UNIVERSITY OF
NORTHERN
COLORADO

University Regulations
Title 3. University Regulations
Article 9: Information Technology

Part 1: Information Technology Security Plan

3-9-101 Purpose. This information Security Plan (“Plan”) describes the University of Northern Colorado’s (UNC) safeguards to protect certain data and information which Federal and State laws and regulations require be protected herein after be referred as “covered data and information.” The purpose of the Plan is to: (1) ensure the confidentiality, integrity, and availability of covered data and information; (2) protect against threats or hazards to the confidentiality, integrity, and availability of such information; and (3) protect against unauthorized access to or use of covered data and information that could result in substantial harm or inconvenience to any student, faculty or staff, hereinafter referred to as “customer.”

3-9-102 This Information Plan Also Provides for Mechanisms to: (1) identify and assess the risks that may threaten covered data and information maintained by UNC; (2) develop written policies and procedures to manage and control these risks; (3) develop and implement technological solutions to manage and control these risks (4) implement and review the plan; and (5) adjust the plan to reflect changes in technology, the sensitivity of covered data and information and internal or external threats to information security.

3-9-103 Identification and Assessment of the Risks to Customer Information. UNC recognizes that it has both internal and external risks. These risks include, but are not limited to: (1) access of covered data and information whether in electronic or hard copy form by any unauthorized parties; (2) compromised system security as a result of system access by an unauthorized person; (3) interception of data during transmission; (4) loss of data confidentiality, integrity, and availability; (5) physical loss of data due to disaster, loss, or theft; (6) errors introduced into the system; (7) corruption of data or system; (8) unauthorized transfer of covered data and information through third parties.

3-9-104 List of Risks. UNC recognizes that the above may not be a complete list of the risks associated with the protection of covered data and information. Since technology growth is not static, new risks are created regularly. Accordingly, the Information

Technology Department will actively participate and monitor reputable advisory groups for identification of new risks.

3-9-105 Information Technology Safeguards. UNC believes that its current Information Technology safeguards are reasonable and sufficient to exercise due care and due diligence in providing confidentiality, integrity, and availability to covered data and information maintained by the University.

3-9-106 Information Security Plan Coordinators. The Assistant Vice President for Information Technology and the Assistant Vice President for Finance have been appointed as the coordinators of this Plan. They are responsible for assessing the risks associated with unauthorized access to and/or transfer of covered data and information and for implementing procedures to minimize those risks. Internal Audit Personnel will also conduct reviews of areas that have access to covered data and information to assess the internal control structure put in place by the administration and to verify that UNC departments comply with the requirements of this policy.

3-9-107 Employee Management and Training. Background checks will be conducted of new employees working in areas that regularly handle covered data and information, including but not limited to the Bursar's Office, Registrar, Financial Services, Student Financial Resources, Health Service and Human Resources, and Information Technology. Please see http://www.unco.edu/hr/job_opportunities.htm. During employee orientation, each new employee in these departments will receive proper training on the importance of confidentiality of student records, student financial information, and other types of covered data and information (including but not limited to the use of the unique UNC identifier, the "Bear Number"). Each new employee is also trained in the proper use of computer information and password management. Training also includes controls and procedures to prevent employees from providing confidential information to an unauthorized individual, including "pretext calling" ("Pretext calling" occurs when an individual improperly obtains personal information of the university customers so as to be able to commit identity theft. It is accomplished by contacting the University, posing as a customer or someone authorized to have the customer's information, and through the use of trickery and deceit, convincing an employee of the University to release customer identifying information) and how to properly dispose of documents that contain covered data and information. Each department responsible for maintaining covered data and information is instructed to take steps to protect the information from unauthorized access, alteration, destruction, loss or damage due to environmental hazards such as fire and water damage, or technical failures. Further, each department is responsible for maintaining covered data and information should coordinate with the General Counsel on an annual basis for the coordination and review of additional privacy training appropriate to the department. These training efforts should help to minimize risk and safeguard covered data and information.

3-9-107(1) Protocol. UNC employees contacted by others, including law enforcement agents, requesting covered data and/or university information must not disclose any such information prior to immediately notifying UNC's General Counsel who will advise them of the appropriate action.

3-9-107(2) Physical Security. UNC has addressed the physical security of covered data and information by limiting access to only those employees who have a business reason to know such information. For example, personal information, accounts, balances and transactional information are available only to UNC employees with an appropriate business need for such information.

3-9-107(3) Paper Documents. Loan files, account information, health information and other paper documents are kept in file cabinets, rooms or vaults that are not left unattended and are locked each night. Only authorized employees know the combinations and the location of keys. Paper documents that contain covered data and information are shredded at the time of disposal.

3-9-107(4) Information Systems. Access to covered data and information via UNC's computer information system is limited to those employees who have a business reason to know such information. Each employee is assigned a user name and password. Databases containing personal covered data and information, including, but not limited to, accounts, balances, health information and transactional information, are available to UNC employees in appropriate departments and positions.

3-9-107(5) Responsibility. UNC will take responsibility and appropriate steps consistent with current technological developments to make sure that all covered data and information is secure and to safeguard the confidentiality, integrity, and availability of records in storage and transmission. Information Technology requires that all servers must be registered before being allowed through UNC's firewall, thereby allowing Information Technology to verify that the system meets necessary security requirements as defined by Information Technology policies. These requirements include maintaining the operating system and applications, including applications of appropriate patches and updates in a timely fashion. User and system passwords are also required. In addition, an intrusion detection system has been implemented to detect and stop certain external threats, along with an incident response policy for occasions where intrusions do occur.

3-9-107(6) Encryption Technology. When commercially reasonable, encryption technology (please see www.unco.edu/cybersecurity for information regarding encryption) will be used for both storage and transmission. All covered data and information will be maintained on servers that are behind UNC's firewall. All firewall software and hardware maintained by Information Technology will be kept current. Information Technology has policies and procedures in place to provide security to UNC information systems. These policies are available upon request from the Assistant Vice President for Information Technology.

3-9-108 Management of System Failures. Information Technology has developed written plans and procedures to detect any actual or attempted attacks on UNC systems and has an incident response policy which outlines procedures for responding to an actual or attempted unauthorized access to covered data and information. This procedure is available upon request from the Assistant Vice President of Information Technology.

3-9-109 Selection of Appropriate Service Providers. Due to specialized expertise needed to design, implement, and service new technologies, vendors may be needed to provide resources that UNC determines not to provide on its own. In the process of choosing a service provider that will maintain or regularly access covered data and information, the evaluation process shall include ability of the service provider to safeguard all confidential information. Contracts with service providers may include the following provisions: (1) an explicit acknowledgement that the contract allows the contract partner access to confidential information; (2) a special definition or description of the confidential information being provided; (3) a stipulation that the confidential information will be held in strict confidence and accessed only for the explicit business purpose of the contract; (4) an assurance from the contract partner that the partner will protect the confidential information it receives according to commercially acceptable standards and no less rigorously than it protects its own confidential information; (5) a provision providing for the return or destruction of all confidential information received by the contract partner upon completion of the contract; (6) an agreement that any violation of the contract's confidentiality conditions may constitute a material breach of the contract and entitles UNC to terminate the contract without penalty; and (7) a provision ensuring that the contract's confidentiality requirements shall survive any termination requirement.

3-9-110 Continuing Evaluation and Adjustment. The Information Security Plan will be subject to periodic review and adjustment. The most frequent of these reviews will occur within Information Technology, where constantly changing technology and evolving risks mandate increased vigilance. Continued administration of the development, implementation, and maintenance of the program will be the responsibility of the designated Information Security Plan Coordinators who will assign specific responsibility for implementation and administration as appropriate. The Coordinators, in consultation with the General Counsel, will review the standards set forth in this policy and recommend updates and revisions as necessary. It may be necessary to adjust the plan to reflect changes in technology, the sensitivity of student/customer data and internal or external threats to information security. [Editor's Note: For specific policy concerning health related information please see HIPAA (Health Insurance Portability and Accountability Act) policy and procedures located under the Student Health Center website. For specific policy concerning student educational records please see FERPA (Family Education Rights and Privacy Act) policy and procedures located under the Dean of Students website.

Part 2: Information Technology Acceptable Use Regulation

3-9-201 Overview. The intention of this Regulation is not to impose restrictions that are contrary to the University of Northern Colorado's (UNC) established culture of openness, trust and integrity. UNC is committed to protecting faculty, staff, students and the University from illegal or damaging actions by individuals. Either knowingly or unknowingly. This Regulation explains the acceptable use of University of Northern Colorado's computing and communication resources, including computers, networks, electronic mail, electronic information sources, voice mail, telephone services and other communication resources.

3-9-202 Purpose. These rules are in place to protect the faculty, staff, students and the University. Inappropriate use exposes all parties to risks including loss of data or data integrity, exposure of personal and/or confidential data, malicious programs, systems compromise, and legal issues.

3-9-203 Scope. This Regulation applies to employees, contractors, consultants, temporary employees, students, and other workers at UNC including all personnel affiliated with third parties. This Regulation applies to all equipment that is owned or leased by UNC.

3-9-204 Regulation. UNC's computing and communications resources are university owned. These resources are to be used to further the university's mission of teaching, learning, the advancement of knowledge and community services. These resources shall be used in a manner consistent with the instructional, research, and administrative objectives of the University. Computing and communication resources are provided for the use of faculty, staff, currently admitted or enrolled UNC students and other properly authorized users. Access to the computing and communication resource environment is a privilege and must be treated as such by all users of these systems.

3-9-205 General Use. By acquiring an account or utilizing University electronic resources, users assume the responsibility to adhere to the following: (1) all computer users must comply with these regulations, state laws, federal laws and all other UNC regulations and policies; (2) individuals will refrain from activities that may damage or obstruct the network and electronic resources and information (such activities are described in Sections 3-9-207 and 3-9-208); (3) computer users are expected to secure their passwords and make them difficult to obtain or guess and are responsible for the security of and actions taken with their accounts; (4) no user shall, knowingly or unintentionally expose Personally Identifiable Information (PII) to unauthorized individuals. This includes, but is not limited to, information such as bear number, social security number and credit card information; (5) users must protect and backup critical data; UNC Information Technology is not obligated to maintain backups of any file for any particular length of time; individual users and university units should develop procedures and practices to ensure regular backups of data and implement steps to ensure that all critical data is compatible with all current generations of computing equipment and storage media and media readers; (6) all UNC units should implement procedures to ensure that access to sensitive data is restricted to those employees who have a need to access the information; (7) default passwords, such as those from a manufacturer, should be immediately changed; (8) agree to cooperate and comply with requests for access to and copies of email messages or data when access or disclosure is authorized by this regulation or required or allowed by law or other applicable procedures, regulations and policies; (9) because information contained on portable computers is especially vulnerable, special care should be exercised to protect these devices (see,http://www.unco.edu/cybersecurity for more information); (10) all devices that are connected to the UNC network, whether owned by the user or UNC, shall be patched to the most current level and running up to date virus-scanning software.

3-9-206 Privacy. UNC's computing resources, including all related equipment, networks and network devices, are provided for authorized UNC use only. UNC computer systems may be monitored for all official purposes. Use of UNC's computing infrastructure, authorized or unauthorized, constitutes consent to this regulation and the policies and procedures set forth by UNC. Evidence of unauthorized use collected during monitoring may be used for administrative action and/or criminal or civil prosecution by University legal counsel and law enforcement agencies. Under the Colorado Open Records Act, electronic files are treated the same as paper files. Any official university documents (as defined by law) in the files of employees of the State of Colorado are considered to be public documents, and may be subject to inspection through the Open Records Act. In such cases, the Legal Counsel to the Board of Trustees should inspect the contents of the applicable files to determine which portions may be exempt from disclosure. Any inspection of electronic files, and any action based upon such inspection will be governed by all applicable U.S. and Colorado laws and by university policy and regulations. (1) It is recommended that any information that users consider sensitive or vulnerable be encrypted; for guidelines on encrypting email and documents, please see http://www.unco.edu/cybersecurity for further information; (2) for security and network maintenance purposes, authorized individuals within UNC's Information Technology department may monitor equipment, systems and network traffic at any time; (3) UNC reserves the right to audit networks and systems on a periodic basis to ensure compliance with this regulation; (4) in cases of suspected violations of UNC policies and procedures, or when required by law, the system administrator may authorize detailed session logging; this may involve keystroke and session logging; in addition the system administrator may perform searches of user files to gather evidence on suspected violations; (5) University owned computers and equipment can be examined to detect unauthorized software use and to evaluate the security of the network; (6) all individuals must respect the rights and privacy of others, including intellectual property and personal property rights.

3-9-207 Unacceptable Use. Under no circumstances is an employee of UNC authorized to engage in any activity that is illegal under local, state, federal or international law, or that is against UNC rules and regulations while utilizing UNC owned resources. The activities listed below are strictly prohibited. These lists are by no means exhaustive, but provide a framework for the types of activities which fall into the category of unacceptable use.

3-9-208 Unacceptable System and Network Activities. (1) Knowingly using any computer, computer system, computer network or any part thereof for the purpose of devising or executing any scheme or artifice to defraud; obtain money, property, or service by means of false or fraudulent pretenses, representations, or promises; using the property or services of another without authorization; or committing theft; (2) negligent or intentional conduct that alters, damages, or destroys any computer, computer system, computer network, or any system logs, computer software, program documentation, or date contained in such computer, computer system, or computer network; (3) use of resources for personal or private business or commercial activities, fund raising or advertising on behalf of non-UNC organizations; (4) misrepresentation or forging your identity on any electronic communication; (5) unlawful communications, including threats of violence, obscenity, child pornography and harassing communications; (6) reselling of UNC resources or services; (7) failure to comply with requests from appropriate UNC officials to discontinue activities that threaten the operation or integrity of computers, systems or networks, or otherwise violate this regulation; (8) violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by UNC; (9) unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, movies, and the installation of any copyrighted software for which UNC or the end user does not have an active license; (10) exporting software, technical information, encryption software or technology, in violation of international or regional export control laws; (11) using a UNC's computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws; (12) making fraudulent offers of products, items, or services originating from any UNC account; (13) engaging in security breaches or disruptions of network communication (Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a device or account that the user is not expressly authorized to access, unless these activities are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network monitoring, ping floods, buffer overflows, spoofing, denial of service, and forged routing information for malicious purposes); (14) vulnerability and port scanning is expressly prohibited unless prior approval from the Information security office; (15) circumventing user authentication or security of any host, network or account; (16) using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet.

3-9-209 Unacceptable Email and Communications Activities. (1) Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam); (2) any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages; (3) unauthorized use, or forging, of email header information; (4) solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies; (5) creating or forwarding or replying to “chain letters” of any type; (6) use of unsolicited email originating from within UNC's networks of other Internet service providers on behalf of, or to advertise, any service hosted by UNC or connected via UNC's network; (7) posting the same or similar non-business-related messages to large numbers of Usenet newsgroups.

3-9-210 Enforcement. Those found to have violated this regulation may be subject to disciplinary action, up to and including criminal prosecution and/or termination of employment.

3-9-211 Related Policies, Procedures, and Codes of Conduct. All applicable laws and University policies, regulations and procedures bind UNC students and employees. Some applicable laws and procedures are listed below. This list is an illustration only. It is not intended to be exhaustive or to limit the applicability of any other law, policy, or regulation.

3-9-212 Mass E-mails to Campus. The University’s official electronic delivery method for communicating campus news, announcements and events to faculty, staff and students is through its e-newsletters. The Office of University Relations sends *UNC Today* by e-mail Monday through Friday, excluding holidays, to faculty and staff. *Around Campus* is a weekly e-newsletter sent to students during fall and spring semesters. Campus announcements also appear on Ursa (under the heading “Campus Announcements), http://ursa.unco.edu , UNC’s campus Web portal.

Making announcements through Ursa, *UNC Today* and *Around Campus* reduces, and in most cases eliminates, the need for sending e-mail to all faculty, classified, exempt and student through listservs. Ursa, *UNC Today* and *Around Campus* combine to reach all of the audiences who belong to those listservs — i.e., all members of the campus community who have university e-mail accounts. By employing this approach, the campus community receives from recognized and credible source relevant campus information in a consolidated format.

Targeted Announcements.
In certain cases, there are exceptions that warrant sending individual announcements directly to one or all of the student, faculty and staff listservs. These include:

(1) Emergency messages sent from UNC's Emergency Alert System.

(2) Messages deemed of critical importance from the offices of university president, provost, chief financial officer, UNC Police, university relations, general counsel, human resources, information technology and dean of students.

Approval for sending mass e-mails resides with these offices or their designees, keeping in mind that the preferred and recommended method is through the e-newsletters: the Provost (faculty and student requests) and Chief Financial Officer (employee requests), in consultation with the newsletter's editor. The university may rescind a community member's eligibility to send announcements for non-compliance with this or other university technology policies contained in "UNC Computer, Internet and Electronic Communication Procedures."

(3) This does not affect:

(a) Professors sending e-mail to students enrolled in their classes;

(b) Other listservs that are requested and managed by faculty, staff and students. These listservs use a Web interface to distribute e-mail to addresses on and off campus and can be modified to allow members to send and receive messages.

(c) This also does not affect sending e-mail to department e-mail distribution lists that have either been set up by an employee or by IT on the department's behalf. These lists can be created and managed locally through Outlook or requested through Information Technology so that they appear in the Global Address List. Members of a distribution list are the only ones available to send to these lists.

Guidelines for Submitting *UNC Today*/Ursa Campus Announcements.

(1) Announcements must be directly related to the university.

(2) Campus announcements must be relevant to a large segment of the university community and fall into one of these categories:

(a) **News and Events.**
Examples: Grants received by faculty, staff and students; ground-breaking research; faculty member's recently published books and articles; honors/awards; new programs and facilities; featured speakers on campus; defense of dissertation/oral exams; retirement receptions; and university-sponsored events such as concerts, speakers, performances, workshops, meetings, celebrations, athletics events and festivals.

(b) **Employee.**
Examples: Job openings, policy changes, training opportunities, updates on benefits plans; important deadlines

(c) **Student.**
Examples: Important deadlines (financial aid, registration, graduation, etc.)

(d) **Human-interest stories.**
Examples: A student's unusual job, a professor's out-of-the-ordinary volunteer activities, an employee who is retiring after 30 years at UNC

(3) Announcements must include a contact name, telephone number and e-mail address.

(4) Announcements may not conflict with UNC policies or regulations or

include material contrary to the university's mission and values.

(5) Announcements about commercial or fund-raising activities not associated with the university (e.g., solicitations) or about activities for personal financial gain will not be published.

(6) Announcements must comply with "UNC Computer, Internet and Electronic Communication Procedures, http://www.unco.edu/it/Policies/computingproceduresindex.html .

(7) To request a *UNC Today* announcement, use the form online at http://www.unco.edu/unctoday . Events on the university's online calendar are automatically considered for publication in Campus Announcements. **The submission deadline to be included in the next day's edition is 4 p.m.**

(8) All announcements are subject to editing (see below).

(9) Each campus announcement may run twice per semester. Following are examples:

(a) Event—two weeks in advance and day before event;

(b) Art exhibit—a few days before opening reception and a week before exhibit closes;

(c) Request for nominations—when nominations open and a few days before deadline;

(d) Last-minute meeting notice—day before and day of meeting.

(10) Calendar entries: All university events occurring on campus and sponsored by official campus groups should be entered into the online calendar. From a campus computer, visit. http://www.unco.edu/calendar/calendar.asp. Click 'Submit or edit an event' at the top of the page. Calendar entries will appear online within 24 hours of the time they're entered. Entries will be published in UNC Today and distributed in an e-mail titled 'Next Week on Campus,' which previews the on-campus events for the upcoming week.

Guidelines for Around Campus.

(1) Events published in Around Campus must be sponsored by official university groups.

(2) Events should be submitted to the online calendar to be included in the newsletter and considered as an announcement. From a campus computer, visit http://www.unco.edu/calendar/calendar.asp. Click 'Submit or edit an event' at the top of the page. Calendar entries will appear online within 24 hours of the time they're entered. Entries will be published in Around Campus under the headings, "Today and This Weekend on Campus," and "Next Week on Campus," which previews the on-campus events for the upcoming week.

(3) Announcements are selected by the Dean of Students Office from a list of upcoming campus events and/or pertinent information that's relevant to students.

(4) To submit ideas for spotlight stories, which are feature stories that appear in Around Campus, send an e-mail to newsletters@unco.edu. Examples of potential stories include, but aren't limited to: a student's unusual job or prestigious award or achievement (such as receiving an internship to work at NASA), a college class that has started as a result of student research, or a student's out-of-the-ordinary volunteer activities.

(5) Calendar entries must include a contact name, telephone number and e-mail address.

(6) Calendar entries may not conflict with UNC policies or regulations or include material contrary to the university's mission and values.

(7) Calendar entries about commercial or fund-raising activities not associated with the university (e.g., solicitations) or about activities for personal financial gain will not be published.

(8) Calendar entries must comply with “UNC Computer, Internet and Electronic Communication Procedures,” http://www.unco.edu/it/Policies/computingproceduresindex.html

(9) All entries are subject to editing (see below).

Editing of Announcements.
The Office of University Relations staff will edit announcement and calendar submissions for accuracy, brevity, clarity and suitability. If a submission is better suited to a different communication vehicle, it will be forwarded. Items that are incomplete or inaccurate or do not meet guidelines will be e-mailed back to the submitter with an explanation. Submitters are encouraged to make necessary changes and resubmit the item. The university reserves the right to review, suspend or deny announcement requests for any reason.

UNC Today and *Around Campus* contact: newsletters@unco.edu.

About the Policy.
This policy is part of the “UNC Computer, Internet and Electronic Communication Procedures.” Along with those procedures, it is reviewed periodically by the Information Technology Committee, a university-wide management and advisory committee established to provide communication, collaboration and coordination on issues regarding information technology policy, planning, resource management, standards, procedures and priorities that will develop and enhance the effective use of information technology by faculty, staff and students.

Administrative policies and procedures and student code of conduct are applicable to University system users,
http://www.unco.edu/it/Policies/computingprocedures.html#whatotherapplicable

CONDITIONS OF ADMINISTRATIVE SERVICE

CONDITIONS OF FACULTY SERVICE

CONDITIONS OF PROFESSIONAL SERVICE

CONFLICT OF INTEREST

COPYRIGHT & DIGITAL MILLENIUM COPYRIGHT ACT

GRAMM-LEACH BLILEY ACT

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT

HONOR CODE

INTELLECTUAL PROPERTY

PERSONAL USE OF UNIVERSITY RESOURCES

POLITICAL ACTIVITY

PRIVACY POLICY

PROCUREMENT PROCEDURES

STUDENT CODE OF CONDUCT

TRADEMARK USE

3-9-209 Plan to Combat Unauthorized Distribution of Copyrighted Material.
In accordance with the Higher Education Act of 2008; the University has adopted this Plan to combat unauthorized distribution of copyrighted material through peer-to-peer file sharing. The Plan consists of 4 elements.

3-9-213(1) Technology Based Deterrents.
The University computing infrastructure has the ability to shape the majority of peer-to-peer applications in use today. This same technology can be used to assist with the identification of individuals who may be accessing P2P networks and potentially downloading and uploading copyrighted material. The University will use technologies that provide the ability to identify P2P applications and assist with the shaping of the traffic associated with such applications as appropriate to enhance the effectiveness of the Plan and consistent with preserving the computing infrastructure and University resources.

3-9-213(2) Education.
The University annually distributes an educational publication(s) to the campus community “Cyber- Security Awareness Month” The publication(s) outline the technology behind peer-to peer file sharing, provides examples of

how certain uses of that technology may constitute unauthorized distribution of copyrighted material, and provides information on resources and alternatives for legally obtaining copyrighted material. The publication describes the institution's policies with respect to unauthorized peer-to-peer file sharing and summarizes potential disciplinary actions for violation of the procedure. It also explicitly informs the campus community that unauthorized distribution of copyrighted material, including unauthorized peer-to-peer file sharing, may result in civil and criminal liabilities and summarizes potential civil and criminal penalties. The information is distributed to the campus community annually and posted on the University's website located at http://www.unco.edu/cybersecurity

3-9-213(3) Policies.

The Student Code of Conduct, Section B.12 prohibits violations of federal law or any other conduct that unreasonably interferes with the operations of the University. This provision makes any copyright infringement by a student a violation of University policy. In addition, University Regulation 3-9-208(9) prohibits any use of the University network for unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, movies, and the installation of any copyrighted software for which UNC or the end user does not have an active license. Unauthorized distribution of copyrighted material through peer-to-peer file sharing is explicitly addressed in the University's Peer-to Peer File Sharing Procedure which appears in the University Regulations, Article 9 Information Technology located at http://www.unco.edu/trustees/University_Regulations.pdf

3-9-213(4) Assessment of Plan Effectiveness.

The Assistant Vice President for Information Technology will coordinate a periodic assessment of the effectiveness of this Plan. The assessment shall consist of a review of current legal alternatives for downloading or otherwise acquiring copyrighted material, a review of the University's current technology based deterrents, a review of the University's current educational efforts and a review of disciplinary actions for unauthorized distribution of copyrighted material. The assessment shall set out the criteria used for assessing Plan effectiveness, which may include tools for assessing campus awareness of the risks and consequences of unauthorized distribution of copyrighted material, availability of legal downloading alternatives, statistics on repeat violators and analysis of DMCA violation notices and settlement letters for trends and fluctuations in type and frequency. Based on this assessment, the Assistant Vice President for Information Technology, in consultation with the Office of General Counsel, the Director of Human Resources and the Office of Student Affairs will update this Plan as needed.

3-9-210 Peer-to Peer File Sharing Procedure.

3-9-214(1) Overview.

The University's culture supports sharing knowledge and information in a manner that does not violate copyright law or University policy or regulation. File sharing is the practice of using the internet to make files available for others to download. Peer-to peer (P2P) file sharing applications allow a computer to connect to a P2P network, and once connected, make it possible to download as well as upload files for other users on the network. Campus computer networks are subject to be used to download and distribute copyrighted music, movies, television shows, pictures, games, software, etc. through the use of P2Pfile sharing networks.

While there are files we can legitimately obtain and share, for instance, works of our own creation or works in the public domain, it is against the law and University policy and regulation to download copyrighted materials (such as music, movies, video games, computer software, photographs, etc.) without legal authorization such as purchasing the work or obtaining the copyright holder's permission. Purchasing a work for your own use does not give you legal authorization to further distribute that work.

P2P file sharing poses risks to the University computer network and to the individuals involved. The University of Northern Colorado respects the intellectual property rights of others and expects students, faculty, and staff to do so as well. We also must ensure that the University's network is not put at risk or misused.

3-9-214(2) Risks of Unauthorized Peer-to-Peer File Sharing.

Illegal P2P downloading and distribution of copyrighted material, even if inadvertent, holds the risk of significant penalties beyond sanctions for violation of University policy and regulation. Under federal law, a person found to have infringed upon a copyrighted work may be liable for actual damages and lost profits attributable to the infringement, and statutory damages from $200 up to $150,000. The copyright owner also has the right to permanently enjoin an infringer from further infringing activities, and the infringing copies and equipment used in the infringement can be impounded and destroyed. If a copyright owner hired an attorney to enforce their rights, the infringer of a work may also be liable for the attorney's fees as well as court costs. Finally, criminal penalties may also be assessed against the infringer and could include jail time depending upon the nature of the violation.

Along with the potential for University sanctions for violations of University policy and regulation and legal complications associated with P2P file sharing, the files downloaded or distributed through P2P file sharing can cause harm to individuals, their computers and the computing network and infrastructure. These risks include but are not limited to virus infections, worm infections, Trojan Horses, Spyware, sensitive information leakage, and identity theft.

3-9-214(3) Purpose.

It is the responsibility of all members of the UNC community to use copyrighted materials in a manner that complies with the United States Copyright Law and University policy and regulation. The purpose of this procedure is to combat unauthorized downloading and distribution of copyrighted materials using P2P file sharing and guard against the associated risks.

3-9-214(4) Scope.

This procedure applies to University employees, staff, faculty, students, guests, and all other users of the University’s computing and network resources.

3-9-214(5) Procedure.

Uses of P2P applications on the University network in a manner that infringes copyright or interferes with or poses a risk to the network integrity or security are prohibited by this procedure.

Using P2P applications to download a copyrighted work is deemed to infringe copyright protection if undertaken without legal authorization, which may be obtained through purchasing the work or obtaining the owner's written authorization. Purchasing a work for downloading does not authorize further distribution.

Using P2P applications interferes with or poses a risk to the University network whenever the use places an unusual burden on the network, for instance, when excessive bandwidth is occupied and when potentially unsafe content is downloaded or uploaded. P2P applications may be used for legitimate academic or research purposes or for personal purposes so long as those uses do not violate the law or this procedure.

3-9-214(6) Enforcement.

The University does not routinely monitor its computer network to detect infringement of copyright protected material; however it receives copyright infringement notifications of various kinds from owners of copyright protected material that has allegedly been infringed by University network users.

The Digital Millennium Copyright Act (DMCA) provides copyright owners with a procedure for notifying service providers of alleged infringing activities by their subscribers. The University is generally deemed a service provider under the DMCA. A notice of infringing activity must contain the following elements to be sufficient.

1) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

2) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.

3) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.

4) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.

5) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.

6) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

If the University receives a notice that meets these requirements it will be taken as evidence of a potential violation of this procedure. The copyright owner's notice will be forwarded to the user at the IP address indicated with an indication of actions required to resolve the complaint.

If a P2P use is interfering with or placing the network at risk, the University will send the user a notice of evidence of a potential procedure violation with an indication of actions required to resolve the complaint.

Actions required to resolve a complaint of potential procedure violation may include one of more of the following: 1) requiring that the user immediately cease any prohibited activity, 2) requiring that the user participate in training on the risks of P2P file sharing 3) other action as deemed appropriate to the circumstances.

Failure of the user to comply with any required actions set out in a notice of potential procedure violation, or alternatively, on receiving a notice of potential procedure violation to provide the University with evidence that the use does not violate the law or University policy or regulation, may result in the immediate disconnection of the offending device from the University's computing network or disabling access for the person at the IP address. The University may disconnect an offending device or disable access for the person at the IP address without prior notice if the use is interfering with network operation or placing the network at risk until appropriate actions can be taken. Furthermore, violation of this procedure may result in disciplinary action under appropriate University disciplinary procedures for employees, faculty, staff, and students. Sanctions may include any sanction available under the appropriate disciplinary policy, up to and including dismissal from the University or termination of a user's University computing account. Civil and criminal legal consequences may also result.

3-9-214(7) Alternatives.

The University allows legal downloading on its network so long as the use does not interfere with or pose a risk to the network. Obtain legal downloading resource information at http://www.educause.edu/Resources/Browse/LegalDownloading/33381. These resources may not remain valid over time. It is up to the individual user to check out the legal statue of any music downloading service they might wish to use.