accounts. This also applies to accounts created for system login use and access.

Policy Details

Please note the creation of accounts including network, email, Self-Service, Learning Management System, Administrative Systems, etc. requires several steps and can take 24-48 hours for all access to systems to be granted.

I. Network Accounts

A. Faculty/Staff Accounts

Accounts naming conventions are comprised of the first six characters of last name, first initial and middle initial when available. When not available a similar format is selected. Accounts are created when hired. Accounts are kept active as long as employed with the University of Mount Union. Faculty and staff accounts permission also include appropriate server file space comprised of departmental and personal file space.

Account user packet which contains account name and password is not distributed to the employee until first day of employment.
Network and email accounts will use the same name. (i.e. User John J. Doe, will have user name doejj and email address of doejj@mountunion.edu.) In cases of name changes, username and email address must remain the same.

Accounts are only active while an employee or a retiree. The Office of Information Technology is notified of terminations, resignations and retirees by Human Resources or running appropriate reports on a regular basis from ERP system.

Employee accounts can only be extended after terminations and resignations if approval is granted by area VP, area Assistant/Associate VP or Director of HR. If access is granted for another employee to manage the account for a duration, the typical time frame that should be granted is 30 days. If additional time is needed to manage the account, the area VP, area Assistant/Associate VP or Director of HR must grant approval of the additional time and give a date for the deadline, which should not exceed 3-6 months unless there are special circumstances. If there are special circumstances, then the area VP and Director of HR must both approve this request.

B. Student Accounts

1. Undergrad

Accounts naming conventions are comprised of the first six characters of last name, first initial, middle initial and entry year (example stuchetm2020 – Current entry year). When middle initial is not available a similar format is selected such as second initial of first name. Accounts are created when students are accepted and are kept active while enrolled at the University of Mount Union. Please note student accounts created between 2014 and 2020 used naming conventions of ending with anticipated grad year. Beginning in Fall of 2020 entry year is added, instead of anticipated grad year. Also accepted students receive accounts beginning Fall 2020, prior to Fall 2020 students who paid their deposits received accounts.

2. Graduate

a. PA, M.ED

Accounts naming conventions are comprised of the first six characters of last name, first initial, middle initial and entry year. (example stuchetm2018 – Current entry year). When middle initial is not available a similar format is selected such as second initial of first name. Accounts are created when students become accepted and are kept active while enrolled at the University of Mount Union. If students do not become paid/registered students, their accounts are disabled. Please note student accounts created between 2014 and 2020 had used naming conventions ending with anticipated grad year. Beginning in Fall of 2020 entry year is used, instead of anticipated grad year (+2 for PA and M.ED programs). Also accepted students receive accounts beginning Fall 2020, prior to Fall 2020 students who paid their deposits received accounts.

b. DPT

Accounts naming conventions are comprised of the first six characters of last name, first initial, middle initial and entry year (example stuchetm2019 – Current entry year). When middle initial is not available a similar format is selected such as second initial of first name. Accounts are created when students are accepted and are kept active while enrolled at the University of Mount Union. If students do not become paid/registered students, their accounts are disabled. Please note student accounts created between 2014 and 2020 had used naming conventions ending with anticipated grad year. Beginning in Fall of 2020 entry year was used, instead of anticipated grad year (+3 for DPT programs). Also accepted students received accounts beginning Fall 2020, prior to Fall 2020 students who paid their deposits received accounts.

NOTE: Please note the additional rules related to student accounts:

- Students who graduate can keep their email account for "life" in the "cloud". This rule began in 2014 and is only for those who graduated from that year forward.
- Non-returning students (for any reason) their accounts are disabled/deleted following their last semester of attendance. The exception to this rule is only possible if a VP or Associate/Assistant VP gives permission to extend the account. (Example maybe in case of illness, medical reasons or incomplete).
- Students who are enrolled in undergrad program, then graduate and immediately goes onto enroll in a master/doctorate work will retain their undergraduate account.

C. Departmental/Office Accounts

These accounts are only created by request of the head of the department/office. These accounts are requested in writing by submitting the appropriate paperwork with appropriate signatures. These are general accounts, example = IT, and are overseen by the head of the department/office.

D. Board of Trustee Accounts

Generic account(s) are maintained for the board of trustee members for appropriate business purpose. Some individual accounts are created for board members for committee work.

E. Vendor Accounts

Vendor account(s) are only created and maintained for the official use to conduct appropriate project work, business related function, and are maintained for a short period of time. These accounts must go through the appropriate approval process to be created. These accounts are reviewed on an annual basis for continued business justification in order to maintain access. Vendors must resubmit appropriate paperwork on an annual basis.

All vendor logins must go through VPN to access campus resources. Appropriate paperwork for VPN access must be completed. Vendor session monitoring is conducted by Bitlyft to assist the University in maintaining security. Vendor sessions will be alarmed and reported on a bi-weekly (each 14 days) basis.

F. Senior Citizen Accounts

Senior citizens (as defined by our registrar's office) who take courses at Mount Union for non-credit are provided an account to perform course work. These accounts are available only when enrolled in courses and use the same formatting rules as students.

G. Guest Accounts

Guest network accounts are only created by request in writing by the appropriate department/office head. Generally, are for short period of times and turned on/off only for specified periods of time. General Library guest accounts passwords are maintained by the library staff.

H. Interns

Intern network accounts are only created upon request of department/office head for a specific period of time by filling out the appropriate paperwork with appropriate signatures.

I. Parent Accounts

Parent network accounts are only created for the use within Self-Service for access to Shared Access functionality. These accounts are generated systematically.

Applies to: Faculty, staff, students, student workers, guests, vendors, senior citizens taking classes and general/departmental network/email accounts. This also applies to accounts created for system login use and access.

j. Admin/High level Accounts (these are also considered privilege accounts)
Within the Office of Information Technology there are various employees who have responsibilities that need administrative network privileges. Those who do, have separate administrative accounts created for such access. The members include Director of IT for Security, network employees, Director of IT for Operations and CIO. These accounts are never reused even after an employee leaves the institution.

Those employees who hold the following positions hold high-level network accounts that will never be reused (this assists with our GLBA and security compliancy efforts):

- Board of Trustee
- President
- Vice President
- Associate and Assistant Vice President
- Provost
- Dean
- Controller
- Administrative Analysts and Manager of Administrative Systems
- Chief Information Officer
- Director of IT for Security
- Director of IT for Operations
- Director of Financial Aid

II. Email Accounts (@mountunion.edu)

A. Faculty/Staff Accounts

Accounts naming conventions are comprised of the first six characters of last name, first initial and middle initial when available. When not available a similar format is selected. Accounts are created when hired. Accounts are kept active as long as employed with the University of Mount Union. The format for email is as follows: xxxxxxxx@mountunion.edu.

Email account and password is distributed in the employee user packet and is distributed on the first day of employment.

NOTE: Please note the additional roles pertaining to employee accounts

- If an alumnus (with a mount union account – so graduate after 2014) & becomes an employee a new mount union account is created for their employment.
- There are times an employee will take courses, in those cases no new student account will be created, they will make use of current employee account.
- In rare occasions when an employee takes classes and then terminates employment but stays on as a student the student/past employee will be allowed to maintain their employee account and use for student work provided they left the institution as an employee in good standing, the time frame for the additional account use is a short period and the employee account is not needed for supervisor. A short period is defined as 1-2 semesters remaining. In all other cases, the employee account will be terminated, and a new student account will be created for student course work.

B. Student Accounts

1. Undergrad

Accounts naming conventions are comprised of the first six characters of last name, first initial, middle initial and entry year (example stuchetm2020 – Current entry year = 2020 resulting in stuchetm2020@mountunion.edu). When middle initial is not available a similar format is selected such as second initial of first name. Accounts are created when students are accepted and are kept

active while enrolled at the University of Mount Union. Please note student email accounts created between 2014 and 2020 used naming conventions of ending with anticipated grad year. Beginning in Fall of 2020 entry year is added, instead of anticipated grad year. Also accepted students receive accounts beginning Fall 2020, prior to Fall 2020 students who paid their deposits received accounts.

2. Graduate

a. PA, M. ED

Accounts naming conventions are comprised of the first six characters of last name, first initial, middle initial and entry year (example stuchetm2018 – Current entry year 2018 resulting in stuchetm2018@mountunion.edu). When middle initial is not available a similar format is selected such as second initial of first name. Accounts are created when students are accepted and are kept active while enrolled at the University of Mount Union. If students do not become paid/registered students, their accounts are disabled. Please note student accounts created between 2014 and 2020 had used naming conventions ending with anticipated grad year. Beginning in Fall of 2020 entry year is used, instead of anticipated grad year (+2 for PA and M.ED programs). Also accepted students began receiving accounts beginning Fall 2020, prior to Fall 2020 students who paid their deposits received accounts.

b. DPT

Accounts naming conventions are comprised of the first six characters of last name, first initial, middle initial and an entry year (example stuchetm2019 – Current entry year 2019 resulting in stuchetm2019@mountunion.edu). When middle initial is not available a similar format is selected such as second initial of first name. Accounts are created when students pay their deposits and are kept active while enrolled at the University of Mount Union. If students do not become paid/registered students, their accounts are disabled. Please note student accounts created between 2014 and 2020 had used naming conventions ending with anticipated grad year. Beginning in Fall of 2020 entry year was used, instead of anticipated grad year (+3 for DPT programs). Also accepted students receiving accounts beginning Fall 2020, prior to Fall 2020 students who paid their deposits received accounts.

NOTE: Please note the additional rules related to student accounts

- Students who graduate can keep their email account for “life” in the “cloud”. This rule began in 2014 and is only for those who graduated from that year forward. A graduate only gets to maintain their account for “life” provided they login at minimum once within a twelve-month period. Accounts that have not been accessed within a 12-month period will be removed and will not be reestablished
- Non-returning students - their accounts are disabled/deleted following their last semester of attendance. The exception to this rule is granted only if a VP gives permission to extend the account. (Example maybe in case of illness or medical reasons).
- If an alumnus (with a mount union account – so graduate after 2014) & becomes a graduate student, no new account is created, uses their alumni account.
- If an alumnus (with a mount union account – so graduate after 2014) & becomes an employee (given a new account for job/position) and then becomes a grad student, they should use their employee account for graduate work (this is so they do not have two accounts showing up in global address book) Note – Alumni email address do not show up in global address book.
- There are times an employee will take courses, in those cases no new student account will be created, they will make use of current employee account.
  In rare occasions when an employee takes classes and then terminates employment but stays on as a student the student/past employee will be allowed to maintain their employee account and use for student work provided they left the institution as an employee in good standing, the time frame for the additional account use is a short period and the employee account is not needed for supervisor. A short period is defined as 1-2 semesters remaining. In all other cases, the

employee account will be terminated, and a new student account will be created for student course work.

C. Departmental Accounts
These accounts are only created by request of the head of the department/office. These accounts are requested in writing by submitting the appropriate paperwork with appropriate signatures.

D. Board of Trustee Accounts
Email accounts are not created for Board of Trustees. (Network account only)

E. Vendor Accounts
Mount Union email accounts to be used by vendors are not created.

F. Senior Citizen Accounts
Senior citizens (as defined by our registrar's office) who take courses at Mount Union for non-credit are provided an account in order to perform course work. These accounts are available only when enrolled in courses and use the same formatting rules as students.

G. Guest Accounts
Guest email accounts are not generally created.

NOTE: To assist in some cases pertaining to account (this is stated above in paragraph form).

- If undergrad
  - Get account.
  - If Graduates – Keep Acct for "life" (Since 2014)
- If Mount Union Alumnus with Acct for "life" & becomes employee
  - New Account is created for employment. Their Alumnus account is still kept for their personal use.
- If Mount Union Alumnus with Acct for "life" & becomes a UMU Graduate Student
  - No new account is created, use Alumnus Acct
- If Alumnus with Acct for "life" & becomes a UMU Employee & then attends graduate school
  - New Account is created for employment and uses this account for graduate school
- If Employee and then becomes student, employee account is used for both work and school, no new student account is created.
- If Employee, then becomes student, then terminates employment but continues on as a student (these are rare occasions), will be permitted to keep use of employee account until graduation if in good standings and within 1-2 semesters of completion and past employee account is not needed by supervisor. In all other occasions a new student account will be created.

III. System Accounts

System accounts are used for access to institutional academic and administrative system. These accounts are reviewed on an annual basis by the Office of Information Technology with verification of appropriate access rights, confirmed by the system owner, such as Registrar, HR, Business Office, Financial Aid, etc. These reviews/audits are recorded within the Office of Information Technology within the Administrative Systems area of IT.

In many cases single sign on (SSO) is used. Two factor authentication (2FA) and multi factor authentication (MFA) is turned on for every system that has the capability to do so. Currently the Office of IT uses MS AzureAD and uses conditional access policy to enforce multifactor authentication.

A. Faculty/Staff Accounts
Accounts are created to give login access to various systems. These include systems that are used for both administrative and academic uses. These accounts are only created with the completion of the appropriate forms along with the appropriate signatures.
The accounts are only active as long as the faculty or staff are employed at the university.

B. Faculty/Staff LMS, Self-Service, MS Office 365, Raider Experience, Accounts

All faculty are given access to D2L/Brightspace for course preparation and delivery. Access is given to faculty part of the on boarding/new account process. Staff who teach a course are given access to D2L/Brightspace. These individuals only maintain access to this system as long as they are employed at the institution. Early access to the LMS can only be granted if permission is requested by Dept. Chair, approved by Dean of the College & Registrar. The earliest that can be granted is July 15th for fall, December 1st for Spring, April 15th for Summer. The Early network/email exception form located in Ellucian Experience on the forms tab under Supervisor must be filled out and approved before early access can be granted. Due to the nature of

Self Service access is granted part of the onboarding process for new employees. Access is terminated the following April 15th-18th, for tax purposes for those who are no longer an employee.

MS Office 365 – access is granted part of the onboarding process and is terminated when an employee is no longer employed. Retirees, do not maintain access to MS Office 365, only email.

Raider Experience access is granted part of the onboarding process is and is terminated when no longer an employee.

All of these systems are SSO. Meaning that their network credentials work to access the system.

C. Student Account access for LMS, Self Service, MS 036, Raider Experience

Each student is given a D2L/Brightspace account for Learning Management Access (LMS) access for class/course work. These accounts are automatically created part of the onboarding process and are active as long as the student is enrolled in classes. IT staff disable the accounts upon notification of a withdraw or graduation.

Each student is given access to Colleague Self Service. This access is automatically assigned part of the onboarding process for new students/account process. Access is kept for students until April 18th - 20th of the following year following withdraw or graduation (unless the student is placed on hold). This allows the student access to tax forms.

Each student is also given access to Raider Experience and MS 0365. Access is given part of the onboarding process and is terminated when no longer a student.

Each of these systems support Single Sign On (SSO), which allows access by the use of network account credentials.

D. Student Worker Accounts

Accounts are created for student workers (students who are employed for campus employment within an office or department). These accounts are only created upon written request with the appropriate signature and are overseen by the head of the department or office.

E. Vendor Accounts

When appropriate vendor accounts are created for a limited time to be used for supporting, maintenance and troubleshooting of a specific system. These accounts are overseen by The Office of Information Technology. Appropriate paperwork must be completed in order to grant vendor system access and are made available for a short period of time and are reviewed on an annual basis. If the system is on-prem, then access must go through VPN from off campus in order to access the system.

F. Administrator Accounts (these are also privileged accounts)

These accounts are used for support of the appropriate systems. Overseen by a select few within the Office of Information Technology. Are kept at the highest security. Default system passwords are always changed and maintained within the Office of Information Technology for those systems overseen by IT. These accounts are not ever reused after the employee retirees or leaves the institution.

G. Privilege Accounts

Applies to: Faculty, staff, students, student workers, guests, vendors, senior citizens taking classes and general/departmental network/email accounts. This also applies to accounts created for system login use and access.

These accounts are used in support of the appropriate systems and are high level accounts. These accounts have high level access to data and sensitive information. These accounts are logged. These accounts are audited/reviewed on a monthly basis. They are reviewed on a regular basis to detect any account misuse. Misuse of privileged accounts either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised system accounts, is serious and can have significant adverse impact on the institution. By logging the use and reviewing these accounts on a regular basis, this helps to mitigate the risk from insider threats and the advanced or a persistent threat.

IV. VPN Access

University of Mount Union recognizes the need of its students, faculty, staff and sometimes vendors to access university data when they are not physically on campus. The use of VPN allows members of the UMU community to securely access UMU network resources from off campus as if they were on campus. All members of the UMU community who need access to VPN must comply with the University Remote Access Policy.

Logging and monitoring of remote access activity is a necessity in order to stay compliant with the NIST requirements and mitigate any risk to the institution. Logging and monitoring of remote access is done on a regular basis (monthly). This is completed for faculty, staff, students and any third-party vendors who have VPN access.

PROCEDURE

Procedures are in place around the creation of accounts within The Office of Information Technology. They are as follows:

V. New Admin System Account Procedure
   A. For employee's system access
VI. New College Credit Plus Student Account Procedure
   A. For College Credit Plus Students (Early Admits & Dual Credit)
VII. New Faculty, Staff & Intern Account Procedure
   A. For employee's network/email access
VIII. New General Account Procedures
   A. For general accounts such as departmental or organizational network/email access
IX. New Guest Account Procedures
   A. For guest accounts (library guests, camp guests, etc.)
X. New Graduate Student Account Procedures
   A. For graduate students
XI. New Individual Bright Space Account Procedures
   A. For faculty/staff/student access for LMS
XII. New Re-Admit & Senior Citizen Student Account Procedures
   A. For students readmitted & students who are senior citizens
XIII. New Student Accounts Procedures
   A. For undergrad student network and email accounts.

Responsibilities

Position or Office	Responsibilities
Office of Information Technology	Creation of accounts for faculty, staff, students, departments, etc.

Account Creation Policy

TEC 3.0

Office of Information Technology

Applies to: Faculty, staff, students, student workers, guests, vendors, senior citizens taking classes and general/departmental network/email accounts. This also applies to accounts created for system login use and access.

Position or Office	Responsibilities
(Administrative Services & Technical Services)	

Contacts

Subject	Office	Telephone	E-mail/URL
	Office of Information Technology	330.823.2854	IT@mountunion.edu

History

Rules associated with creation of accounts have been in place since 1993. They have been maintained on IT internal web pages through the years and placed into this written policy in 2016.

FUTURE CHANGES:
All changes must be listed sequentially, including edits and reviews. Note when the policy name or number changes.

Issued: 9/1/1993
Revised: 5/23/2023
Edited by: Tina Stuchell
Reviewed: 5/23/2023