Computer Network Security
And Intellectual Property:

A Risk and Resource Guide for Educational Institutions

By D. Frank Vinik, Esq.

Contents

Computer Network Security .................................................................5
Patents and Technology Transfer .........................................................11
Trademarks ..........................................................................................16
Copyright ............................................................................................19
Distance Learning ................................................................................23
Software Creation ..............................................................................27
Exclusively for the use of United Educators member institutions. Not for public distribution.

For an electronic version with active links to the web addresses cited in the footnotes, please e-mail your request to risk@ue.org.
PREFACE TO 2005 REVISED EDITION

United Educators is pleased to offer a revised edition of its popular publication *Intellectual Property and Cyberspace: A Risk and Resource Guide for Educational Institutions*. As reflected by the guide’s new title, the first section now focuses more on computer network security than cyberspace. Its revised content provides detailed risk management measures and resources for the prevention, detection, and mitigation of computer network breaches. While much of the content of the first edition remains relevant, its numerous web links have been updated, and new links to more current resources have been added.

The author would like to thank the following individuals for reviewing drafts of the first edition of this guide and providing valuable comments and suggestions: Beverly Costello, former risk manager, Yale University; Thomas R. Henneberry, former assistant director for industrial agreements, Office of Sponsored Programs, Massachusetts Institute of Technology; and Margareth Schubert, associate general counsel, Loyola University of Chicago. The author also appreciates the invaluable assistance of Bjorn Wickstrom of United Educators in preparing the revised edition.
INTRODUCTION

Rapid advances in information technology and intellectual property have transformed education for the good. Professors can teach students thousands of miles away. Students at small liberal arts colleges can obtain research materials over the Internet that are unavailable in their libraries. Universities have reaped millions of dollars in royalties from commercialization of discoveries by campus researchers.

But these advances in information technology and intellectual property also bring disadvantages. The same connectivity that provides the benefits of technology also creates dangers. With the touch of a button, a student can send a harassing e-mail to thousands of his peers. A hacker or disgruntled employee can access confidential records or destroy valuable data that would take months to re-create. And that researcher’s valuable discovery can embroil a campus in expensive patent litigation.

Although United Educators has not yet seen many claims in these areas, intellectual property and computer network security present major risk management challenges for education. Numerous institutions have failed to institute risk management procedures and have not updated their policies since the 1980s. Because these risks involve disparate areas of a campus, they require a coordinated effort. Consequently, we believe that a commitment to manage these risks needs to come from the top: the president, the board, and senior administrators.

The first step to systematic risk management is the development of sound policies. But policies alone are not enough. Institutions also need to develop procedures to implement, monitor, and enforce good practices. In addition to devoting resources to new computer systems, distance learning initiatives, and research programs, institutions must spend time and effort managing the risks that these innovations can pose.

This guide covers six key areas: (1) computer network security, (2) patents and technology transfer, (3) trademarks, (4) copyright, (5) distance learning, and (6) software creation. In each area, the guide lists some of the common risks that United Educators has identified in handling claims and reviewing the literature; outlines suggested risk management measures to mitigate liability and protect students, faculty, and employees; and provides resources for developing policies, including numerous web links to sample policies. We hope this guide helps your institution position itself not only to benefit from the new advances but also to manage the new risks.
I. RISKS INVOLVING COMPUTER NETWORK SECURITY

A. Overview

American educational institutions provide their students and employees with access to high speed Internet connections and some of the most powerful computer networks in the world. Researchers can resolve complex technological problems, students can create their own websites, and the entire academic community can access the World Wide Web. Unfortunately, the high power and relative openness of these systems make them targets for wrongdoers. The challenge is to strike a balance between the security needs of the system and the need to maintain accessibility for users who play by the rules.

B. Common Risks

1. A student suffers identity theft after a hacker obtains her Social Security number and other confidential records due to lax security.
2. A computer virus destroys valuable records and scientific data.
3. A natural disaster destroys computer records that were not backed up.
4. A laptop computer is stolen that contains confidential institutional information that is not encrypted.
5. A faculty member opens an e-mail attachment containing a “Trojan horse” that infiltrates the institutional network.
6. Students receive an e-mail that directs them to a phony institutional website asking them to provide personal information.
7. A student steals the password to another student’s e-mail account and uses the account to send harassing e-mails.
8. An administrator browses websites that attach adware to her computer and record every keystroke she enters.
9. An institution needs to terminate an information technology employee but fears that his knowledge of the system’s weaknesses will allow him to engage in sabotage.
10. An outside hacker breaks into the university system and uses its power to engage in attacks on other systems.

C. Risk Management Measures

1. Securing the System

a. Focus on education and awareness of users. Research has shown that inadequate education is the primary cause of computer incidents.

b. Establish stringent job requirements for IT personnel and provide them with clear procedures to prevent careless mistakes.

c. Use automated tools for detection of network intruders and rapid institutional response.
d. Identify categories of sensitive information stored electronically that needs special protection. These include: medical records, personnel files, student records, donor records, institutional financial data, credit card information, social security numbers, legal advice, and research. In consultation with your IT staff, develop strong security for these records.

e. Make security an ongoing priority. Many system administrators spend so much time making sure the system is running that they overlook security concerns.

f. Find ways to involve auditors and risk managers so that computer security is considered in assessing overall risks to the institution.

g. Keep abreast of the latest weapons used by hackers. Numerous organizations, both publicly and privately funded, report on methods of recent attacks and how to improve security, including the following:
   The System Administration, Networking and Security Institute (SANS Institute)\(^1\)
   The Computer Emergency Response Team Coordination Center (CERT/CC)\(^2\)
   United States Computer Emergency Readiness Team (US-CERT)\(^3\)
   Center for Education and Research in Information Assurance and Security (CERIAS)\(^4\)
   Computer Incident Advisory Capability (CIAC)\(^5\)

h. Install patches for common vulnerabilities as soon as the patches become available from reliable sources such as the organizations listed above.

i. Establish firewalls so that the disabling of one part of the computer system does not affect the entire campus, but be careful not to over-rely on firewalls as your sole security measure.

j. Encrypt all confidential information contained on laptop computers so that the information cannot be easily accessed if the laptop is lost or stolen.

k. Change all default passwords that come from the manufacturer. Many hackers get in because users never change the common defaults.

l. Require users with special privileges to periodically change their passwords by making their passwords automatically expire every few months. Many hackers infiltrate a system for years because their stolen passwords never change.

\(^1\) [http://www.sans.org/top20/](http://www.sans.org/top20/)
\(^2\) [http://www.cert.org](http://www.cert.org)
\(^3\) [www.us-cert.gov](http://www.us-cert.gov)
\(^4\) [http://www.cerias.purdue.edu](http://www.cerias.purdue.edu)
\(^5\) [www.ciac.org/ciac/index.html](http://www.ciac.org/ciac/index.html)
m. Search the system for “backdoor passwords” and eliminate them so that it will be more difficult for hackers to bypass regular security protections.

2. Educating Users

a. Require that users understand the institution’s policies and the basics of the computer system before they are allowed access to the institutional network.

b. Tell users up front, both in writing and orally, under what circumstances the institution may view their e-mails or stored data.

c. Outline the various penalties for inappropriate uses, including but not limited to revocation of access, institutional discipline, and personal criminal liability.

d. Require employees to perform multiple generations of data backup, and store backup materials in places where they can be retrieved in case of a natural disaster.

e. Require employees to log off their computers at the end of the day to protect the confidentiality of information accessible from that terminal.

f. Check for abnormally high traffic on personal websites of students and employees that may indicate an improper use.

3. Incident Handling and Response

a. Develop broad-based computer emergency response teams that include IT personnel, legal counsel, external relations, law enforcement, and other constituencies needed to provide a comprehensive institutional response to incidents.

b. Ensure constant communication between members of the computer emergency response team so that the institution can assess IT risks as a whole and create institutionwide solutions.

c. Establish clear procedures for IT personnel to follow whenever incidents occur and be sure to educate IT personnel continuously on changes in procedures.

d. Develop a system for classifying the seriousness of incidents.

e. Give your IT department authority to quarantine contaminated computers if they threaten the security of the system.

f. Conduct periodic meetings of the emergency response team to identify potential weaknesses in the system.
After all serious incidents, engage in postmortems to determine lessons learned and make necessary changes to avoid similar incidents in the future.

D. Components of a Computer-Use Policy

A recent study of the computer-use policies at 71 state universities in all 50 states concluded that there is little agreement about what a policy should contain. See “Computer Use Policies at Major U.S. Universities” by Susan Athey. At least half the policies discussed the following three issues:

- Harassing e-mail.
- Commercial use.
- Software copyright.

Other issues discussed in at least one-third of the policies include:

- Copyright.
- Interfering with normal operations.
- Accessing other programs or data.
- Sharing accounts.
- Worms and viruses.
- Personal financial gain.
- Unauthorized access to systems.
- Chain letters.

The “Checklist for Drafting Electronic Information Policies” is a valuable resource in preparing a computer-use policy. Prepared by Paula Kaufman of the University of Tennessee and Gerald Lowell of the University of California, San Diego in conjunction with the Association of Research Libraries, the checklist covers the following topics: access; e-mail; websites and web publishing; network use; coordination on campus; archiving; due process; definitions; and implementation and review.

It is also important that computer-use policies cross-reference and incorporate other institutional policies that may apply, such as harassment and discipline policies.

E. Sample Computer-Use Policies

1. University of Virginia

---

7 http://www.arl.org/newsltr/196/checklist.html
The University of Virginia has adopted some of the most extensive policies on responsible computing. It has adopted both a *Handbook for Students* and a *Handbook for Faculty and Staff*. Few institutions have the resources to establish policies as comprehensive as those at the University of Virginia. But these policies are an excellent starting point for gathering ideas and deciding on your institution’s approach.

2. **The SANS Institute (SysAdmin, Audit, Network, Security)**

The SANS Institute is the world’s largest provider of information security training and certification. One of its most helpful resources is a series of templates for policies on more than 20 topics ranging from acceptable encryption to wireless communication. The templates are provided in both Word and PDF formats.

F. **Sample Computer-incident Handling Policies**

1. **Educause**

EDUCAUSE is a nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology. It provides excellent resources and hosts numerous conferences on IT issues in higher education. It has developed a good overview of incident handling and response that covers all of the major topics and contains links to sample policies at select educational institutions.

2. **Rochester Institute of Technology**

Rochester Institute of Technology has developed a detailed set of standards for handling computer incidents. The standards contain links to other relevant policies at the university. In addition, the university has created the *Plain English Guide to the Computer Incident Handling Standard* and a list of 20 steps users can take to protect their information.

- Information Security Standards
- *Plain English Guide to the Computer Incident Handling Standard*
- Top Twenty Things to Do for Protecting Your Personal Information

---

10 [http://www.sans.org/resources/policies/#template](http://www.sans.org/resources/policies/#template)
11 [http://www.educause.edu/content.asp?page_id=1269&bhcp=1](http://www.educause.edu/content.asp?page_id=1269&bhcp=1)
12 [http://security.rit.edu/standards/](http://security.rit.edu/standards/)
13 [http://security.rit.edu/articles/desktopstandard-plain_english.pdf](http://security.rit.edu/articles/desktopstandard-plain_english.pdf)
14 [http://security.rit.edu/articles/toptwenty.pdf](http://security.rit.edu/articles/toptwenty.pdf)
3. Southern Methodist University\textsuperscript{15}

Southern Methodist University has developed a detailed set of incident handling procedures for IT personnel that identifies whom to contact in specific situations, explains what information to keep in logs, outlines what information to release, provides guidance on how to return to normal operating mode, and requires a postmortem of each incident.

4. Carnegie Mellon Software Engineering Institute\textsuperscript{16}


5. The University of Iowa\textsuperscript{17}

The University of Iowa has created a computer emergency response team that categorizes incidents based on their level of seriousness and coordinates contacts with law enforcement, legal counsel, and university external relations. The institutional policy includes team responsibilities, qualifications for joining the response team, and e-mail code descriptions to facilitate communication within the team.

\textsuperscript{15} http://www.smu.edu/its/is/incident_hand.asp
\textsuperscript{16} http://www.cert.org/archive/pdf/csirt-handbook.pdf
\textsuperscript{17} http://cio.uiowa.edu/itsecurity/resources/I-CERT.htm
II. PATENTS AND TECHNOLOGY TRANSFER

A. Overview

The Bayh-Dole Act of 1980 revolutionized technology transfer in the United States. Congress passed the act to encourage educational institutions to find commercial applications for basic research sponsored by the federal government. The law gives educational institutions the right to patent basic research discoveries supported by federal funds, license the technology to private entities, and receive all the royalties. The financial rewards to some institutions stagger the imagination. The University of Minnesota received $300 million for an AIDS treatment, the University of California received $200 million for discoveries related to human growth hormones, and Florida State University has received more than $350 million for a cancer drug developed from a research breakthrough on its campus.

Unquestionably, technology transfer offers the potential of huge rewards. But consider this statement by Louis Berneman, former president of the Association of University Technology Managers:

Any university thinking about getting into technology transfer because they see . . . $200 million is playing a fool’s game. They’d get a better return on opening up the McDonald’s franchise on campus than investing in patent licensing, if all they are interested in is a financial return.18

United Educators believes that the rush to cash in on these rewards has made some researchers and institutions ignore the risks. The challenge for institutions is to manage the risks without stifling the entrepreneurial spirit necessary for effective technology transfer programs.

B. Common Risks

Based on United Educators’ experience in handling claims and review of the literature in this area, we have identified 10 common risks of technology transfer:

1. Competitors use patent litigation as a business weapon.

Company A purchases a nonexclusive license to a university patent. Company B wants its own license on favorable terms and wants to tie up A, its competitor. To obtain leverage, B sues both A and the university, alleging that the patent was improperly obtained and should be invalidated. (An actual claim involving a UE member follows this scenario.)

2. *Academic collaborators cease to collaborate.*\(^{19}\)

A researcher makes a scientific breakthrough and confirms the findings at his collaborator’s lab at another university. There is no written agreement between the researchers. The two universities file competing patent applications claiming ownership to the breakthrough. After extensive litigation, the universities agree to assume their own legal costs.

3. *Institution claims rights to ideas of researcher who left.*

A researcher leaves institution 1 for institution 2. At institution 2, the researcher finalizes a technology that institution 2 patents and licenses. Institution 1 claims that key ideas in developing the technology came from work done by the researcher on its campus, and it deserves a share of the royalties. (An actual claim involving a UE member follows this scenario.)

4. *Researcher prematurely discloses research results.*\(^{20}\)

A researcher publishes the results of a study funded by a biotechnology company. The study showed that the company’s drug was not effective in clinical trials. The company sues the university and researcher for $10 million.

5. *University and licensee disagree over royalty amounts.*

A university negotiates royalties in a licensing agreement as a percentage of revenues or profits but suspects that the licensee is artificially deflating revenue or profit figures to decrease its royalty payments.

6. *Technology turns out to be a gift horse.*\(^{21}\)

A company donates a patent to a university to obtain a tax write-off, but it turns out that the legal costs of maintaining worldwide patent rights exceed the value of the patent.

7. *Patent is unenforceable due to lack of specificity.*\(^{22}\)

A university specifies technology in a patent application according to prevailing scientific standards. The university sues a pharmaceutical company for using the technology without a license. The courts rule that the university failed to adequately describe the

---


\(^{22}\) See, e.g., *The Regents of the University of California v. Eli Lilly and Company*, 119 F.3d 1559 (Fed. Cir. 1997).
technology in its patent application according to new legal standards. As a result, the university incurs $12 million in legal fees and receives no royalties.

8. The exclusive licensee fails to market the technology.

A university provides an exclusive license to Corporation X to develop patented technology. The university later learns that Corporation X has decided to stop developing the technology but will not give up the exclusive license because it does not want a competitor to develop and market the technology.


A university manufactures a genetically engineered crop in its labs in collaboration with a commercial partner. A consumer of the product suffers health problems and sues both the university and its commercial partner alleging defective manufacture or design of the genetically engineered crop.

10. Researcher ignores conflicts of interest.

A researcher working with a commercial partner tells her campus colleagues confidential information about the status of product development. The Securities and Exchange Commission (SEC) starts an investigation, which leads to adverse publicity for the institution and potential criminal and civil charges against the researcher and her colleagues.

C. Risk Management Measures

1. Find out what patenting and licensing activity is occurring on your campus. Many smaller institutions without a heavy emphasis on research may be surprised about the extent of such activity.

2. Develop a risk management task force that includes researchers, business officers, legal counsel, and any other players in technology licensing.

3. Charge back to the technology licensing office the litigation costs arising out of patent licenses in order to motivate that office to weigh both the risks and benefits of licensing agreements.

4. Develop formulas for allocating royalties between the institution and the researcher who makes a discovery.

5. In a licensing agreement, require the licensee to pay the costs of defending patent litigation, and deduct a percentage of litigation costs out of royalties.

6. Require academic collaborators at different institutions to enter into a written agreement on ownership of inventions and resulting royalties. The requirement
should be stated as an institutional responsibility, and the entities should sign a contract covering these issues.

7. Require new researchers to negotiate who owns what with their prior institutions. Upon employment at your institution, require them to sign a statement that they are not bringing intellectual property with them that belongs to others. In addition, all new employees and visiting scholars and scientists (especially international visitors) from other institutions should sign agreements assigning their intellectual property rights to the institution.

8. Require researchers to spell out publication rights and privacy expectations with commercial sponsors or collaborators.

9. Include audit clauses in all licensing agreements. The article “Protecting Your Royalty Payments Using Audit Clauses in License Agreements,”23 by Vincent J. Kiernan, offers advice on structuring audit clauses.

10. Include a diligence clause in all exclusive licenses that allows the institution to terminate the license if the licensee does not make substantial efforts to develop the patented technology.

11. Work with your development office to establish guidelines for accepting patents. Ask the hard questions:
   a. Why is the donor giving away these patents instead of developing or selling them?
   b. What will be the legal costs of maintaining each patent internationally?
   c. Do these particular patents fit the institution’s research expertise?
   d. Will the donor share necessary know-how and technical assistance?

12. Encourage researchers to work with patent attorneys to predict ways that potential licensees may try to circumvent the patent and avoid paying royalties.

13. Include conflict of interest policies in either the patent agreement or a separate agreement.

14. Develop a user-friendly handbook to guide faculty through the technology transfer process.24

---

23 [http://www.autm.net/pubs/journal/97/3-97.html](http://www.autm.net/pubs/journal/97/3-97.html)
D. Sample Policies

Institutions need to establish policies on contracting and intellectual property that designate authority within the institution for each area. In addition, institutions need standardized policies that outline which requirements are absolute (such as indemnification) and which requirements can be altered in exchange for substantial consideration.

1. University of Vermont\textsuperscript{25}

This policy divides inventions into three categories and establishes separate rules for each category. Type A inventions are subject to an agreement between the university and a sponsor. Type B inventions are not subject to a sponsor agreement but involve the use of university time, funds, or other resources. Type C inventions are not subject to a sponsored agreement and do not involve the use of university resources.

2. George Washington University\textsuperscript{26}

This policy establishes good definitions and thorough procedures for disclosing inventions, evaluating inventions, determining patent rights, distributing royalties, resolving disputes, and reviewing the policy periodically.

3. Texas A&M University\textsuperscript{27}

This policy provides an excellent series of steps for its implementation and for distribution of income from patented or copyrighted works.

4. Rice University\textsuperscript{28}

This policy has a unique income distribution formula and is one of the few patent policies that establish procedures for multi-institution research efforts.

\textsuperscript{25} http://www.uvm.edu/~uvmppg/ppg/general_html/patent.htm
\textsuperscript{26} http://www.gwu.edu/~avprgs/Patpolicy.htm
\textsuperscript{27} http://sago.tamu.edu/policy/17-02-01.htm
\textsuperscript{28} http://www.professor.rice.edu/professor/Patent_and_Software_Policies.asp?SnID=723114320
III. TRADEMARKS

A. Overview

An institution’s trademarks are some of its most important assets. They may include the institutional name, seal, mascot, athletic team names, slogans, and familiar campus landmarks. Campus affiliated entities are typically allowed to use institutional trademarks. However, any commercial entity or separately incorporated entity should be required to obtain written permission or a license to use institutional trademarks. Many institutions view their trademarks as their “brand” and devote considerable effort to obtaining royalties from companies benefiting from the brand. It is estimated that over 400 American colleges and universities have established trademark licensing programs and earn more than $2 billion a year in licensing fees.

B. Common Risks

1. An apparel manufacturer deprives the institution of royalties by using institutional trademarks on clothing without permission.

2. An apparel manufacturer with a license to use institutional marks engages in poor employment practices, tarnishing the institution’s image.

3. A faculty member establishes an independent consulting organization that incorporates the institutional name, even though his consulting work does not involve his university duties (for example, Harvard Business Consulting).

4. A company with no affiliation to a university uses the institution’s name, in the hope that customers will associate the quality of the university with its products (for example, Stanford Microdevices).

5. An alumni group unaffiliated with a school uses its name and trademarks to raise money.

6. A pornographic website uses the institution’s name in its domain name to lure customers (for example, Michigan.com instead of Michigan.edu).

7. An institution fails to protect its trademarks from infringement for so long that the marks become diluted and lose their legal protection.

C. Risk Management Measures

1. Decide what entities on your campus are responsible for monitoring trademarks.
2. Search the website of the U.S. Patent and Trademark Office to determine which trademarks your institution has registered.  

3. Define and register all unregistered marks with the U.S. Patent and Trademark Office. 

4. Determine what groups and companies are using the institutional names and trademarks. Be sure to look at Internet companies. In addition, use your alumni to help spot infringers. Alumni are often the best source of information.

5. Require all affiliated and outside entities, both nonprofit and for profit, to obtain written permission to use the institution’s trademarks.

6. Develop a trademark licensing program.

7. Establish a code of conduct for employment and marketing practices of licensees.

8. Establish guidelines for the appropriate use of institutional trademarks by both internal and external entities.

9. Take action against unauthorized or inappropriate users of institutional trademarks.

D. Useful Resources


2. Basic Facts About Registering a Trademark, by the U.S. Patent and Trademark Office. 


E. Sample Policies

1. University of California at Berkeley
UC Berkeley has established a separate Office of Marketing and Management of Trademarks with a full-time staff. The office’s website provides a wealth of information including frequently asked questions and one of the country’s first codes of conduct.

2. Iowa State University

The Iowa State University policy has three parts. The Trademark Management Policy provides an overview of why the policy exists and its basic components.\(^{35}\) The Guidelines for Internal Use of Iowa State University’s Marks address legal issues, design standards, and approval guidelines for members of the Iowa State community desiring to use its trademarks.\(^{36}\) The Iowa State University Research Foundation’s Licensing Program Guidelines for the Use of Iowa State University's Marks discusses licensing of users and suppliers, royalties, licensing and approval procedures, product standards, and standards for nonproduct use.\(^{37}\)

\(^{35}\) [www.iastate.edu/~isurf/trade/trademng.html](http://www.iastate.edu/~isurf/trade/trademng.html)

\(^{36}\) [http://www.iastate.edu/~isurf/trade/internguides.html](http://www.iastate.edu/~isurf/trade/internguides.html)

\(^{37}\) [http://www.public.iastate.edu/~isurf/trade/tmguides.html](http://www.public.iastate.edu/~isurf/trade/tmguides.html)
IV. COPYRIGHT

A. Overview

United Educators has not seen significant litigation involving copyright violations at educational institutions. Nevertheless, the sheer volume of copyrighted materials available through educational institutions makes copyright infringement a concern. Furthermore, as information ranging from music to computer software has become digitized, it is far easier for individuals to download vast quantities of copyrighted material. Some institutions have created one policy addressing all copyright issues, while others have treated copyrighted computer software separately. This section includes examples of both types of policies.

B. Common Risks

1. A faculty member creates for his classes course packs that violate federal copyright law by copying entire articles and multiple chapters of books.

2. A student photocopies an entire book in the library because it is less expensive than purchasing the book.

3. The recording industry threatens to sue the institution because students are pirating copyrighted music using the institution’s high speed Internet access.

4. An outside consultant develops a website for the institution that violates copyright law by improperly including digitized images taken from other sources.

5. A faculty member and a commercial note taker wage a protracted legal battle over who owns the rights to the notes from a course.

6. A disgruntled former employee informs a software vendor that several university departments are sharing its software without a sufficient number of licenses.

7. A student uses university hardware to copy commercial software.

8. An employee takes university software home and installs it on her home computer.

9. A student or faculty member inserts copyrighted materials into a website developed using institutional resources.

C. Risk Management Measures

1. Educate members of the campus community about copyright laws and appropriate fair uses.
The Copyright Crash Course of the University of Texas System\textsuperscript{38} is an excellent education initiative. The crash course is easy to use and includes hyperlinks covering a wide variety of topics ranging from faculty lecture notes to music file sharing. A separate crash course tutorial is available to the general public and uses graphics, text, music, and voice to work through common hypothetical situations. At the end of the tutorial, users can take a 12-question test and receive a certificate if they answer the questions correctly. The Ask a Lawyer feature allows Texas system employees to e-mail in-house attorneys with copyright questions.

Another excellent education initiative is the Copyright Management Center\textsuperscript{39} of Indiana University-Purdue University at Indianapolis. It offers links to articles and resources. The section on fair use includes a helpful checklist on the fair use of copyrighted material.

2. Place signage next to every copy machine on campus with the following text:

   Notice: The copyright law of the United States (Title 17 U.S. Code) governs the making of photocopies or other reproductions of copyrighted material. The person using this equipment is liable for any infringement.

3. Reserve materials in the library should be marked with the statement “NOTICE: This material may be protected by copyright law (Title 17 U.S. Code).” In addition, terminate access to reserve materials for a class once the class has ended.

4. Do not include multiple chapters of a book or multiple articles from a journal issue in photocopied course packs. The course packs need appropriate citations and attributions to sources. In addition, they should not be sold to students at a profit (for example, by an outside copy center).

5. Include the institution’s policy on copyrights in class syllabi.

6. Require students and faculty to sign statements agreeing to abide by copyright law and license requirements as a prerequisite for using software purchased by the institution.

7. Review contracts with outside vendors that create websites for the institution to determine whether the vendor or institution is responsible for copyright violations.

8. Mandate that individuals who use institutional resources to develop websites are solely responsible for copyright violations within those sites.

\textsuperscript{38} www.utsystem.edu/OGC/IntellectualProperty/cprtindx.htm
\textsuperscript{39} http://copyright.iupui.edu
9. Keep notebooks, either at a central or departmental level, containing copies of software licenses and shareware receipts. Periodically review the licenses in case the institution is audited by a software vendor.

D. Components of a Policy

Consider including these elements in your copyright policy:

1. A basic overview of copyright protection
2. Discussion of the fair use doctrine
3. When to seek permission from the owner
4. Photocopying materials
5. Use of materials in course packs
6. Audiovisual works
7. Audio recordings of music and voice
8. Material from the Internet including digitized images and text
9. Examples of situations in which copying software is and is not permissible
10. Institutional and legal sanctions for policy violation
11. Responsibility for ensuring compliance
12. Answers to frequently asked questions

E. Sample Policies

1. General copyright policies

The CopyOwn website operated by the University of Maryland has links to dozens of copyright policies at various institutions. Some good models include:

a. Wellesley College

This policy provides a good explanation of copyright law and numerous questions and answers that apply the law to common situations at an educational institution.

b. Dartmouth College

This policy provides excellent guidance on fair use in the areas of document reproduction, databases, CD-ROMs, performances of dramatic and nondramatic works, music, and audiovisual works.

2. Software use policies

a. University of Florida

http://www.inform.umd.edu/copyown
http://www.wellesley.edu/Library/copyright.html
http://www.dartmouth.edu/copyright/
http://pirate.ifas.ufl.edu/INDEX.HTML
The University of Florida has developed one of the most detailed and comprehensive software use policies in the country. It includes guidelines, resources, and training materials.

b. University of Illinois\textsuperscript{44}

This policy uses a question-and-answer format to educate the campus community on appropriate uses. It also outlines the implementation procedures for the university’s policy on software piracy.

\textsuperscript{44} \url{http://www.uic.edu/depts/accc/newsletter/adn30/piracy.html}
V. DISTANCE LEARNING

A. Overview

Distance learning is one of the fastest growing areas of higher education. It provides opportunities to reach new students and the potential to attract new revenues. Unfortunately, many institutions are proceeding full steam ahead with distance learning initiatives without addressing the most fundamental question in this area: Who owns what? Traditionally, a faculty member lectured from notes. Without a faculty member, there was no course. But what happens when lectures are recorded on videotape? What happens when faculty use institutional technical resources to develop learning tools?

B. Common Risks

1. A faculty member videotapes his lectures at your institution and later sells them to a for-profit distance learning company.

2. A faculty member creates a distance learning course for your institution. She demands royalties for use of the course in semesters when she is not teaching it.

3. A faculty member asks for teaching credit whenever a distance learning course that he created is offered, even if he has no involvement in that particular offering.

4. A faculty member obtains technical assistance from an outside vendor in creating a distance learning course and then seeks reimbursement.

5. A faculty member who developed a distance learning course denies the institution permission to modify it at a later date.

6. A faculty member who developed a successful online course leaves the institution, taking the software with her.

D. Risk Management Measures

1. Going forward

The most important step for managing distance learning risks is developing clear guidelines on who owns what and when faculty may provide services to other institutions. This process involves negotiation over very sensitive issues. The rights can be held entirely by the institution or by the creator, or they can be shared. Issues sometimes overlooked include:

- The right to make subsequent revisions with or without the other party’s consent.
- The right to use the materials without the involvement of the other party.
Once the guidelines are adopted, the institution should notify all faculty in writing and require faculty to sign a written agreement before engaging in future distance learning endeavors.

2. Existing Distance Learning Initiatives

What if faculty members are already engaging in distance learning activities and no agreements were ever worked out in advance? This situation is especially sensitive, and administrators may be tempted to ignore the matter, knowing that faculty may perceive any attempt to regulate the process as a change in the rules. Nevertheless, we believe it would be wise for the institution to negotiate agreements with faculty now rather than allowing misunderstandings to develop into litigation down the road.

E. Developing a Distance Learning Policy

Each institution must develop a policy to fit its particular needs and situation. Some institutions, such as the University of Texas System, incorporate distance learning and all other policies into one omnibus policy. Others create separate policies. On the one hand, distance learning policies that grant ownership of everything to the institution may lack incentives for faculty to devote time to distance learning initiatives. On the other hand, a policy that grants everything to the faculty may prevent the institution from obtaining revenues necessary to recoup the costs of technical assistance. Fortunately, there are numerous articles and sample policies that can help you develop and refine a policy to fit your institution’s needs.

1. Components of a policy

Although this is not an exhaustive list, we recommend that an institution’s distance learning policy address the following issues:

a. Criteria for when faculty members own coursework

b. Criteria for when the institution owns courses

c. A clear description of the parties’ respective rights to make subsequent modifications and to use the course without approval from the other party

d. Formulas for allocating royalties

e. Conflict of interest provisions discussing when faculty members may prepare courses for outside vendors

f. Provisions for licensing of coursework

---

45 http://www.utsystem.edu/ogc/intellectualproperty/polguide.htm
2. Articles on developing a policy

“Developing a Distance Education Policy for 21st Century Learning”

This briefing paper, published by the American Council on Education in March 2000, provides an excellent roadmap for developing a policy. Its seven sections examine: intellectual property, ownership of distance education courses, faculty issues, student issues, limiting liability, commercialization, and teaching beyond state and international borders.


This short article by one of the leading experts on copyright law in higher education covers the basic issues a university should consider in developing a policy.

F. Sample Policies and Other Resources

1. University of North Texas

The University of North Texas policy contains incentives for faculty to create distance learning materials. The policy identifies the following five types of work: totally faculty or staff generated, minimal university resources provided, substantial university resources provided, work made for hire, and faculty member uses own work as part of course offering. The policy contains examples under each category. In addition, the policy provides downloadable agreement templates for the first four categories in Microsoft Word format.

2. Indiana University

This institution provides a good sample agreement between a university and a faculty member for creation of distance learning materials.

3. Technology, Education and Copyright Harmonization Act (TEACH ACT)

In 2002, Congress passed the TEACH Act, which provides guidance on the use of copyrighted materials in distance education. Indiana University professor Kenneth Crews developed an excellent summary of the law and also prepared a helpful set of FAQ’s.

---

47 Journal of College & University Law, Vol. 27, No. 1, Summer 2000, p. 5
49 http://www.copyright.iupui.edu/dl_agreement.htm
50 http://copyright.iupui.edu/teach_summary.htm
51 http://www.ala.org/ala/washoff/WOissues/copyrightb/distanceed/teachfaq.htm
4. AAUP Guidelines\textsuperscript{52}

Distance education guidelines from the American Association of University Professors emphasize the faculty role in course development and control.

\textsuperscript{52} http://www.aaup.org/Issues/DistanceEd/Archives/speccmt/deguide.htm
VI. SOFTWARE CREATION

A. Overview

Computer software is unique in that it can be both patented and copyrighted. Consequently, some institutions treat computer software creation as a separate category. As computer programming becomes easier, more employees at educational institutions are developing custom software for teaching, research, or administrative functions. Sometimes, the programmers recognize that the program itself, or the knowledge they gained in creating the program, has commercial applications with value to those outside their particular institution. The difficult question then becomes who owns the rights to products that employees develop with institutional resources or with know-how they acquired on the job.

B. Common Risks

1. An employee in the registrar’s office develops software for the institution and then sells the rights to the software to a commercial vendor.

2. A university employee uses university computers and know-how gained from developing university software to create software for commercial use.

3. A professor develops software as part of his research with the goal of later selling that software to commercial entities and taking all the profits.

4. A student develops valuable software using the college’s resources and ideas he learned from working with a professor.

C. Risk Management Measures

As with distance learning, the most important step in risk management of software creation is developing clear guidelines as to who owns what and how the proceeds from any commercial successes will be shared between the institution and the software developer. The institution should ensure that all faculty, students, and staff are aware of the policy so that they have the same expectations as the institution and can still take advantage of the institution’s resources. This can be particularly important with students who may become major future donors to the institution if they believe the institution helped them develop a product.

D. Components of a Policy

Check your policies on software creation against this list of useful elements:

1. Methods for disclosure of software invention
2. Discussion of rights to ownership
3. Copyright of software
4. Patenting of software
5. Distribution of income

E. Sample Policies

1. University of Texas System – Administrative Policy Regarding Disclosure, Distribution and Licensing of Software\(^5\)\(^3\)

This comprehensive and detailed policy begins with the premise that some software inventions should be treated differently from other types of patentable inventions, and it establishes guidelines for when software should receive different treatment.

2. Rice University – Patent and Software Policies\(^5\)\(^4\)

This policy acknowledges that software is different from other patentable inventions by including software in a separate portion of the patent policy.

\(^{5}3\) [http://www.utsystem.edu/ogc/intellectualproperty/swadmpol.htm](http://www.utsystem.edu/ogc/intellectualproperty/swadmpol.htm)  
\(^{5}4\) [http://professor.rice.edu/professor/Patent_and_Software_Policies.asp](http://professor.rice.edu/professor/Patent_and_Software_Policies.asp)
CONCLUSION

The array of risks presented in this guide may seem daunting. They are multifaceted and changing rapidly, and they affect disparate areas of campus. Do not succumb to the temptation to ignore the risks and hope they will go away. If anything, these risks will increase over time as educational institutions become more dependent on information technology and assume a larger role in creating technology for commercial applications.

We believe the primary challenge for risk management is to reach all of the affected constituencies on campus. An institution needs to identify and prioritize the risks it faces. In evaluating them, consider both monetary and non-monetary costs such as campus disruption, negative publicity, and breaches of trust within the campus community. Build broad-based task forces to tackle problems by involving experts on each risk as well as people with an overview of your institution and its mission.

Effective management of computer network security and intellectual property risks requires a commitment to devote resources to anticipating problems and planning for things that can go wrong. Technology moves at such a dizzying pace that most people are just trying to keep up with their day-to-day tasks. Researchers race to make the discovery first. Computer systems administrators try to keep the system running. However, failure to look beyond day-to-day tasks will hurt the institution in the long run. We hope this resource increases awareness of the computer security and intellectual property risks facing your institution and guides you to the tools to manage those risks.