SUNY ADIRONDACK

Policy Title:	Acceptable Use of Information Technology Resources
Document #:	6000
Effective Date:	3/21/19
Category:	Technology
Responsible Office:	Information Technology Services
This policy applies to:	Employees, Affiliated Entity Employees, Students and Authorized Guests

Table of Contents:

Summary:

The College provides its Employees, Affiliated Entity Employees, Students and Authorized Guests (collectively, the "Users") with access to information technology equipment, software and data. The College protects and preserves the privilege of use of College Information Technology Systems to ensure Users have access to reliable information technology that is safe from unauthorized or malicious use.

Policy:

The College provides standards and guidelines to protect Users of information technology equipment, software and data from illegal and/or harmful actions. All Users are responsible for appropriate and acceptable use of College Information Technology Systems.

1. Responsibilities of Users

   The College makes every attempt to ensure that information technology equipment, software, data and its users are protected from any illegal and/or harmful activity. However, Users should be aware that the College cannot guarantee security and confidentiality. Therefore, it is the responsibility of all Users to ensure proper use of College Information Technology Systems including:

   a. Use that is efficient and consistent with the College's mission, values, policies, manuals, handbooks, and standard/best practice guides.

b. Use which consistently protects the confidentiality, integrity, and availability of Data. This includes the responsibility of all Users to ensure that:
    i. Data is accurate, including the prevention of any defacement or mishandling;
    ii. Data is restricted based on the needs of a job function, and ensure that proper authorization has been granted for all data that is accessed;
    iii. Data is available for appropriate stakeholders;
    iv. Confidential Data is rigorously protected and used solely for College purposes.

c. Use that complies with federal, state and local law (including, but not limited to, all laws outlined in the Legal Standards section below), including copyright and intellectual property rights as well as license agreements and contracts.

2. Privacy and Monitoring

The College reserves the right at any time to monitor and access any data, including the contents of any College computer or College communication, for any legitimate business or legal reason. Portions of the technology infrastructure include automatic and manual monitoring and recording systems that are used for reasons that include, but are not limited to, security, performance, backup, and troubleshooting.

3. Personal Use

The College reserves the right to restrict personal use of College Information Technology Systems. While these systems are provided for College use only, the College recognizes that occasional, brief personal uses of computers may be necessary from time to time to attend to personal matters that cannot be handled outside work/school hours. Personal use of systems must not interfere with or disrupt any College business or educational use. Use of personal equipment on the wireless network is allowed.

4. Prohibited Behavior

a. Circumvention of any security systems and/or procedures, including any unauthorized activities aimed at compromising system or network security, including: hacking, probing, or scanning; attempts to break into other users' accounts or to obtain passwords; use of computer viruses, worms, or any kind of spyware or malicious software; use of an unauthorized firewall.
b. Sharing a username or password with another person, or using another’s account name or password; using a College password with any non-college system.
c. Storing non-protected confidential data on non-college systems.
d. Removing/transmitting/copying non-protected confidential data from College Information Technology Systems without authorization.
e. Any attempt to add or reconfigure any College Information Technology System, connecting a personal computer or other non-college computing device to the wired network, without written authorization from the Chief Information Officer.
f. Running IT servers, whether virtual or physical, without the written authorization from the Chief Information Officer.
g. Attempts to forge email or other electronic information or any actions that degrade the accuracy of data.
h. Using College Information Technology Systems for any unlawful activity including but not limited to accessing child pornography, illegally downloading copyrighted

material, or violating any license agreement or intellectual property rights in any way.

i. Using College systems to send spam, pranks, chain letters, pyramid schemes or other activities that negatively impact resources.
j. Using College Information Technology Systems in ways which violate College policy.

5. Legal Standards

All Users are expected to abide by all Federal, State and local laws. The following list is used for illustrative purposes, and is not intended to be a comprehensive guide:

a. FERPA (Family Educational Rights and Privacy Act): regulates the confidentiality of student records.
b. GLBA (Graham Leach Bliley Act): regulates the confidentiality of financial information.
c. HIPAA (Health Insurance Portability and Accountability Act): regulates the security and privacy of health information.
d. PCI DSS (Payment Card Industry Data Security Standard): regulates the confidentiality of credit card information.
e. DMCA 1998 (Digital Millennium Copyright Act): regulates the protection of intellectual property.
f. USC Title 18 §1030 (United States Code: Fraud and related activity in connection with computers)

6. Unauthorized Use/Violations

All Users of College information technology will comply with this policy. Violations are unethical and may constitute a criminal offense.

a. If a user suspects an account has been compromised, it must be reported immediately to the Chief Information Officer or designee.

b. All individuals doing work on behalf of the Collage are encouraged to report potential violations of this policy. Reports can be made to a direct supervisor, department head or chair; the Chief Information Officer; the Director of Compliance and Risk Management; a Vice President or the President. Any allegations will be investigated and reviewed. Retaliation against any user reporting a concern is prohibited.

c. An individual found to be in violation of this policy may be subject to loss or limitation of use of information technology resources; financial lability for the cost of such use and/or abuse; legal action, other action and/or formal disciplinary action, in accordance with applicable Federal laws; Chapter 156 and 165.15 of the New York State Penal Law; laws of the State of New York and the United States of America; the College's Codes of Conduct; College and/or State University of New York [SUNY] policies, applicable employee and student handbooks or collective bargaining agreements which may result in suspension, demotion or termination as deemed appropriate.

Definitions:

Affiliated Entity. Per the Board of Trustees Policy Manual Section 9.1 - 9.3, the purpose, relationship, responsibility and agreements between the SUNY Adirondack Foundation, Faculty-Student Association and the Adirondack Housing Association, are outlined.

Authorized Guest: Any special adjunct faculty, employees of affiliated entities, external contractors or partners and any other individual that is granted access or use of SUNY Adirondack's technology services or resources.

College. Use of this term explicitly refers to Adirondack Community College and/or the College's acceptable short name, SUNY Adirondack.

College Information Technology Systems: This applies to all technology equipment, software and data owned or supported by SUNY Adirondack which includes, but is not limited to, computers and mobile devices and any data contained on them, external storage devices, printers, network and server resources such as Banner, Blackboard, internet access, email, file shares, software, and system/user accounts.

Confidential Data: Information that includes, but is not limited to, student or employee records (social security number, ID number, grades, financial data, account numbers, bills, employee performance reviews, personnel files, personal information), business data (credit card numbers, account information, passwords, etc.), and any other information deemed confidential by SUNY Adirondack.

Data: All information used by the College in its academic or business operations.

Protected Data: Confidential data that is encrypted, password protected or stored on encrypted drives.

Other Related Information:

Board of Trustees Policy Manual Section 8 - General
N:\Policies, Processes, Procedures and Guidelines\Board of Trustees\Section 8 General Policies

Email as an Official Means of Communication for Employees Policy
N:\Polices, Processes, Procedures and Guidelines\Technology\ # 6001 Email as an Official Means of Communication for Employees

Processes and Procedures:

None

Forms:

There are no related forms relevant to this policy.

Authority:
Authority to Approve: President
Responsible for Oversight: Chief Information Officer

History:
This is the first acceptable use of information technology resources policy. This policy was approved by the President on 3/13/19.

Review:
Annually in August.

Appendices:
None