User Account Overview

Information on user account provisioning, usage, and lifecycle.

- Faculty/Staff user accounts
- Student user accounts

Faculty/Staff user accounts

Your faculty/staff CU account is your single sign-on account for virtually all university related systems, including campus computers, Microsoft 365 resources including your email, Banner OneSIS, Brightspace, PASSHE Portal/Employee Self-Service, wireless connections, and remote access VPN service, as well as any other resources protected by university Single Sign-On.

Faculty/Staff account lifecycle

Employees will have a CU account automatically created once HR has the completed paperwork and completes the hiring action in SAP. The assigned username along with the initial password that can be used to logon to your computer and to access other university resources will be communicated directly to your supervisor or department secretary to be communicated to you.

Please understand that Faculty/Staff will not get to keep their account once they separate from employment with the university, therefore it is recommended that you do not use your work email account or storage for personal use.

Employees that have officially retired will get to keep their account for an additional 4 months after retirement date.

Separated employees that are granted emeritus status are able to request that they keep their email account indefinitely. Emeriti accounts only include email and will only remain in the system if they are accessed at least once every 90 days.

Password requirements and information

Certain password requirements must be followed when creating a new password. Please see the password information page for detailed requirements and information on changing or resetting your password.

Two-Factor Authentication (2FA)

Duo Two-Factor Authentication is required for all remote access. Faculty/Staff will be prompted to enroll when they sign in to a web resource. If you are not yet enrolled, it is recommended that you go to https://duo.commonwealthu.edu/ from your smartphone because this helps ensure you choose the correct app from the app store and it streamlines activating your account on the device.

Keep the office/phone up to date on your account

Employees should be sure to keep their campus office and phone number information up to date with HR and other systems including the Outlook address book and web directory. To set or update

the information, log on to the PASSHE Portal/ESS, click on the "Employee Self-Service" tab, click on the "Personal Information" tab, click on "Address and Contact Information", then under "Campus Address", click on "Change Campus Address". Update your Office (Building & Room Number) and Work Phone (enter full number including area code), and click "Save Changes".

Keep your account secure

Please keep your password to yourself and do not provide it on an external website in response to a phishing email no matter how convincing an email request for your password looks. Do not ever enter it onto a Google Form or Microsoft Form. You should not click on questionable links or links that you know are phishing. Also do not provide Duo 2FA passcodes via text message or email or on external websites and also do not approve Duo Pushes you did not initiate. Please familiarize yourself with the official university policies, PRP 2510 - Information Security Policy and PRP 2550 - Acceptable Use of Technology Policy.

Student user accounts

Your student CU account is your single sign-on account for virtually all university related systems, including public computers across CU campuses in computer labs, Microsoft 365 resources including your student email, Banner OneSIS, Brightspace, wireless connections, Housing related systems, Print related services, Student Worker eTime, and any other resources protected by Single Sign-On.

Student account lifecycle

Undergraduate degree students will have a CU account automatically created after they pay their tuition deposit. They are given their username and initial password in the application portal.

Graduate degree students and non-degree undergraduate students (no tuition deposit required for these types of students) will have a CU account automatically created when they have at least one course scheduled. If you were a recent CU undergraduate student and your account has not yet become inactive, your active CU account and password remain the same. If your account did become inactive or you forget what your password was, you will need to reset your password to gain access to your account. If you are a brand new CU grad student, you will receive notice of your username and password from the graduate office. You may also reset your password to gain access to your account.

Your CU account will become inactive approximately 8-9 months after you last attend CU, typically shortly after two succeeding semesters conclude. At that time you will receive an email notification that your CU account will be deleted in 1 month, and during that time you will need to save any data from your M365 Email, OneDrive, and any campus network drives that you want to keep, since it will be deleted with your account, unless you re-enroll prior to deletion, which a separate email notification would confirm.

Password requirements and information

Certain password requirements must be followed when creating a new password. Please see the password information page for detailed requirements and information on changing or resetting your password.

Two-Factor Authentication (2FA)

Duo Two-Factor Authentication is required for all remote access. Students will be prompted to enroll when they sign in to a web resource. If you are not yet enrolled, it is recommended that you go to https://duo.commonwealthu.edu/ from your smartphone because this helps ensure you choose the correct app from the app store and it streamlines activating your account on the device.

Keep your account secure

Please keep your password to yourself and do not provide it on an external website in response to a phishing email no matter how convincing an email request for your password looks. Do not ever enter it onto a Google Form or Microsoft Form. You should not click on questionable links or links that you know are phishing. Also do not provide Duo 2FA passcodes via text message or email or on external websites and also do not approve Duo Pushes you did not initiate. Please familiarize yourself with the official university policies, PRP 2510 - Information Security Policy and PRP 2550 - Acceptable Use of Technology Policy.