(POLICY)

Policy:	Secure Authentication and Responsible Use (Draft)	**Policy No.:**	IT9005
Authority:	SUNY Broome Community College Board of Trustees		
Delegated Authority:	President		
Policy Owner:	VPAA	**Responsible Party:**	*Chief Information Officer*
Approved:	June 20, 2024		
Revised:	(DATE)		

Purpose

The purpose of this policy is to support protection of the confidentiality, integrity and availability of the College's Information and Information Systems while setting guidelines for the responsible and acceptable use thereof. This policy has also been adopted to comply with laws governing the College's Information and/or Information Systems.

Statement of the Policy

Compliance with Applicable Laws and Contractual Obligations

College information and information systems are subject to numerous laws and regulations relating to security. The College also is or may become a party to contracts that require the College to maintain a certain level of information and information system security. The procedures and guidelines in this policy and the overall Information Security Program shall comply with all applicable legal and contractual requirements governing College information and information system security.

Responsibilities and Oversight

The College's Chief Information Officer (CIO) shall be tasked with overseeing the administration of this policy and the overall Information Security Program. The College's ITS Department shall oversee the training of all users, as set forth in this policy and the overall Information Security Program. Subject to approval of the Office of the President, the CIO may delegate specific functions under this policy and the overall Information Security Program but must retain oversight responsibility for the delivery of all goals and objectives of the Assistant Director for Information Technology Security.

Authentication Ownership

The College retains exclusive ownership of all usernames, passwords, tokens, or other means of authentication to the information, systems, and services it manages. These means of authentication are to be confidentially maintained, not to be written down or stored as text in a file, never to be shared with another user or otherwise disclosed. These means of authentication are provided for the exclusive use of each user and may be suspended or revoked at any time at the sole discretion of the College.

Information Ownership

The College retains exclusive ownership of all assigned Google accounts, their content, and their accessibility. With any exception defined by an Intellectual Property policy, the College retains exclusive ownership of all content of individual (personal) folders/drives, local folders/drives, department folders/drives, and any other data stored on College devices, or College provided services such as Google apps. Additionally, the College retains exclusive ownership of all content and data transmitted utilizing the College network.

Password Complexity and Duration

All SUNY Broome user accounts must have a password length of at least 14 characters and multi-factor authentication will be enforced on all Google accounts. Complexity requirements will ensure that passwords are unique and difficult to replicate.

Subject to the College's Data Retention policy

Unless otherwise stated, all information (data) described above and the data associated with the account types below will be subject to the Retention and Disposition of College Records Policy.

User Account Types

New Student Accounts (including FAFSA applicants): unique login and Google account will be created upon acceptance, with additional functionality added after registration.

Returning Student Accounts: will be restored (if still being retained) once the returnee registers.

Non-Credit Students: will be provided with login credentials, no Google account, and will be deactivated after one year of inactivity.

Graduating Student Accounts: will be notified upon graduation that they will have access for another 90 days. Reminder emails will be sent with 7 and 3 days remaining.

Unused Student Accounts: will be deleted when no data is associated with the account.

Inactive Student Accounts (students who do not return for a subsequent Fall or Spring term): will be notified that they will have access for another 90 days. Reminder emails will be sent with 7 and 3 days remaining.

Faculty Emeriti: will be granted lifetime access to their College email account at the College's continuing sole discretion.

Faculty/Staff Retirees: will be notified upon retirement that they will have access for another 90 days. Reminder emails will be sent with 7 and 3 days remaining.

Departing non-Retiree Faculty/Staff: accounts will be deactivated upon departure.

Vendors and Guests: may be provided a network logon, will not be given an email account, and will be deactivated following a preset duration. Technical Sponsors and Vendors must submit a Third-Party Access Agreement to be supplied.

Rights and Responsibilities

- Users who identify any security issue, suspicious activity, potential security event or incident involving information or information systems must notify the College's Information Technology Security staff immediately (ITSecurity@sunybroome.edu). Under no circumstances should the user demonstrate the security issue to another user or encourage any other user to exploit or replicate the security issue.
- As a user of SUNY Broome's information technology resources, it is the user's responsibility to notify the administrator (ITSecurity@sunybroome.edu) if any violations are observed.
- Users are responsible for protecting and backing up their own data.
- Any person issued a username and password in order to access SUNY Broome's information technology resources is responsible for all activity that takes place with that account. It is prohibited to let another person use one's username and password. Passwords are NOT to be shared.
- All users of SUNY Broome information technology resources are obligated to manage and use institutional data in a manner that is compliant with all federal, state, and local laws and regulations in addition to conforming to College policy.
- All users of SUNY Broome information technology resources must respect the work product and copyrights of others.

Acceptable Uses

The following are standards by which all students, faculty, staff, affiliates, and authorized guests may use their assigned computer accounts, email services, and the shared network.

- The Office of Information Technology Services grants access in the form of computer accounts to registered students, faculty, staff and others as appropriate for purposes such as research, education or administration.
- The purpose of a computer account is to support educational initiatives and SUNY Broome campus services by providing access to unique resources and the opportunity for collaborative work. The use of an account must be in support of education and/or academic research. Transmission of any material in violation of any U.S. or state regulation is prohibited.
- Authorized users may connect personally owned devices to SUNY Broome's wireless network provided that they have an active anti-virus software program and the latest operating system patches running on the device.

Prohibited Uses

The following activities are specifically prohibited. Access to SUNY Broome's information technology resources may be revoked if an account is used in an unacceptable way. Unacceptable uses include, but are not limited to:

- Attaching any personal computer via any cable to the SUNY Broome network.
- Attaching any unauthorized network devices or extenders to the wired or wireless campus network.

- Disconnecting a network cable from any computer.
- Playing video games, unauthorized eSports, or other bandwidth-consuming activities (except for official clubs sponsored by the College) on or through the use of any of SUNY Broome's information technology resources.
- Viewing or accessing offensive material. Any material may be considered offensive in nature if someone experiencing or witnessing it, whether intentional or not, is offended by it.
- Viewing, watching, or listening to any explicit/obscene, threatening, copyrighted, or illegal material.
- Using College resources for product advertisement, political lobbying, and activities deemed illegal by law.
- Giving one's password to or offering one's SUNY Broome Computer Account to anyone. A user is responsible for any activities associated with their account. Administrators, employees or other students should never ask for or be given one's password. Under no circumstances should a user give their account access information to anyone or log in as anyone else.
- Installing any software on any SUNY Broome Computer. This includes remote control software such as: GOTOMYPC, TeamViewer, etc.
- Attempting to break in or in any way use a SUNY Broome account that is not assigned to a user.
- Creating, sharing, or distributing computer viruses.
- Setting up a server on the network or using the network for any unapproved purpose.
- Saving confidential data or data with personally identifiable information (PII) on any portable device or laptop that is not encrypted or on an unauthorized cloud service such as Dropbox, iDrive, etc.
- Attempting to disguise one's identity, the identity of their account or the machine that one is using. Users may not attempt to impersonate another person or organization.
- Attempting to intercept, monitor, forge, alter or destroy other users' communications. Users may not infringe upon the privacy of others' computers or data. Users may not read, copy, change, or delete another user's data or communications without the prior express permission of the owner.
- Attempting to bypass computer or network security mechanisms. Possession of tools that bypass security or probe security, or of files that may be used as input or output for such tools, shall be considered as the equivalent to such an attempt. The unauthorized scanning of the SUNY Broome Network is also prohibited.

Review

Although the College does not generally monitor or restrict the content of material transported across networks, it reserves the right to access and review all aspects of its computing systems and networks, including individual login sessions and account files, to investigate performance or system problems, investigate information security incidents, or upon reasonable cause to determine if a user is violating this policy or state or federal laws.

Enforcement
Violations of this policy or the Information Security Program may result in suspension or loss of a user’s privileges to access or use Information or Information Systems based on the guidelines set forth in the Information Security Program and/or pursuant to other applicable College policies and procedures. Additional penalties also may apply pursuant to other College policies, contracts, and/or applicable civil and criminal laws.

Access to and/or use of SUNY Broome’s information technology resources is a privilege, not a right, and as such may be revoked should circumstances warrant such an action.

Related Policies (by number)

To Whom it Applies (title or department)
This policy applies to all students, faculty, affiliates, emeriti, and staff of the College (part-time and full-time), as well as all independent contractors, interns, consultants, and other third parties, inclusive of anyone who has access to network or email services. The policy applies regardless of the user's physical location (e.g., College offices, hotels, airports, user homes, etc.).

General Guidelines

Definitions

Appendix

Ex. Written communication, location (where published)

Action *(Created, Reviewed, Retired)*	**Date**	**Initials**	**Position Title**
ex. Created	01/01/2020	SC	*ex. Director Sponsored Programs*