Network Acceptable Use Policy

I. Purpose

The College Network incorporates all electronic communication systems and equipment at the Independence Community College (the "College"). This Network Acceptable Use Policy ("AUP") sets forth the standards by which all Users may use the shared College Network.

The College Network is provided to support the College and its mission of education, service, and research. Any other uses (other than permitted personal use as discussed below), including uses that jeopardize the integrity of the College Network, the privacy or safety of other Users, or that are otherwise illegal are prohibited. The use of the College Network is a revocable privilege.

By using or accessing the College Network, Users agree to comply with this AUP and other applicable College policies which may be implemented from time to time, as well as all federal, state, and local laws and regulations. Only Users are authorized to use and/or access the College Network.

The term "User" refers to any faculty, staff, or student associated with the College, as well as any other individual with access to computers or other network devices that have been approved by the Chief Information Officer for connection to the College Network. This definition includes, but is not limited to, contractors, visitors, and temporary affiliates.

II. Principles

General requirements for acceptable use of the College Network are based on the following principles:

1. Each User is expected to behave responsibly with respect to the College Network and other Users at all times.
2. Each User is expected to respect the integrity and the security of the College Network.
3. Each User is expected to behave in a manner consistent with College's mission and comply with all applicable laws, regulations, and College policies.
4. Each User is expected to be considerate of the needs of other Users by making every reasonable effort not to impede the ability of others to use the College Network and show restraint in the consumption of shared resources.
5. Each User is expected to respect the rights and property of others, including privacy, confidentiality and intellectual property.
6. Each User is expected to cooperate with the College to investigate potential unauthorized and/or illegal use of the College Network.
7. Each User is expected to respect the security and integrity of College computer systems and data.

III. Prohibitions

Without limiting the general guidelines listed above, unless expressly agreed to by the Chief Information Officer, the
following activities are specifically prohibited:

1. Users may not attempt to disguise their identity, the identity of their account or the machine that they are using.
2. Users may not attempt to impersonate another person or organization. Users may likewise not misuse or appropriate the College's name, network names, or network address spaces.
3. Users may not attempt to intercept, monitor, forge, alter or destroy another User's communications. Users may not infringe upon the privacy of others' computer or data. Users may not read, copy, change, or delete another User's data or communications without the prior express permission of such other User.
4. Users may not use the College Network in a way that (a) disrupts, adversely impacts the security of, or interferes with the legitimate use of any computer, the College Network or any network that the College connects to, (b) interferes with the supervisory or accounting functions of any system owned or managed by the College, or (c) take action that is likely to have such effects. Such conduct includes, but is not limited to: hacking or spamming, placing of unlawful information on any computer system, transmitting data or programs likely to result in the loss of an individual's work or result in system downtime, sending "chain letters" or "broadcast" messages to lists or individuals, or any other use that causes congestion of any networks or interferes with the work of others.
5. Users may not distribute or send unlawful communications of any kind, including but not limited to cyberstalking, threats of violence, obscenity, child pornography, or other illegal communications (as defined by law). This provision applies to any electronic communication distributed or sent within the College Network or to other networks while using the College Network.
6. Intentional access to or dissemination of pornography by College employees, temporary staff, contractors, or vendors is prohibited unless (1) such use is specific to work-related functions and has been approved by the respective manager or (2) such use is specifically related to an academic discipline or grant/research project. This

provision applies to any electronic communication distributed or sent within the College Network or to other networks while using the College Network.

7. Users may not attempt to bypass network security mechanisms, including those present on the College Network, without the prior express permission of the owner of that system. The unauthorized network scanning (e.g., vulnerabilities, post mapping, etc.) of the College Network is also prohibited.

8. Users may not engage in the unauthorized copying, distributing, altering or translating of copyrighted materials, software, music or other media without the express permission of the copyright holder or as otherwise allowed by law. Information on the Digital Millennium Copyright Act can be found at:http://www.copyright.gov/legislation/dmca.pdf and the Copyright Act at: http://www.copyright.gov/title17/.

9. Except as allowed under the Personal Use Policy or the Policy on Use of College Resources in Support of Entrepreneurial Activities. Users may not use the College Network for private business, commercial or political activities, fundraising, or advertising on behalf of non-College organizations, unlawful activities, or uses that violate other College policies.

10.Users may not extend or share with public or other users the College Network beyond what has been configured accordingly by the Department of Information Technology. Users are not permitted to connect any network devices or systems (e.g., switches, routers, wireless access points, VPNs, and firewalls) to the College Network without advance notice to and consultation with the Department of Information Technology at the College.

11.Users are responsible for maintaining minimal security controls on their personal computer equipment that connects to the College Network, including but not limited to: current antivirus software, current system patches, and strong passwords.

12.Users may not violate any laws or ordinances, including, but not limited to, laws related to copyright, discrimination, harassment, threats of violence and/or export controls.

IV. Review and Penalties

The College reserves the right to review and/or monitor any transmissions sent or received through the College Network. College access to electronic mail on the College Network is permitted in accordance with the College’s Policy on the Privacy of Electronic Information. Access to other transmissions sent or received through the College Network may occur in the following circumstances:

1. In accordance with generally accepted, network-administration practices.
2. To prevent or investigate any actual or potential information security incidents and system misuse, if deemed necessary by authorized personnel.
3. To investigate reports of violation of College policy or local, state, or federal law.
4. To comply with legal requests for information (such as subpoenas and public records requests).
5. To retrieve information in emergency circumstances where there is a threat to health, safety, or College property involved.

Penalties for violating this AUP may include:

6. Restricted access or loss of access to the College Network;
7. Disciplinary actions against personnel and students associated with the College.
8. Termination and/or expulsion from the College, and Civil and/or criminal liability.

The College, in consultation with its legal counsel, may contact local or federal law enforcement authorities to investigate any matter at its sole discretion.

V. Policy Updates

The College reserves the right to update or revise this AUP or implement additional policies in the future. Users are responsible for staying informed about College policies regarding the use of computer and network resources and complying with all applicable policies. The College shall provide notice of any such modifications or amendments by email to the College community. Any such modification shall be effective immediately upon notice being provided regardless of whether subscriber actually reads such notice. The current version of this policy can be found at ??.

VI. Additional IT Acceptable Use Policies

Additional policies related to the acceptable use of other IT systems and services at the College can be found at ?? .

Data Network Infrastructure Policy

Policy on the Privacy of Electronic Information

Personal Use Policy

Policy on Use of College Resources in Support of Entrepreneurial Activities

Data Network Infrastructure Policy

As with any large public utility, such as basic telephony services or electrical distribution, the College communications infrastructure needs to be centrally planned, managed and maintained. It is only through centrally coordinated information technology strategic planning and implementation that the core technology goals of the institution are met.

An aggregation of separate, discrete, and privately-managed backbone or “backbone-like” data, voice or video networks does not constitute a utilities infrastructure that can meet these institutional goals nor does it provide for the best and most efficient return on the College’s investment in this infrastructure.

To ensure a high-performance, high-availability, production-quality communications infrastructure at Independence Community College, the Department of Information Technology must provide a number of components and architectural considerations, as described below.

To ensure reliability, security and efficient use of limited resources, the Department of Information Technology must

develop and implement the physical connectivity design: how buildings connect to the campus fiber infrastructure. The design architecture for the physical layer consists of all campus buildings being designated as hubs or spurs, based on the fiber path and proximity to other buildings. All spur buildings connect to a high-speed switch port in an adjacent hub building. All hub buildings connect to high-speed switch ports in the Cessna Learning Center not only for security and high-reliability considerations, but also for high-performance connectivity to the Department of Information Technology’s production systems and to the Internet.

To ensure compatibility, mobility, bandwidth and security, the Department of Information Technology must design, implement and maintain the campus networking architecture. This higher layer architecture is currently based on high-speed switching technologies, with support for virtual LANs and Layer 3 switching, incremental bandwidth upgrades where appropriate (based on proactive traffic management), and support for meshed topologies to allow for

load balancing and alternate paths.

To ensure compatibility and high performance, the Department of Information Technology must maintain campus Internet connectivity. This connectivity is presently based on redundant high speed links to Cable One and AT&T, which requires a single campus entity for coordination and management.

To ensure reliability, the Department of Information Technology must support a 8Å~5-staffed operations center to provide proactive performance monitoring and to react immediately to any unscheduled outages. This also includes maintaining appropriately configured spares of all network electronic components.

To ensure security, only appropriate Department of Information Technology personnel will be permitted to monitor traffic over backbone links through network protocol analyzers (sniffers). The design of both the fiber physical connectivity and of the networking architecture do not allow random, unauthorized traffic eavesdropping across the links: all fiber terminations are in locked cabinets, port mirroring is permitted only through the secured network management system, and the nature of network switching eliminates the shared topologies of earlier network systems. In any case, the Department of Information Technology continues to maintain that the emphasis on security needs to be at the host system level.

To ensure reliability, security and high performance, the Department of Information Technology must provide central management of network devices and systems to the wall-plate in all Independence Community College locations. Any and all data network electronics must be managed by the Department of Information Technology. This includes any and all 802.11 WiFi wireless access points and switches. Note: On-campus resident students will not be allowed to use networking equipment (i.e. home routers, hubs).

In addition to the requirement that only the Department of Information Technology can install and maintain switches and routers on the campus data network, no device with multiple network interfaces (including, but not limited to, VPN gateways, firewalls, and servers) can be connected to the network without advance notice to and consultation with the Department of Information Technology. This advance notice must be submitted in the form of a Help Desk ticket. Failure to provide this advance notice will result in said devices being isolated from the network, and unable to communicate on the network. If the connection of said device is of an emergency nature (such as replacing an existing device), the ticket can be marked as Critical and we will receive immediate notification.

Policy on the Privacy of Electronic Information

I. Introduction and Purpose of this Policy

This Policy clarifies the applicability of law and certain other College policies to electronic mail and the College's Policy on the privacy of electronic information. Users are reminded that all uses of the College’s information technology resources, including electronic mail, are subject to all relevant College policies and relevant state and federal laws, including federal copyright law.

Appropriate use of College electronic resources includes instruction, research, service, and the official work of the offices, departments, recognized student and campus organizations, and other agencies of the College, and as described below, incidental personal usage by faculty, staff, and students. Since resources are not unlimited, the College may give priority for resources to certain uses or certain groups of users in support of its mission. Consistent with the College's non-discrimination policy, the use of information resources should not be denied or abridged because of race, creed, color, sex, sexual orientation, religion, national origin, age, or physical disability.

II.Privacy of Email Files

The College encourages the use of electronic mail and respects the privacy of users. It does not inspect or monitor electronic mail routinely, nor is the College responsible for its contents. Nonetheless, users of electronic mail systems should be aware that, in addition to being subject to authorized access as detailed below, electronic mail in its present form cannot be secured and is, therefore, vulnerable to unauthorized access and modification by third parties. Receivers of electronic mail documents should check with the purported sender if there is any doubt about the identity of the sender or the authenticity of the contents, as they would with print documents.

Users of electronic mail services also should be aware that even though the sender and recipient have discarded their copies of an electronic mail record, there may be back-up copies of such electronic mail that can be retrieved on College systems or any other electronic systems through which the mail has traveled.

College electronic mail services may, subject to the foregoing, be used for incidental personal purposes provided such use does not interfere with College operation of information technologies including electronic mail services, burden the College with incremental costs, or interfere with the user's employment or other obligations to the College.

Access by authorized College employees to electronic mail stored on the College's network of computers may be necessary to ensure the orderly administration and functioning of College computing systems. Such access, gained for purposes such as to back up or move data, ordinarily should not require the employee gaining access to the electronic mail to read messages. The College requires employees, such as system administrators, who as a function of their jobs routinely have access to electronic mail and other electronically stored data to maintain the confidentiality of such information.

Access to electronic mail on the College's network of computers that involves reading electronic mail may occur only where authorized by the College officials designated below and only for the following purposes:

1. Troubleshooting hardware and software problems, such as rerouting or disposing of undeliverable mail, if deemed necessary by the Chief Information Officer or his or her authorized designee.
2. Preventing or investigating unauthorized access and system misuse, if deemed necessary by the Chief Information Officer.
3. Retrieving or reviewing for College purposes College-related information*.
4. Investigating reports of violation of College policy or local, state, or federal law*.
5. Investigating reports of employee misconduct. *
6. Complying with legal requests for information (such as subpoenas and public records requests)*; and
7. Retrieving information in emergency circumstances where there is a threat to health, safety, or College property involved*.

*The system administrator will need approval from the President and General Counsel or their designee(s) approved by the President to access specific mail and data for these purposes. The extent of the access will be limited to what is reasonably necessary to acquire the information for a legitimate purpose.

In addition to the foregoing, when a College employee leaves employment or when a student graduates or otherwise withdraws from the College, a system administrator may, with approval of the unit head to which the employee was assigned or in which the student was enrolled, remove the departing employee's or student's email files from College systems in order to conserve space or for other business purposes. An employee's email may be retained and accessed by the unit as necessary for use in connection with College business. A student's email should be deleted unless otherwise required in connection with College business. In all such cases the extent of the access will be limited to what is reasonably necessary to acquire the information for a legitimate purpose. Units and departments are encouraged to make arrangements for disposition of email files with departing employees and students in advance of their departure.

III. Privacy of data, other than electronic mail, stored on College computers and networks

As is the case with electronic mail, access by authorized College employees to electronic data stored on the College's network of computers may be necessary to ensure the orderly administration and functioning of College computing systems. Such access may require the employee gaining access to the data to read specific files. The College requires system administrators and other employees who, as a function of their jobs, routinely have access to electronically stored data, to sign statements agreeing to maintain the confidentiality of such information.

In order to conduct its business without interruption, the College must have access to data stored on College computers and networks. Accordingly, for legitimate business purposes, the head of any College administrative unit or department may in his or her discretion authorize the accessing or retrieval of any files other than electronic mail stored on College computers under that unit or department's control. Where necessary and appropriate, College network support personnel may assist with retrieval of such information on behalf of a unit or department, even if the information is stored at a site other than the unit or department's computer systems.

There is no guarantee of privacy or confidentiality for documents or data stored on College-owned equipment.

IV. Public records consideration

Electronic mail and other data stored on College computers may constitute a public record like other documents subject to disclosure under the Kansas Public Records Act or other laws, or as a result of litigation. However, prior to such disclosure, the College evaluates all requests for information submitted by the public for compliance with the provisions of the Act or other applicable law.

Destruction of such records is governed by the Records Retention Policies of one's unit of employment. Information about such policies is available from one's supervisor. Incidental personal electronic mail may be destroyed at the user's discretion.

V. Conclusion

Wherever possible in a public setting, individuals' privacy should be preserved. However, there is no guarantee of privacy or confidentiality for data stored or for messages stored or sent on College-owned equipment. Persons with questions about the applicability of this Policy to specific situations should contact the Human Resources Department.

Violations of College policies governing the use of College electronic resources, including mail services, may result in restriction of access to College information technology resources in addition to any disciplinary action that may be applicable under other College policies, guidelines or implementing procedures, up to and including dismissal. Suspected violations of College Policy may be reported to helpdesk@indycc.edu.

Personal Use Policy

The use of the College's resources and services for non-official purposes is permitted only in compliance with the following criteria:

1. The cost to the College must be negligible.
2. The use must not interfere with a College employee's obligation to carry out College duties in a timely and effective manner. Time spent engaged in the non-official use of College resources is not considered to be College work time.
3. The use must in no way undermine the use of College resources and services for official purposes.
4. The use neither expresses nor implies sponsorship or endorsement by the College.
5. The use must be consistent with state and federal laws regarding obscenity, libel, or the like, and state and federal laws and College policies regarding political activity, the marketing of products or services, or other inappropriate activities.
6. Users should be aware that internal or external audit or other needs may require examination of uses of College resources or services and should not expect such uses to be free from inspection.

Application: Each case will depend upon the particular circumstances and other important factors such as materiality or reasonableness. The ultimate control, therefore, lies with each employee's supervisor, as that person should have direct knowledge of the behaviors and needs of the individual employee.

Appropriateness of Practices: Employees should consult with their supervisors in advance if they have any questions about appropriateness of certain practices. A supervisor's decision cannot, however, circumvent other policies and procedures of Independence Community College that may restrict personal use beyond the limitations cited herein. For example, the use of the College's telephones, fax machines, mail services, and vehicles must comply with existing College policies, and the use of College resources in political activity is prohibited.

Telephones and Fax Machines: Only calls related to College business may be charged to College lines or calling cards. Personal calls may not be billed to College telephone numbers. Personal long distance calls may be made from College telephones only when these calls are placed as credit card, collect, third number (non-College) calls. This telephone policy also applies to the use of College fax machines.

Mail Services: College Mail Services states, "The campus mail system will be used solely for the distribution of U.S. mail delivered to the Campus Mail Center and for intra-College mail, including publications produced by the College or its related units but excluding student publications." The College mail system will not be used for the distribution of non-College related publications that are designed primarily for free circulation, nor for printed publications containing only advertising or designed primarily for advertising purposes. Use of the campus mail system for real estate advertising, chain letters, or private use for personal advantage is specifically prohibited. Individuals or departments that abuse the campus mail service will, at a minimum, be billed regular first class postage for all copies distributed.

Vehicles: A supervisor also cannot allow the use of a State vehicle that is not in compliance with Motor Pool Policy.

Political Activity: Political activity by College employees is regulated by Federal and State law and College policy. No employee may use College funds, vehicles, equipment, supplies, or other resources in connection with partisan political activities. This includes the use of College electronic resources.

Reason for Policy

Public Trust: The College deals constantly with the public's perception of how we conduct the business of the College. All College employees must be constantly mindful of the public trust that we discharge, of the necessity for conducting ourselves with the highest ethical principles, and avoiding any action that may be viewed as a violation of the public trust. As custodians of resources entrusted us by the public, government entities, and private donors, we
should always be mindful of how we utilize these resources. As members of a campus community, we should also be
mindful of our responsibility to act so that others are not deprived of access to these same resources as they perform their duties. These resources include, but are not limited to, employee's time, facilities, supplies, and equipment, such as telephones, fax machines, and computers.

Accountability: In any business environment, however, accountability must be balanced with a consideration of the needs of employees to carry on normal day-to-day responsibilities related to their personal lives. The complex task of balancing accountability to the State with the life-needs of employees calls for the College to provide direction for managers when weighing these two essential obligations.

Support of Entrepreneurial Activities

Independence Community College values and supports entrepreneurial activity by faculty. Consistent with the College’s goal to support the economic development of the Independence and the State of Kansas, entrepreneurial activities of College faculty are considered part of their duties. Faculty use of College resources in support of appropriate entrepreneurial activities may be allowed provided these activities do not conflict with applicable policies regarding use of public facilities for private gain. Incidental and minimal use of office, library, personal desktop work stations, storage servers, communication devices, or clerical staff is permitted.

For the purpose of this policy, “entrepreneurial activities” performed by a member of the College faculty as part of College duties are activities that contribute to the College’s economic development, technology transfer or other public service goals. Examples include environmental or educational issues, a startup company in which the College expects to acquire an equity position through licensing College intellectual property, or activities in support of the development of a licensing agreement with an established company. Where activities are undertaken purely for an employee’s personal gain without connection to the College’s mission, use of College resources in support of such activities is not appropriate except as otherwise allowed by College policy.

Consulting activities undertaken as allowed are not considered entrepreneurial activities that are part of the faculty member’s College duties unless they are so noted.

While this policy is meant to clarify and encourage such activity, faculty should be aware that other current College policies remain in place and are thus applicable to certain aspects of entrepreneurial activity.