**1.0 Purpose and Benefits of the Policy** –OK, 08/11

This document establishes policy for the acceptable use of information technology resources (“IT Resources,” as defined in Section 8.0 herein) at SUNY Polytechnic Institute (“SUNY Poly”) within a culture of openness, honesty, trust, integrity, academic freedom, and respect.  SUNY Poly is committed to putting safeguards in place to assist in protecting its students, faculty, staff, and guests and partners from damaging, illegal, unethical, and/or prohibited actions by anyone using SUNY Poly IT Resources.

Except for terms defined in this policy (see Section 8.0), all terms shall have the meanings found in <http://www.its.ny.gov/glossary>.

**2.0 Scope of the Policy** – OK, 08/11

Securing and protecting SUNY Poly IT Resources is a team effort that requires the participation and support of all individuals that have access to or manage SUNY Poly IT Resources (hereinafter “Authorized Users,” as defined in Section 8.0). Therefore, every Authorized User is required to know and adhere to the policies and practices found in this Acceptable Use Policy and the SUNY Poly Information Security Policy.

**3.0 Policy Statement** – 08/11, 3rd paragraph needs revisions

Authorized Users shall use SUNY Poly IT Resources for purposes related to SUNY Poly's mission (learning, instruction, research, support of student life, duties as employees, official business of SUNY Poly, and other SUNY Poly sanctioned activities) unless otherwise specified in this policy or other SUNY Poly policies.  Colleges, departments, and other administrative units may develop complementary acceptable use policies and procedures so long as those policies are consistent with this policy and have been approved by the Chief Information Officer and Legal Department.

SUNY Poly takes measures to appropriately protect the privacy of individuals and the confidentiality of the information stored on its IT Resources.  While some personal use of SUNY Poly’s IT Resources and the use of some personal devices is permitted, information transmitted via or stored on SUNY Poly IT Resources is not afforded privacy from SUNY Poly.

SUNY Poly may preserve, monitor, analyze or terminate an Authorized User’s access and use to SUNY Poly IT resources. SUNY Poly may investigate (preserve, access, monitor, take custody of, analyze, or terminate access to) any SUNY Poly device or information on SUNY Poly’s IT Resources during the course of a legal matter, an examination/inquiry of damaging, illegal, unethical, and/or prohibited actions and/or in response to a Freedom of Information Law request.  Prior to investigating, written approval shall be obtained from the President or the President’s designee.  When investigating IT Resources, SUNY Poly officials should attempt to avoid accessing information that is personal in nature and not relevant to the inquiry. Unauthorized access of devices or information on SUNY Poly’s IT Resources is prohibited.

SUNY Poly may impose restrictions on the use of a particular IT Resource.  For example, SUNY Poly may block access to certain websites or services not serving legitimate business purposes or may restrict Authorized Users’ ability to attach devices to SUNY Poly IT Resources (e.g., personal USB drives, iPods).

**3.1 Acceptable Use**

All uses of IT Resources shall comply with SUNY Poly policies, standards, procedures, and guidelines, as well as any applicable Federal, State, and local laws, including copyright laws and licensing agreements.

Consistent with the foregoing, acceptable use of SUNY Poly IT Resources encompasses the following duties:

* Protection of confidential information from unauthorized use or disclosure;
* Observing authorized levels of access and utilizing only approved technology devices or services; and
* Immediately reporting suspected computer security incidents to the appropriate manager and the SUNY Poly Information Security Officer (“ISO”).

**3.2 Unacceptable Use**

The following list is not intended to be exhaustive, but is an attempt to provide a framework for activities that constitute unacceptable use.  Authorized Users may be exempted from one or more of these restrictions during the course of their authorized job responsibilities, after approval from SUNY Poly management, in consultation with SUNY Poly IT management (e.g., storage of objectionable material in the context of a disciplinary matter).

Unacceptable use includes, but is not limited to, the following:

* Distributing, transmitting, posting, or storing any communications, material or correspondence that is threatening, obscene, harassing, pornographic, offensive, defamatory, discriminatory, inflammatory, illegal, or intentionally false or inaccurate unless an exception has been granted to the Authorized User in writing by the Chief Information Officer or the President’s designee;
* Purporting to represent SUNY Poly in matters unrelated to official authorized job duties or responsibilities;
* Connecting unauthorized devices to a SUNY Poly network or any other SUNY Poly IT Resource;
* Connecting SUNY Poly IT resources to unauthorized networks;
* Connecting to any unauthorized wireless network while simultaneously physically connected to a SUNY Poly wired network;
* Installing, downloading, or running software on SUNY Poly’s IT Resources to conduct SUNY Poly business activities that have not been approved following appropriate security, legal, and/or IT review in accordance with SUNY Poly policies, unless for situations involving education, educational research or which are otherwise protected by the concept of academic freedom an exception is granted in writing by the Chief Information Officer or the President’s designee;
* Conducting official SUNY POLY business outside of the designated email environment;
* Using SUNY Poly IT Resources to circulate unauthorized solicitations or advertisements for non-SUNY Poly purposes including for religious, political, or not-for-profit entities;
* Providing unauthorized third parties, including family and friends, access to SUNY Poly IT Resources or facilities [facilities?];
* Using SUNY Poly IT Resources for commercial or personal purposes to support “for-profit” activities or to support outside employment or business activity (e.g., consulting for pay, business transactions);
* Propagating chain letters, fraudulent mass mailings, spam, or other types of undesirable and unwanted email content using SUNY Poly IT Resources; and
* Tampering, disengaging or otherwise circumventing SUNY Poly or third-party IT security controls.

**3.3   Personal Use**

Personal use of IT Resources, including the use of personal technology devices to interact with SUNY Poly’s IT Resources, shall adhere to all applicable SUNY Poly policies and cannot involve damaging, illegal, unethical, or prohibited actions.  Further, such use shall be consistent with: this policy; the requirements of Executive Order No. 7;[[1]](#footnote-1) and shall not impede the ability of the individual or other users to fulfill their SUNY Poly responsibilities and duties, including but not limited to, extensive bandwidth, resource, or storage utilization.  SUNY Poly, through the Chief Information Officer or the President’s designee may revoke or limit this privilege at any time.

An Authorized User’s judgment regarding incidental and occasional personal use is important.  While this policy does not attempt to articulate all required or proscribed behavior, it does seek to assist in the exercise of good judgment.  Any Authorized User who is unclear about the acceptable “personal” use of a SUNY Poly provided IT Resource should seek authorization from his/her immediate supervisor.

**3.4   Individual Accountability**

Individual accountability is required when accessing any and all SUNY Poly IT Resources.  Each individual is responsible for protecting against unauthorized activities performed under her/his assigned user ID.  This includes locking computer screens when an authorized user walks away from his/her system and protecting credentials (e.g., passwords, tokens or similar technology) from unauthorized disclosure, including sharing.  Credentials shall be treated as confidential information and shall not be disclosed or shared.

**4.0   Restrictions on Off-Site Transmission and Storage of Restricted Data Information**

Authorized Users must not transmit non-public, confidential, sensitive, or restricted SUNY Poly information to or from personal email accounts (e.g., Gmail, Hotmail, Yahoo) or use a personal email account to conduct SUNY Poly business unless explicitly authorized.  **Authorized Users must not store non-public, confidential, sensitive or restricted SUNY Poly information on a non-SUNY Poly issued device, or with a third party file storage service that has not been approved for such storage by SUNY Poly management in consultation with appropriate IT personnel.**

Devices that contain SUNY Poly information must be attended at all times or physically secured and must not be checked in transportation carrier luggage systems.

**5.0   User Responsibility for IT Equipment**

Authorized Users are routinely assigned or given access to IT equipment in connection with their official duties.  This equipment belongs to SUNY Poly and shall be immediately returned upon request or at the time an employee is separated from SUNY Poly service.  Authorized Users may be financially responsible for the value of equipment assigned to their care if it is not returned to SUNY Poly.  Should SUNY Poly IT equipment be lost, stolen or destroyed, Authorized Users are required to provide a written report of the circumstances surrounding the incident.  Authorized Users may be subject to disciplinary action, which may include repayment of the replacement value of the equipment.  SUNY Poly has the discretion to not issue or re-issue IT devices and equipment to Authorized Users who repeatedly lose or damage SUNY Poly IT equipment.

**6.0   Use of Social Media Accounts**

Accounts used to manage SUNY Poly’s social media presence are Privileged Accounts, as defined in Section 8.0, below, and shall be treated as such.  These accounts are for official use only and shall not be used for personal use.  Passwords for Privileged Accounts shall follow SUNY Poly information security standards, be unique on each site, and shall not be the same as those used to access other SUNY Poly IT Resources.

As with other SUNY Poly data and records, information posted online on behalf of the SUNY Poly may be subject to the record retention/disposition provisions of the Arts and Cultural Affairs Law and may be subject to Freedom of Information Law (FOIL) requests.

The “Use of Social Media” policy provides additional guidelines concerning how individuals may use accounts to manage SUNY Poly’s social media presence.

?? Social media policy?

Verbiage below from NYS AU Policy

Use of Social Media

The use of public social media sites to officially promote SUNY Poly activities requires written pre-approval of the SUNY Poly executive management. Approval is at the discretion of SUNY Poly’s executive management and may be granted upon demonstration of a business need and review and approval of service agreement terms by SUNY Poly legal, if appropriate. Final approval by the executive management will define the scope of the approved activity, including, but not limited to, identifying approved users.

Unless specifically authorized by SUNY Poly, the use of SUNY Poly email addresses on public social media sites is prohibited. In those instances in which Authorized Users access social media sites on their own time utilizing personal resources, they must remain sensitive to expectations that they will conduct themselves in a responsible, professional, and secure manner with regard to references to SUNY Poly and its employees, staff and students. These expectations are outlined below.

### Use of Social Media within the Scope of Official Duties

SUNY Poly’s executive management, or designee, must review and approve the content of any official posting of public information, such as blog comments, tweets, video files, or streams, to social media sites on behalf of SUNY Poly. However, SUNY Poly approval is not required for postings to public forums for technical support, if participation in such forums is within the scope of the Authorized User’s official duties, has been previously approved by his/her supervisor, and does not include the posting of any sensitive or confidential information, including specifics of SUNY Poly’s IT infrastructure. In addition, SUNY Poly approval is not required for postings to private SUNY Poly approved social media collaboration sites (e.g., Yammer). Blanket approvals may be granted, as appropriate.

Accounts used to manage SUNY Poly’s social media presence are Privileged Accounts, as defined in Section 8.0, below, and must be treated as such. These accounts are for official use only and must not be used for personal use. Passwords for Privileged Accounts must follow SUNY Poly information security standards, be unique on each site, and must not be the same as those used to access other SUNY Poly IT Resources.

As with other SUNY Poly data and records, information posted online on behalf of the SUNY Poly may be subject to the record retention/disposition provisions of the Arts and Cultural Affairs Law and may be subject to Freedom of Information Law (FOIL) requests.

### Guidelines for Personal Use of Social Media

Authorized Users should be sensitive to the fact that information posted on social media sites reflects on the individual and may reflect on the individual’s professional life. Consequently, Authorized Users should use discretion when posting information on these sites and be conscious of the potential perceptions of and responses to the information.  It is important to remember that once information is posted on a social media site, it can be captured and used in ways not originally intended.  Posted information is nearly impossible to retract, as it often lives on in copies, archives, backups, and memory cache.

Authorized Users should respect the privacy of other members of the SUNY Poly community and not post identifying information of any individual without permission (including, but not limited to, names, addresses, photos, videos, email addresses, and phone numbers).  When an Authorized User chooses to post comments on social media sites, the Authorized User is legally responsible for the comments.

If a personal email, posting, or other electronic message could be construed to be an official SUNY Poly communication, a disclaimer is strongly recommended.  A disclaimer might be:  “The views and opinions expressed are those of the author and do not necessarily reflect those of SUNY Poly, the State University of New York or the State of New York.”

Authorized Users should not use their personal social media accounts for SUNY Poly official business, unless specifically authorized by SUNY Poly executive management. Authorized Users are strongly discouraged from using the same passwords in their personal use of social media sites as those used to access SUNY Poly IT Resources, to prevent unauthorized access to SUNY Poly IT Resources in the event that the password is compromised.

**7.0 Policy Compliance**

This policy shall take effect upon publication.  SUNY Poly shall review the policy at least once every year to ensure relevancy.  SUNY Poly may also assess Authorized User’s compliance with this policy.

If compliance with this policy is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, the Authorized User is required to request an exception through the SUNY Poly [Exception Process](http://www.its.ny.gov/document/information-security-exception-policy).

Any violation of this policy may subject the Authorized User to disciplinary action, civil penalties, and/or criminal prosecution.  SUNY Poly will review alleged violations of this policy on a case-by-case basis and pursue recourse, as appropriate.

**8.0 Definitions of Key Terms**

|  |  |
| --- | --- |
| **Information Technology(IT) Resources** | Equipment or services used to input, store, process, transmit, and output information, including, but not limited to, desktops, laptops, mobile devices, servers, telephones, fax machines, copiers, printers, Internet, email, and social media sites. |
| **Privileged Account** | A privileged account is an account which provides increased access and requires additional authorization. Examples include a network, system, social media or security administrator account. |
| **Restricted Data** | Data in any format that is collected, created, or maintained by or on behalf of the SUNY Poly and its affiliates, or within the scope of SUNY Poly activities AND subject to specific protections under federal or state law or regulations, or legal contracts. (Note: This definition is used by the University of Florida.) |
| AUTHORIZED USER | Faculty, staff, students and all other individuals (e.g., contractors, vendors, guests, solution providers), that access SUNY Poly information or IT resources with consent. |

**9.0 Revision Schedule and Revision History**

|  |  |  |
| --- | --- | --- |
| **Date** | **Description of Change** | **Reviewer** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1. Executive Order No. 7 Prohibitions Against Personal Use of State Property and Campaign Contributions to the Governor states, among other things, that:  State computers shall be used only for official business, except that state computers may be used for incidental and necessary personal purposes, such as sending personal electronic mail messages. [↑](#footnote-ref-1)