## 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

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 coordeiifc -U 2 7 0 T d 1 hazards such as fire and water damage, or technical failures. Further, each department is responsible for maintaining covered data and information should 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

**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 a 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 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 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, tel1 (e)-3 8%(or)-6 (m)-.57 0 Td(-Tw 0 g )]TJ-0.003l8 <6 (i)-1 (t)

Making announcements through Ursa, *UNC Today* and

(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:

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 — and a few days before1

o Td3 (f)s; 5 ( 3)-6.5 Td (xhi)a1y(f)-5 (e)-8(e)s)[b]0(8 7d 0 Tw(4)-2 0 Td m)-9 (((8Td[(d)-m0 3T(x)[(o)-1us(f)T(x) g(

## 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.

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 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 Infor

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.

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 a) o 0 Td( )T Tj- .003 Tc 0.00Ac9.1 (n)1 ( o1f.003 Tcj- .0004

**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.