User Account Acceptable Use Policy Policy
Number 40007.1

Type of Policy:	Administrative
Last Revised:	May 4, 2021
Review Date:	May 4, 2024
Contact Name:	Dustin Gardner
Contact Title:	Information Security Officer
Contact Email:	gardnedj@cobleskill.edu

Reason for Policy: This policy pertains to how SUNY Cobleskill creates, assigns, manages, and secures user accounts. A "user account" refers to the username and password used to access SUNY Cobleskill resources including a SUNY Cobleskill network computer, using campus Wireless Networks, and accessing SUNY Cobleskill administered Email and Cloud services.

Policy Statement: Users will act with honesty, integrity and respect for the rights, privileges, and privacy of the College community. Users are responsible for the proper stewardship and protection of their college provided accounts to access College resources.

User Account Creation:

Faculty and Staff: Upon official appointment to the College and notification from the designated Human Resources Office, a Cobleskill.edu account is created for the campus employee. The account naming convention consists of the first six letters of last name, first initial, and middle name initial based on employee official name as defined by the Human Resources Office. If a faculty/staff member has a legal name change and it is processed and filed via the Human Resources Office, the employee can then request Human Resources to notify the ITS Office of official name change, and request that the network/email account be modified accordingly.

Volunteers and Affiliates: Upon official appointment to the College and notification from the designated Human Resources Office, a Cobleskill.edu account is created for the campus employee. Account naming convention consists of the first six letters of last name, first initial, and middle name initial based on employee official name as defined by the designated Human Resources Office. If a Volunteer/Affiliate member has a legal name change and it is processed and filed via the designated Human Resources Office, the employee can then request their Human Resources Office to notify the ITS Office of official name change and request that the network/email account be modified accordingly.

Students: Upon acceptance to the College, a student network/email account is automatically generated based on Banner enrollment status. Naming convention for student network/email account is the first six letters of the last name, first name initial, and last 3 digits of the 800 ID number, which is derived from the official College record. If a student has a legal name change and it is processed and filed with the Registrar's Office, the student

can then submit a name change request for their network/email account with the ITS Office to the official name change. The student will need to provide ITS with a picture ID with their name change.

User Account Deletion:

Faculty/Staff/ Affiliates/Volunteers: Based on official notification from the Human Resources Office, network/email accounts will be de-activated and/or deleted when faculty and staff terminate employment with SUNY Cobleskill. Based on official notification from the Human Resources Office of retirement status, retirees may submit an appropriate request form with the ITS Office to keep their Cobleskill.edu email account.

Students: Network/email accounts assigned to students are issued with an expiration date based on enrollment status; accounts are automatically disabled if student is not enrolled for the following academic semester.

Expectations of Appropriate Use of User Accounts:

Users are expected to act with honesty, integrity and respect for the rights, privileges, and privacy of the College community. Users are responsible for the proper stewardship and protection of their college provided accounts to access College resources. For the protection of both the user and the College, users are not to share their college provided account username or password with anyone. Exceptions to this will come at the request of any official College executive (VP, President), College HR, College UPD, or local, state, national legal agency. Users are permitted to share their password with SUNY Cobleskill ITS in order for ITS to provide service or to solve technical issues with the user's account.

Users are expected to abide by all applicable federal and state laws and rules, including SUNY Cobleskill policies, SUNY regulated policies, as well as all applicable State and Federal regulations. Please find the applicable Codes of Conduct at the bottom of this document.

Password Policies and Requirements:

SUNY Cobleskill users are responsible for configuring the password used to access their SUNY Cobleskill network and email resources.

When configuring these passwords, users are expected to create complex and secure passwords that:

- Do not match the passwords used with any other account, including any other of their SUNY Cobleskill administered accounts.
- Do not contain any part of their SUNY Cobleskill username, or other openly available directory information that would make the password easy to guess.
- Are not similar to their previously configured password.

SUNY Cobleskill users are expected to maintain the security of their user account password by never:

- Storing a hand-written password on or inside their desk or in their work area.
- Displaying their account password or any other authentication secret (BitLocker Encryption key) on their laptop or desktop computer.
- Storing passwords in plain text on any computer.
- Sending passwords via email.
- Sharing their account password with any unauthorized user, inside or outside of SUNY Cobleskill.

Multi-Factor Authentication:

Multi-factor authentication (MFA) is a process that requires that the person attempting to access a computer resource provide a one-time code, or positive approval of the login using an out-of-band verification device such as a cellular telephone, landline telephone, or mobile telephone application. MFA is used by SUNY Cobleskill as a supplement to strong passwords to authenticate users and authorize their access to resources such as Email, Office 365 services such as OneDrive and SharePoint, and the campus Virtual Private Network (VPN) connection more effectively. MFA protects against unauthorized access to SUNY Cobleskill accounts, and is a necessity for appropriate information security and regulatory compliance.

MFA is applied to all student, faculty, staff, affiliates, volunteer, retiree, and alumni accounts. It is the responsibility of the SUNY Cobleskill account holder to make appropriate provisions to receive MFA confirmation codes via SMS text message, audio call, or by installing the software required for verification. If provisions are not made to comply with SUNY Cobleskill MFA policy, the user will not be able to access protected resources until these provisions are made.

Compromised Accounts:

An account becomes compromised when an unauthorized user acquires the credentials to log into an account, with or without the knowledge of the authorized owner of the account. To preserve the integrity and security of the SUNY Cobleskill network and ancillary resources, an account that is believed to be compromised will be disabled, altered, or blocked by ITS without warning.

When the compromised account has been fully investigated, the unauthorized activity has been documented, and any applicable security controls have been implemented, the authorized user of the account will be contacted and informed of the compromise of their account.

Account Investigation

A SUNY Cobleskill User Account is subject to investigation if prompted with evidence of a policy or legal violation. The Chief of University Police and the Director of Human Resources will need to approve of the investigation concerning any College employee before any data will be collected by ITS. All investigations will follow appropriate, reasonable protocols and legal/regulatory parameters. The investigations will be supported by ITS, by having ITS provide raw data to the Chief of University Police and the Director of Human Resources to evaluate and take appropriate action, if warranted. All employees, regardless of employment status, must follow these guidelines.

SUNY Cobleskill Computer Resources Policy: https://www.cobleskill.edu/about/offices-services/informationtechnology/resources-policy.aspx
SUNY Cobleskill Conduct Codes: https://www.cobleskill.edu/campus-life/student-conduct/conduct-codes.aspx

Policy History:

Revision Date	Author/Owner	Description of the action on the revision date
5-4-21	Dustin Gardner	Policy Update