DOCUMENT RESUME

ED 401 904 IR 056 147

AUTHOR	Leung, Shirley; Bisom, Diane
TITLE	Information Technology Policies. SPEC Kit 218.
INSTITUTION	Association of Research Libraries, Washington, D.C.
REPORT NO	ISSN-0160-3582
PUB DATE	Oct 96
NOTE	161p.
AVAILABLE FROM	Association of Research Libraries, Office of Management Services, 21 Dupont Circle N.W., Washington, DC 20036.
PUB TYPE	Reports - Research/Technical (143)
EDRS PRICE	MF01/PC07 Plus Postage.
DESCRIPTORS	Academic Libraries; Access to Information; Fair Use (Copyrights); Guidelines; Higher Education; *Information Policy; *Information Technology; Library Development; *Library Policy; *Library Role; *Library Surveys; Users (Information)
IDENTIFIERS	Association of Research Libraries

ABSTRACT

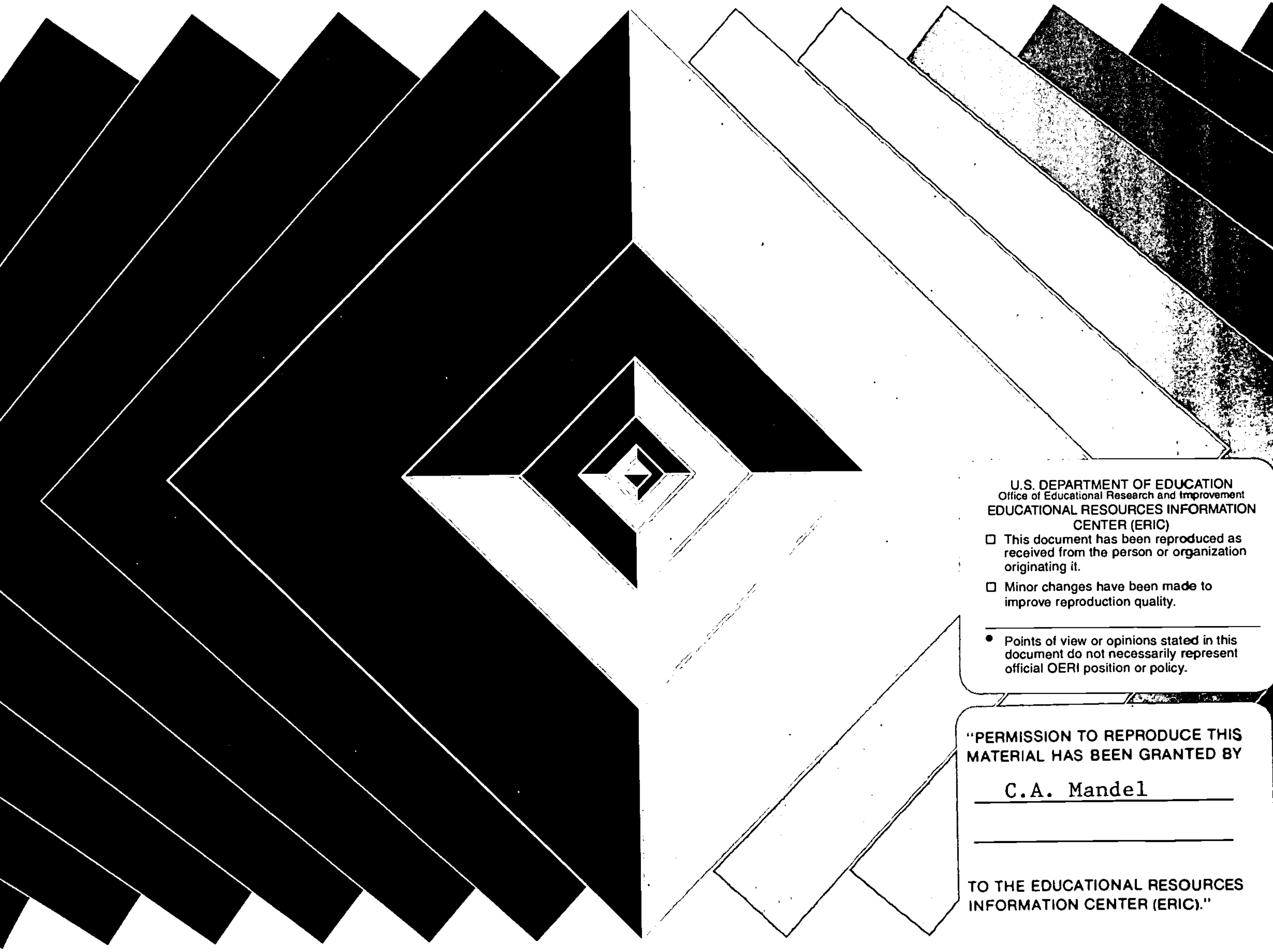
The objectives of this survey were: to gather information on the development of institutional information technology policies and guidelines for responsible computing and use of electronic information; to identify the scope of such policies and guidelines; and to determine the role of the library in the development and/or use of the policies and guidelines. Thirty-nine responses were received from the 119 ARL institutions surveyed; not all respondents answered all questions. Of the 39 respondents, only two indicated that their institutions have not established electronic information policies. The remaining 37 reported that their institutions have either established policies or are in the process of doing so. Six indicated that they have a combination of official and interim policies. Four responding institutions are ARL members not affiliated with higher education institutions. Survey data is discussed in terms of promoting user access of policies; participants in developing policies; relationship to other institutional policies or guiding principles; issues concerning access and use; Internet/World Wide Web access; personal homepages, and linking to commercial sites; copyright and intellectual ownership; areas and issues for future policies; incidents of improper computer usage; whether institutions should develop policies (as opposed development of policies by state and federal agencies); and whether this survey topic should be revisited at a later date. The survey confirmed that libraries have much to contribute to the development of institutional policies and guidelines, and that they should continue to participate in this development by assuming coordinating, facilitating, and collaborating roles within the institution. There is a need to structure policies to serve as an educational tool to raise the awareness of users that many issues (privacy, harassment, and copyright, for example) transcend technologies. (AEF)

SPEC

SYSTEMS AND PROCEDURES EXCHANGE CENTER

Kit 218

Information Technology Policies
October 1996



ASSOCIATION OF RESEARCH LIBRARIES OFFICE OF MANAGEMENT SERVICES

SPEC
SYSTEMS AND PROCEDURES EXCHANGE CENTER

Flyer 218

Information Technology Policies
October 1996

Introduction

The rapid expansion of networks and information systems, widespread use of electronic communications, and the unprecedented success of the World Wide Web are all contributing to the burgeoning growth of the electronic environment in many sectors, but especially in academic institutions. Although campus computing centers continue to hold a key position in matters related to the use of computing resources and electronic information, research libraries are beginning to assume an increasingly active and visible role in providing and facilitating access to networks, information systems, and electronic communications, as well as in disseminating electronic information. While all research libraries have assumed expanded roles vis-à-vis the delivery of computer-mediated services, public academic institutions have a "public face" and an additional capacity as a community resource. Campus computing units may be able to focus on providing services to students, faculty, and staff; libraries in public institutions, on the other hand, must also address issues related to making electronic information resources available to external users. For example, the library may provide key access to the Internet for community users.

The objectives of this survey were: to gather information on the development of institutional information technology policies and guidelines for responsible computing and use of electronic information; to identify the scope of such policies and guidelines; and to determine the role of the library in the development and/or use of the policies and guidelines.

Thirty-nine responses were received from the 119 ARL institutions surveyed. This 33% response rate may well be one of the smallest SPEC Kit survey returns. No doubt the expectation that one needs to have a certain degree of knowledge about activities and issues relating to electronic information policies and guidelines at both the institutional and library level contributed to the difficulty of this survey. Several institutions, in fact, took a collaborative approach in responding to the survey by coordinating and consulting other campus units, such as computing centers and administrative units. Further, it is important to note that not all respondents answered all questions. As one respondent commented, "I believe that this survey addresses a scope much wider than libraries are involved with. For a librarian to get these answers from his/her campus would entail a long and difficult process." The same individual also said, "since the field is now in great flux, and probably will be like that for a long time, I doubt that the responses would hold true for long after these survey results are published." While this respondent's views are well-taken, comments from other respondents quite clearly showed that librarians are staying abreast of activities related to electronic information policies and guidelines at both the campus and the library level and that in fact a number of libraries have been actively engaged in such activities. Finally, in spite of the dynamic nature of the networked information environment, the findings of this survey provide a sketch of the state of electronic information policies and guidelines as reported by one-third of the ARL member libraries.

Survey Results

Among the 39 respondents, only two indicated that their institutions have not established electronic information policies. The remaining 37 (95%) reported that their institutions have either established policies or are in the process of doing so. Six indicated that they have a combination of official and interim policies. As one respondent noted, "we have a mix, and probably always will." Respondents were asked to provide their institutions' information technology polices; these came in the form of both URL's and paper copies.

Four of the 39 responding institutions are ARL members not affiliated with higher education institutions. In a number of the survey questions, the responses from these "nonacademic" institutions are reported separately.

Issues & Trends

Promoting User Awareness of Policies: Electronic medium (e.g. gopher, bulletin boards, homepages, email distribution) appears to be more widely used to disseminate electronic information policies to users and to promote their awareness of these policies than print

Association of Research Libraries Office of Management Services

medium (e.g. student handbook, faculty/staff handbook, and other policy manuals). Several institutions require acknowledgment of their policies at the time accounts are activated, by either requiring users to "pass through a page" or by signing a printed form for file. When asked about the effectiveness of their communication of their policies to users, the responses showed that internal communication to students, faculty, and staff was viewed as more effective than communication to external or public users.

Participants in Developing Policies: Among the 33 academic institutions with electronic information policies, six reported that a single campus unit, working alone, was responsible for the development of such policies at their institutions. In these cases, the initiative appeared to have originated within the unit. The 27 libraries which reported the involvement of representatives from multiple campus units noted that, aside from computing unit members, the standard participants included: faculty and staff (both 24 cases); library (20 cases); legal counsel (17 cases); and students (14 cases). Senior administrators at the vice chancellor/vice president level or above served as the initiators or conveners of such efforts. Clearly, libraries have been actively engaged in institutional planning efforts related to the development of electronic information policies.

Relationship to Other Institutional Policies or Guiding Principles: While electronic information policies and guidelines frequently relate or refer to other institutional policies, the relationships are often implicit rather the explicit. From the responses, a relationship to other policies emerged (in descending order): code of conduct; legal authorities (state codes, statutes, policies and administrative statutes); privacy; intellectual ownership and rights; principles of academic freedom; and speech code. One respondent commented that "Policy is silent by design on issues that are not technology-based. Speech and other codes are based at the campus level and the same rules apply to print, network, etc." Another respondent made note of the institution's policies: "Some are official university policies that do not focus specifically on computing but can be applied to computing." The notion of an "implicit" relationship also appeared to be the thread linking electronic information policies to existing policies.

Issues Concerning Access and Use: Nearly 76% of the respondents reported that their institutions have developed policies on the use of electronic mail by students (undergraduate and graduate), faculty, and staff. Email privacy clearly emerged as the issue that has received the most attention, although one respondent observed, "email privacy/security is a big unresolved issue." In comparison, only 58% of the libraries reported that they have established policies on the use of electronic library databases.

Responses regarding the other "use"-related areas, such as creation and maintenance of institutional records, and use and access to private and public institutional ation, showed that a significant number of the responding academic institutions have developed such policies and guidelines. Although 70% of the academic institutions indicated that they have developedpolicies in the five categories listed, only 35% have also established their own policies on these issues in addition to their institution's.

Internet/WWW Access, Personal Homepages, and Linking to Commercial Sites: In the last three years, there has been exponential growth in the use of the Internet, especially the World Wide Web, to access and create information. Academic institutions have been particularly active in this arena, often with the libraries playing a leadership role. At the same time, the speed of growth of the use of the Internet/WWW appears to be outpacing the development of policies by the academic institutions based on the responses received. Among the 33 academic institutions that have electronic information policies, 20 (61%) have established policies that address Internet/WWW access by staff and faculty, and 18 (55%) have policies for students. Nineteen respondents have policies to address the creation of personal homepages by faculty and staff; 16 noted that their institutions have guidelines for students. One respondent noted, "The Library's guidelines preclude creation of library staff personal homepages on library servers. All use of resources is to be related to mission of the Library." Another commented, "The Libraries' policies state that personal homepages by librarians and library staff are not appropriate for the Libraries' web, but many librarians and library staff have personal homepages on the university's web."

Commercial use of the Internet has surpassed the educational use in the last two years, and the majority of commercial enterprises, especially technology companies, have easily accessible corporate homepages on the Internet. Yet, only eight respondents among the academic institutions reported having policies that address linking institutional homepages to commercial or private corporations. One respondent noted "any linking to private sector is discouraged," and another stated " the university is very protective of who links to our homepage ..." Several respondents commented that policies on this topic were either under discussion or in development in their institutions, and one respondent said, "Frankly, I had never thought of this until this questionnaire."

Copyright and Intellectual Ownership: Eighteen respondents among the 33 (55%) academic institutions that have established electronic information policies said that their institutions have policies to address intellectual ownership or copyright issues in the electronic environment, and 13 respondents (39%) said that their libraries had such policies. One respondent commented, "General guidelines on intellectual property are understood to apply in the electronic environment. The Library maintains an institutional webpage on copyright and has produced printed guidelines for distribution." Another respondent noted that their libraries' guidelines "for librarians and staff who create web resources and services point out the importance of acknowledging intellectual ownership of Internet resources." Two other respondents added, "we could use some institution/library specific guidelines to this category."

Areas and Issues for Future Policies: Respondents were asked to list additional areas that they thought their institution's or library's policies needed to address. There was surprisingly little overlap in the comments. Several respondents identified specific items such as: universal access, student rights and responsibilities, access to listservs and discussion lists, and standards. Others identified conceptual areas, with one respondent commenting, "In order to establish liability and responsibility, we are searching for a clear definition of the boundary between an "official" institution web site and the uncontrolled, outside world;" another noting, "the right of faculty and staff to a base level of technology;" and yet another identifying, "the institution's need to place controls in the networked environment vs. intellectual/academic freedom issues."

Incidents of Improper Computer Usage: The majority of respondents from academic institutions indicated that there had been incidents of improper computer usage at their institution. Twenty respondents knew of harassment incidents; 16 reported advertising; 15 reported incidents of pornography; and 7 noted freedom of speech incidents. From the responses and comments, it seemed that respondents were aware of incidents within or involving the selected areas, but that knowledge of other institutional incidents was primarily anecdotal since such incidents are often not widely publicized. The incidents of improper computer usage seemed to focus around the use of public access computers for "other than posted purposes": chat rooms, email mailbox "flooding," "unprofessional usage," or "offensive messages;" network "sniffing," password compromise or "other unwelcome network connections;" and the display or printing of pornographic images. As one respondent commented, "someone sent an image of a "healthy" young woman to my networked laser printer. Was that pornography?"

Should Institutions Develop Policies or Wait for State and Federal Policies?: Thirty-five of the 37 respondents felt that it was important for their institutions to develop policies or guidelines for proper and ethical use of electronic facilities. While one respondent cautioned, "but with discretion at this time," the general consensus from the respondents seemed to be that there is a significant role for the institution in defining local standards of acceptable use. As another respondent noted, "Federal and state legislation may address pornography, etc., but proper use deals with more important issues like bogging down the net with game-playing, hogging bandwidth, properly configuring servers, and in general using the net for the educational purposes which are paying the bills."

Should This Topic Be Revisited?: There was a clear, strong consensus from the respondents (87%), that this topic should be revisited at a later date. That "later date" ranged from a few months to three years. The comments indicated that, overall, the respondents felt that policies and guidelines are needed now, and as one respondent explained, "Obviously we will need to make changes as we learn more and our environment changes, but we have a responsibility to address the topic now because the need is here." Several respondents viewed attention to information technology policies as an ongoing need: "Technology changes often result in capabilities not previously accounted for in existing paper-based policies."

Conclusion

Although the response rate to this survey was lower than anticipated, it is significant to note that the respondents overall were cognizant of the scope and complexity of the issues encompassed by information technology policies. While it is clear, as one respondent rightly observed, that this survey "goes well beyond the scope of library-related issues that most ARL surveys cover," the thoughtful comments from all of the respondents confirmed that these policies are needed. The survey also confirmed that libraries have much to contribute to the development of institutional policies and guidelines, and that they should continue to participate in this development by assuming coordinating, facilitating, and collaborating roles within the institution. While a number of policies are based on specific technologies, and the speed, range, minimal cost and effort with which users can perpetrate havoc with electronic information presents unique problems, there is a definite need to structure policies to serve as an educational tool to raise the awareness of users that many issues (e.g., privacy, harassment, and copyright) transcend technologies. Several respondents commented that there is an assumption in their institutions that information technology policies are implicit; that electronic information is the same as non-electronic, and that users should, and do, know that.

This Kit and Flyer were compiled by Shirley Leung, Associate University Librarian, Research and Instruction, and Diane Bisom, Head, Systems Department, University of California, Irvine Libraries and were prepared as part of the OMS Collaborative Research/Writing Program.

SPEC

SYSTEMS AND PROCEDURES EXCHANGE CENTER

Information Technology Policies

A SPEC Kit compiled by

Shirley Leung
and
Diane Bisom
University of California, Irvine

October 1996

Editor....Laura A. Rounds, OMS Program Officer for Information Services
Production Assistant....Marianne Seales, Program Assistant

SPEC Kits are published by the

ASSOCIATION OF RESEARCH LIBRARIES
OFFICE OF MANAGEMENT SERVICES
21 Dupont Circle, NW
Washington, DC 20036
(202) 296-8656 Fax (202) 872-0884
<URL:http://arl.cni.org> <pubs@cni.org>

ISSN# 0160 3582

∞ *The paper used in this publication meets the minimum requirements of American National Standard for Information Sciences—Performance of Paper for Printed Library Materials, ANSI Z39.48-199X.*

ASSOCIATION OF RESEARCH LIBRARIES OFFICE OF MANAGEMENT SERVICES

Systems and Procedures Exchange Center: Supporting Effective Library Management for Over Twenty Years

Committed to assisting research and academic libraries in the continuous improvement of management systems, OMS has worked with its constituents since 1970 to seek the best practices for meeting the needs of users. The OMS Information Services Program maintains an active publications program best known for its Systems and Procedures Exchange Center (SPEC) Kits. Through the OMS Collaborative Research/Writing Program, librarians work with OMS staff in joint research and writing projects. Participants and staff work together in survey design, writing, and editing publications that provide valuable insights and management perspectives on emerging trends, issues, and concerns of the academic and research library community. Originally established as an information source for ARL member libraries, the SPEC program has grown to serve the needs of the library community world-wide.

What Are SPEC Kits and Flyers?

Published ten times per year, SPEC Kits and Flyers contain the most valuable, up-to-date information on the latest issues of concern to libraries and librarians today. SPEC Kits and Flyers are the result of a program of surveys on a variety of topics related to current practice and management of library programs in the ARL membership. The SPEC Flyer is a two-page summary of the status of a current area of interest. It comments on the present situation, reports on the results of an ARL membership survey, and forecasts future trends. The SPEC Kit contains the SPEC Flyer and the best representative supporting documentation from the survey in the form of policy statements, handbooks, manuals, cost studies, user studies, procedure statements, planning materials, and issue summaries. A valuable feature of each SPEC Kit is its selected reading list containing the most current literature available on the topic for further study.

Subscribe to SPEC Kits

Subscribers tell us that the information contained in SPEC Kits and Flyers is valuable to a variety of users, both inside and outside the library. The SPEC Flyer is an inexpensive current awareness tool for keeping up-to-date on important library management topics. The documentation found in SPEC Kits is a good point of departure for research and problem solving. SPEC Kits and Flyers lend immediate authority to proposals and aid in setting standards for designing programs or writing procedure statements. SPEC Kits function as an important reference tool for library administrators, staff, students, and professionals in allied disciplines who may not have access to this kind of information.

SPEC Kits and Flyers can be ordered directly from the ARL Office of Management Services or through your library vendor or subscription agent. For more information contact the ARL Publications Department at (202) 296-8656, or fax (202) 872-0884. Information on this and other OMS products and services can be found on the ARL Gopher <URL:gopher://arl.cni.org> and World Wide Web <URL:http://arl.cni.org>.

SPEC
SYSTEMS AND PROCEDURES EXCHANGE CENTER

Table of Contents

INSTITUTIONAL POLICIES

SURVEY RESULTS

ASSOCIATION OF RESEARCH LIBRARIES

OFFICE OF MANAGEMENT SERVICES

TO: SPEC Liaisons

FROM: Shirley Leung and Diane Bisom, University of California, Irvine Libraries
Laura Rounds, OMS Program Officer for Information Services

DATE: March 4, 1996

RE: SPEC Survey and Call for Documentation on Information Technology Policies

With the tremendous growth of networks and information systems, widespread adoption and use of electronic communications at all levels of academic organizations, and the unprecedented success of the World Wide Web, the electronic community is growing at a exponential rate in the 1990's. The issues of the rights and responsibilities of citizens in this electronic community, as consumers and producers of information, are being formulated and debated in academic institutions, in professional organizations, and in the media. How, or whether, electronic rights and responsibilities relate to, parallel, or intersect established institutional policies such as codes of conduct, intellectual property rights, and academic freedom, are also under scrutiny.

While some academic institutions have developed comprehensive, campus-wide information technology policies and guidelines, others have addressed selected, specific aspects, and some may not have dealt with these issues much at all. Policy development in some institutions has followed a coordinated approach, involving faculty, staff, and students; others have evolved from the policies of a specific unit, such as a computing center.

In many institutions, Libraries play a strategic role in providing and facilitating access to networks, information systems, and electronic communications, as well as in disseminating information. The objectives of this survey are to: gather information on the state and level of development of institutional information technology policies and guidelines for responsible computing; identify the breadth and depth of such policies and guidelines; and to determine the role of the Library in developing and/or using the policies and guidelines.

Please complete the following survey and return to Diane Bisom at <dbisom@uci.edu>.

Please mail all supporting documentation to Diane at:

Research and Instructional Services
Science Library
University of California, Irvine
Irvine, CA 92713

Surveys should be returned no later than March 29, 1996.

A total of 39 responses were received:

- 35 from ARL members affiliated with higher education institutions (henceforth referred to as academic institutions);
- 4 from ARL members not affiliated with higher education institutions (henceforth referred to as nonacademic institutions)

This survey generated the following response rates:

- 32% from ARL academic institutions (i.e. 35 out of 108 ARL academic institutions) or
- 33% from a total of 119 ARL institutions (both academic and nonacademic)

Some respondents did not answer all questions.

1. Do you know if your institution has policies or guidelines governing the use of computing resources?

Academic Institutions		Nonacademic Institutions
33	Yes	4
8	Development Underway	0
2	No (please proceed to questions 13 and 14)	0
5	checked off Yes and Development Underway	0

Out of the 35 responses from the academic institutions, 33 (or 94%) reported that they have developed or are in the process of developing, policies/guidelines related to information technology policies/guidelines.

2. If your institution has such policies or guidelines, are they:

Academic Institutions		Nonacademic Institutions
11	Interim/Draft?	0
29	Official?	4
6	indicated both INTERIM and OFFICIAL	0

3. What methods are/were used to increase awareness or to distribute the policies or guidelines to users?

Internally (to your institution's faculty, staff, students)

Academic Institutions		Nonacademic Institutions
23	Online (i.e. gopher, bulletin boards, etc.)	2
24	Institution's home page	1
7	Via email	2
11	Printed in student handbook	0
6	Printed in faculty handbook	0
4	Printed in staff handbook	1
16	Printed in policy manuals	0
17	Other; please specify:	

On a scale from 1-10 (10 being most effective) how would you rate the quality of these communications?

Academic Institutions		Nonacademic Institutions	
0 - 10	7 - 5	1 - 10	0 - 5
1 - 9	3 - 4	0 - 9	0 - 4
8 - 8	2 - 3	1 - 8	0 - 3
6 - 7	1 - 2	1 - 7	1 - 2
2 - 6	0 - 1	0 - 6	0 - 1

Higher than 6 = 17
Lower than 6 = 14

Externally (to community users, i.e. people who access the institution's computing resources through a public network service provider)

Academic Institutions

19 Online (i.e. gopher, bulletin boards, etc.)
18 Institution's home page
2 Via email
4 Other; please specify:
Hard copy
Not yet done
Given to all who are given accounts
Copies available on request

On a scale from 1-10 (10 being most effective) how would you rate the quality of these communications?

Academic Institutions		Nonacademic Institutions	
1 - 10	5 - 5	0 -10	0 - 5
0 - 9	0 - 4	0 - 9	0 - 4
3 - 8	3 - 3	0 - 8	0 - 3
3 - 7	0 - 2	1 - 7	0 - 2
3 - 6	2 - 1	0 - 6	0 - 1

Higher than 6 = 10
Lower than 6 = 10

4. Who participated (or is participating) in the development of such policies or guidelines? **NOTE: Only responses from the academic institutions are tabulated below.**

6 A single campus unit (such as a department or computing center). Please specify name:
Division of University Computing (DUC)
Computing and Communications; the University Library
Office of Computing Services
Computing Services.
Computing and Administrative Services.
Dept. of Information Technology.

27 Representatives from multiple campus units or a task force. Please specify name:
Information Technology Committee
The Anti-Virus Committee, a cross-campus group of senior computer support staff.
University Computer Security Committee
Joint Campus Committee on Information Technology
ITEC (Information Technology Task Force), Council of Dean, many other committees.
Task Force on Computer Ethics Policy Development (or something similar)
Campus Committee on Networking and Computing.
Executive Policy Board for Computing and Telecommunications; Academic Steering Committee for Computing and Telecommunications; Administrative Steering Committee for Computing and Telecommunications. The last two are advisory to the first.

a. Who was represented on this group, other? Please specify:
24 Faculty
24 Staff
14 Students
20 Library
17 Legal Counsel
14 Administrative Computing
16 Academic Computing
12 Campus Computing
11 Check here if your institution has only one computing unit.
3 Other; please specify:
Legal Counsel; not on committee but involved as necessary
Administration
Telecommunications, Internal Auditing

b. Who established or authorized this group? Please specify:
12 President or Chancellor of University
9 Vice President or Vice Chancellor of University
5 Administrator
1 Faculty
7 Other; please specify:
Computing and Network Services
Joint Committee with Academic Senate
Information Technology Policy Board (Library represented on this)
Administrator : Associate Vice Chancellor
V.P., Information Systems & Technology
Officers of the University (Pres. & All Vice-Presidents)
Provost and President

5. Do these policies or guidelines relate or refer to other institutional policies or guiding principles?

Academic Institutions		Nonacademic Institutions
22	Code of Conduct	2
9	Principles of Academic Freedom	1
7	Speech Code	1
18	Intellectual Ownership and Rights	1
20	Privacy	1
22	State codes/policies/administrative codes/statutes	1
2	Don't know	

6. Does your institution have policies or guidelines that address issues of equity of access and availability of electronic information?

Academic Institutions		Nonacademic Institutions
10	Yes	1
6	Development Underway	0
11	No	3

7. Does your institution have policies or guidelines concerning access to and use of electronic information, specifically in the following areas:

Academic Institutions				Non-Academic Institutions
Yes	No	Don't Know		
25	4	1	Creation of E-Mail by undergrad students	0
25	4	1	Use of E-Mail by graduate students	0
25	4	2	Use of E-Mail by faculty and staff	2
26	2	2	E-Mail privacy	3
19	8	2	Use of electronic library databases by students, faculty and staff	1
19	7	2	Use of electronic library databases by community or unaffiliated users	1
18	8	2	INTERNET/WWW access by students	0
20	6	2	INTERNET/WWW access by faculty/staff	1

8. Does your institution and/or library have policies or guidelines for the following areas:

Academic Institutions			Non-Academic Institutions
Library	Institution		
13	25	Creation of institutional records	4
12	24	Maintenance (including archiving and deletion) of institutional records)	4
12	26	Use/access to private institutional information (hiring, reviews, budgets)?	3
11	25	Use/access to public institutional information (i.e. course requirements, catalog,faculty names)?	2
10	23	Creation/use/access of personal (home addresses, phone numbers, etc.) or personnel (performance reviews, benefits, etc.) information?	3

9. Does your institution and/or library have policies or guidelines that address the creation of personal home pages on the World Wide Web by students, faculty, or staff?

Academic Institutions			Nonacademic Institutions
Library	Institution		
1	16	Students	0
7	19	Faculty	0
10	19	Staff	3

10. Does your institution and/or library have any policies or guidelines that address linking institutional homepages to private corporations, which either have sponsorship or business relationships with the institution on the INTERNET/WWW?

Academic Institutions

8	Institution
1	Library

Nonacademic Institutions:

1

11. Does your institution and/or library have policies or guidelines that address intellectual ownership or copyright issues in the electronic environment?

Academic Institutions

18	Institution
13	Library

Nonacademic Institutions

2

12. What additional areas do your institution's or library's policies or guidelines need to address? Please list those areas.

Comments:

- In order to establish liability and responsibility, we are searching for a clear definition of the boundary between an "official" UCSD web site and the uncontrolled, outside world.
- Use of university resources for political campaigning, University compliance with Communications Decency Act (CDA), University's liability for individual faculty, staff, and student compliance with CDA.
- Electronic services: access to listserv, discussion lists, use of Webserver
- The area of what is "commercial" is being considered.
- The institution's need to place controls in the networked environment vs intellectual/academic freedom issues. Universal access. Students rights and responsibilities. Libraries responsibility to provide access. "Right" of faculty and staff to a base level of technology. Standards.
- Intellectual property and Internet/new media courseware or courses; 2. Commercial use of Internet.

13. Has your institution experienced any recent incidents of improper computer usage?

Academic Institutions				**Nonacademic Institutions**
Yes	**No**	**Don't Know**		
20	**6**	**6**	Harassment	**1**
16	**3**	**9**	Advertising	**1**
15	**8**	**8**	Pornography	**1**
7	**4**	**15**	Freedom of Speech issues	**0**

14. Do you think that:

35 It is important for your institution to develop policies or guidelines for proper and ethical use of electronic facilities?

2 It is better to wait for federal state legislation to address these issues?

15. Articles in recent literature indicate that information technology policies are in a fluid or developing state. Do you think that this topic should be revisited at a later date?

34 Yes, when?
    12 Annually
    1 18 months
    8 Every 2 years
    1 Every 3 years
    3 Continuously
5 No

RESPONDING INSTITUTIONS

University of Alabama
University of Alberta
Auburn University
University of California, Davis
University of California, Irvine
University of California, Riverside
University of California, San Diego
University of California, Santa Barbara
Center of Research Libraries
University of Colorado
Colorado State University
University of Georgia
Georgia Institute of Technology
University of Hawaii
University of Houston
University of Illinois at Urbana-Champaign
Indiana University
Johns Hopkins University
Université Laval
Library of Congress
Louisiana State University
McMaster University
University of Massachusetts
National Library of Canada
University of Nebraska-Lincoln
University of New Mexico
Northwestern University
University of Notre Dame
Oklahoma State University
Pennsylvania State University
Purdue University
Rutgers University
Smithsonian Institution Libraries
University of South Carolina
Syracuse University
University of Tennessee-Knoxville
University of Toronto
Washington State University
York University

Information Technology Policies URLs Provided by Responding Institutions

University of Alberta	http://libits.library.ualberta.ca/library_html/copyright.html
Auburn University	http://www.auburn.edu/its/guide/policies.html
University of California,Davis	http://www.ucdavis.edu/AUP.html
University of California, Irvine	http://www.oac.uci.edu/oacweb-v3/org/computer_use_policy.html
University of California, Riverside	gopher://gopher.ucr.edu:70/11 /Computing%20%26%20Communication%20Services/Academic
University of California, San Diego	http://www-acs.ucsd.edu/main/instsupp.html
University of California, Santa Barbara	http://www.ucsb.edu/policy.shtml
University of Colorado	http://www.cudenver.edu/public/cins/ethics.html
University of Georgia	http://www.uga.edu/~ucns/sites/use.html
Georgia Institute of Technology	http://www.gatech.edu/itis/policy/usage/contents.html
University of Hawaii	http://rs6000.adm.fau.edu/rinaldi/netiquette.html
University of Houston	http://www.uh.edu/info_serv/users_guide/guidelines.html
University of Illinois at Urbana	http://www.uiuc.edu/cgi-bin/print_hit_bold.pl/ccso/ETB /Minutes2_96.html?policy#first_hit
Indiana University	http://infotech.indiana.edu/policy/policy.html
Johns Hopkins University	http://www.jhu.edu/www/jhuniv/guidelin.html
Université Laval	http://www.ulaval.ca/sg/reg/Politiques/index.html
Louisiana State University	http://www.lsu.edu/OCS/homedocs/usage_policy.html
McMaster University	http://www.mcmaster.ca/cgibin/bold/cis/policy /comm.htm?policy#first_hit

UNIVERSITY OF NEW MEXICO	http://www.unm.edu/cirt/info/general/ethics.html
NORTHWESTERN UNIVERSITY	http://www.nwu.edu/it/policies
PENNSYLVANIA STATE UNIVERSITY	http://www.personal.psu.edu/dept/cac/publications/web/policies/ind.html
PURDUE UNIVERSITY	http://www.purude.edu/PUCC-Services/docs.and.training/PUCC.Docs/docindx/Zdocs/zzpolicy.html
UNIVERSITY OF SOUTH CAROLINA	gopher://vega.lib.nscu.edu:70/00/library/reference/guides/netiquette
UNIVERSITY OF TENNESSEE-KNOXVILLE	http://www.cas.utk.edu/CAS/casccp.html
UNIVERSITY OF TORONTO	http://www.utoronto.ca/security/appuse.htm#Use
YORK UNIVERSITY	http://www.yorku.ca/admin/ccis/general/policy.htm

EMAIL POLICIES

University of California, Office of the President

University of California Electronic Mail Policy

As per the appended letter from President Richard Atkinson, the University of California Electronic Mail Policy was issued August 6, 1996. On that date, it became effective as interim policy with final Universitywide implementation to be effective on January 1, 1997. The intervening period is to allow campuses time to develop supporting guidelines and procedures.

The final Policy was undoubtedly shaped to a considerable extent by the many constructive comments on earlier drafts provided by members of the U.C. community. The Electronic Mail Task Force would like to thank all those who took the time to read earlier drafts and provide those comments, and who participated in the general dialog that led to this Policy.

Although the Policy has now been issued, comments are still welcome. Please email them to: emailpol@ucop.edu, with the understanding that it will not be possible to reply to all comments received.

Policy Table of Contents

August 6, 1996

CHANCELLORS

Dear Colleagues:

Enclosed is the University of California Electronic Mail Policy. It is effective immediately as interim policy, with final universitywide implementation to take place by January 1, 1997.

The Electronic Mail (Email) Policy clarifies the applicability of existing law and University policies to electronic mail, the use of which is now pervasive across the University, and addresses electronic mail issues not specifically contained in existing policies. The Policy also discusses a number of misunderstandings surrounding the use of email.

All nine campuses and the Office of the President were represented on the Email Policy Task Force (list appended to the policy document) responsible for development of this Policy, with faculty, staff, and students participating. The Task Force membership covered diverse areas of expertise, representing many different perspectives. I appreciate the work of the Task Force in this complex undertaking.

The Policy recognizes that principles of academic freedom, freedom of speech, and privacy of information hold important implications for electronic mail communications. These implications have been an important part of the universitywide dialog and consultation undertaken by the Electronic Mail Policy Task Force. The Policy as formulated by the Task Force and supported by the Academic Council seeks to strike the right balance between these principles of privacy and academic freedom and the often conflicting needs of law, University policy, and administrative practice.

Section IX of the Policy requires campuses to develop implementing procedures during the Fall academic term, 1996. Therefore, I am accepting the recommendation of the Email Policy Task Force that the Interim Policy become final Universitywide effective January 1, 1997. Associate Vice President for Information Resources and Communications Stuart Lynn will assist on implementation and questions of interpretation; please inform him (510-987-0405) as to whom you will designate as your campus Email Policy Coordinator for this purpose.

Sincerely,

Richard C. Atkinson
President

cc: Members, President's Cabinet
Laboratory Directors Senior Vice President Kennedy
Associate Vice President Lynn
Special Assistant Gardner
Academic Council Chair Leiman
Principal Officers of The Regents

Back to UCOP Home Page

This page last updated August 7, 1996.

Electronic Mail Policy

University of California
Office of the President
August 1, 1996

TABLE OF CONTENTS

I. INTRODUCTION

This Policy clarifies the applicability of law and of other University policies to electronic mail. It also defines new policy and procedures where existing policies do not specifically address issues particular to the use of electronic mail.

The University recognizes that principles of academic freedom, freedom of speech, and privacy of information hold important implications for electronic mail and electronic mail services. This Policy reflects these firmly-held principles within the context of the University's legal and other obligations.

The University encourages the use of electronic mail and respects the privacy of users. It does not routinely inspect, monitor, or disclose electronic mail without the holder's (as defined in Appendix A, Definitions) consent. Nonetheless, subject to the requirements for authorization and notification defined in this Policy, the University may deny access to its electronic mail services and may inspect, monitor, or disclose electronic mail when required by and consistent with law, when there is substantiated reason (as defined in Appendix A, Definitions) to believe that violations of policy or law have taken place, or, in exceptional cases, when required to meet time-dependent, critical operational needs. These provisions are comparable to those of policies that apply to other forms of communications, such as conventional mail.

Cautions:
Users should be aware of the following:

1. Both the nature of electronic mail and the public character of the University's business (see Caution 2 below) make electronic mail less private than users may anticipate. For example, electronic mail intended for one person sometimes may be widely distributed because of the ease with which recipients can forward it to others. A reply to an electronic mail message posted on an electronic bulletin board or "listserver" intended only for the originator of the message may be distributed to all subscribers to the listserver. Furthermore, even after a user deletes an electronic mail record from a computer or electronic mail account it may persist on backup facilities, and thus be subject to disclosure under the provisions of Section V of this Policy. The University cannot routinely protect users against such eventualities.

2. Electronic mail, whether or not created or stored on University equipment, may constitute a University record (see Appendix A, Definitions) subject to disclosure under the California Public Records Act or other laws, or as a result of litigation. However, the University does not automatically comply with all requests for disclosure, but evaluates all such requests against the precise provisions of the Act, other laws concerning disclosure and privacy, or other applicable law.

   Users of University electronic mail services also should be aware that the California Public Records Act and other similar laws jeopardize the ability of the University to guarantee complete protection of personal electronic mail resident (see Section VI. A. 8) on University facilities.

   The California Public Records Act does not, in general, apply to students except in their capacity, if any, as employees or agents of the University. This exemption does not, however, exclude student email from other aspects of this Policy.

3. The University, in general, cannot and does not wish to be the arbiter of the contents of electronic mail. Neither can the University, in general, protect users from receiving electronic mail they may find offensive. Members of the University community, however, are strongly encouraged to use the same personal and professional courtesies and considerations in electronic mail as they would in other forms of communication.

4. There is no guarantee, unless "authenticated" mail systems are in use, that electronic mail received was in fact sent by the purported sender, since it is relatively straightforward, although a violation of this Policy, for senders to disguise their identity. Furthermore, electronic mail that is forwarded may also be modified. Authentication technology is not widely and systematically in use at the University as of the date of this Policy. As with print documents, in case of doubt receivers of electronic mail messages should check with the purported sender to validate authorship or authenticity.

5. Encryption of electronic mail is another emerging technology that is not in widespread use as of the date of this Policy. This technology enables the encoding of electronic mail so that for all practical purposes it cannot be read by anyone who does not possess the right key. The answers to questions raised by the growing use of these technologies are not now sufficiently understood to warrant the formulation of University policy at this time. Users and operators of electronic mail facilities should be aware, however, that these technologies will become generally available and probably will be increasingly used by members of the community.

II. PURPOSE

The purpose of this Policy is to assure that:

A. The University community is informed about the applicability of policies and laws to electronic mail;

B. Electronic mail services are used in compliance with those policies and laws;

C. Users of electronic mail services are informed about how concepts of privacy and security apply to electronic mail; and,

D. Disruptions to University electronic mail and other services and activities are minimized.

III. DEFINITIONS

The terms electronic mail and email are used interchangeably throughout this Policy.

The following terms used in this Policy are defined in Appendix A. Knowledge of these definitions is important to an understanding of this Policy.

- □ Computing Facility(ies)
- □ Electronic Mail System or Services
- □ University Email System or Services
- □ Email Record or Email
- □ University Record
- □ University Email Record
- □ Use of University or other Email Services
- □ Possession of Email
- □ Holder of an Email Record or Email Holder
- □ Substantiated Reason

IV. SCOPE

This Policy applies to:

- □ All electronic mail systems and services provided or owned by the University and
- □ All users, holders, and uses of University email services; and
- □ All University email records in the possession of University employees or other email users of electronic mail services provided by the University.

Excluded from the foregoing are electronic mail services of Department of Energy Laboratories managed by the University, and email users of such electronic mail services who are employees and agents of those Laboratories.

This Policy applies only to electronic mail in its electronic form. The Policy does not apply to printed copies of electronic mail. Other University records management policies (see Appendix B, References), however, do not distinguish among the media in which records are generated or stored. Electronic mail messages, therefore, in either their electronic or printed forms, are subject to those other policies, including provisions of those policies regarding retention and disclosure.

This Policy applies equally to transactional information (such as email headers, summaries, addresses, and addressees) associated with email records as it does to the contents of those records.

This Policy is effective immediately as interim policy, with final Universitywide implementation to be effective January 1, 1997.

V. GENERAL PROVISIONS

As noted in the Introduction, the University recognizes that principles of academic freedom, freedom of speech, and privacy of information hold important implications for electronic mail and electronic mail services. This Policy reflects these firmly-held principles within the context of the University's legal and other obligations.

A. **Purpose**. In support of its threefold mission of instruction, research, and public service, the University encourages the use of University electronic mail services to share information, to improve communication, and to exchange ideas.

B. **University Property**. University electronic mail systems and services are University facilities as that term is used in other policies and guidelines. Any electronic mail address or account associated with the University, or any sub-unit of the University, assigned by the University to individuals, sub-units, or functions of the University, is the property of The Regents of the University of California.

C. **Service Restrictions**. Those who use University electronic mail services are expected to do so responsibly, that is, to comply with state and federal laws, with this and other policies and procedures of the University, and with normal standards of professional and personal courtesy and conduct. Access to University electronic mail services, when provided, is a privilege that may be wholly or partially restricted by the University without prior notice and without the consent of the email user when required by and consistent with law, when there is substantiated reason (as defined in Appendix A, Definitions) to believe that violations of policy or law have taken place, or, in exceptional cases, when required to meet time-dependent, critical operational needs. Such restriction is subject to established campuswide procedures or, in the absence of such procedures, to the approval of the appropriate campus Vice Chancellor or University Vice President.

D. **Consent and Compliance**. An email holder's consent shall be sought by the University prior to any inspection, monitoring, or disclosure of University email records in the holder's possession, except as provided for in Section V. E. University employees are, however, expected to comply with University requests for copies of email records in their possession that pertain to the administrative business of the University, or whose disclosure is required to comply with applicable laws, regardless of whether such records reside on a computer housed or owned by the University. Failure to comply with such requests can lead to the conditions of Section V. E.

E. **Restrictions on Access Without Consent**. The University shall only permit the inspection, monitoring, or disclosure of electronic mail without the consent of the holder of such email when: (i) required by and consistent with law, (ii) there is substantiated reason (as defined in Appendix A, Definitions) to believe that violations of law or University policy have taken place, or (iii) in exceptional cases, to meet time-dependent, critical operational needs.

When the contents of email must be inspected, monitored, or disclosed without the holder's consent:

1. **Authorization**. Except in emergency situations, such actions must be authorized in advance and in writing by the authority specified by the law or policy under which the action is taken. If the authority is not specified, authorization must be sought from the responsible (see Section IX, Campus Responsibilities) campus Vice Chancellor or University Vice President. This latter authority may not be further re-delegated. University counsel's advice should normally be sought prior to authorization because of changing interpretations by the courts of laws affecting the privacy of electronic mail, and because of potential conflicts among different applicable laws. Authorization shall be limited to the least perusal of contents and the least action necessary to resolve the situation.

2. **Emergencies**. In emergency situations (for instance, when the community or its members are endangered or when access to electronic mail records must be secured to ensure the preservation of evidence), the least perusal of contents and the least action necessary to resolve the emergency may be taken immediately without authorization, but appropriate authorization must then be sought without delay following the procedures described in Section V. E. 1 above. If the action taken is not subsequently authorized, the responsible authority shall seek to have the situation restored as closely as possible to that which existed before action was taken.

3. **Notification**. In either case, the responsible authority or their designee shall, at the earliest possible opportunity consistent with law and other University policy, notify the affected individual of the action(s) taken and the reasons for the action(s) taken.

4. **Compliance with Law**. Actions taken under Paragraphs 1. and 2. shall be in full compliance with the law and other applicable University policy, including laws and policies listed in Appendix B. This has particular significance for email residing on computers not owned or housed by the University. Advice of counsel always must be sought prior to any action taken under such circumstances. It also has particular significance for email whose content is protected under the Federal Family Educational Rights and Privacy Act of 1974, which applies equally to email as it does to print records.

F. **Recourse**. Procedures for the review and appeal of actions taken under Sections V. C, D, and E and under Section VII shall be implemented (or existing procedures adapted) by each campus to provide a mechanism for recourse to individuals who believe that actions taken by employees or agents of the University were in violation of this Policy.

G. **Misuse**. Both law and University policy prohibit, in general, the theft or other abuse of computing facilities. Such prohibitions apply to electronic mail services, and include (but are not limited to): unauthorized entry, use, transfer, and tampering with the accounts and files of others; interference with the work of others and with other computing facilities. Under certain circumstances, the law contains provisions for felony offenses. Users of electronic mail are encouraged to familiarize themselves with these laws and policies (see Appendix B, References).

VI. SPECIFIC PROVISIONS

A. Allowable Use

In general, use of University electronic mail services is governed by policies that apply to the use of all University facilities. In particular, use of University electronic mail services is encouraged and is allowable subject to the following conditions:

1. **Purpose**. Electronic mail services are to be provided by University organizational units in support of the teaching, research, and public service mission of the University, and the administrative functions that support this mission.

2. **Users**. Users of University electronic mail services are to be limited primarily to University students, faculty and staff for purposes that conform to the requirements of this Section.

3. **Non-Competition**. University Electronic mail services shall not be provided in competition with commercial services to individuals or organizations outside the University.

4. **Restrictions**. University Electronic mail services may not be used for: unlawful activities; commercial purposes not under the auspices of the University; personal financial gain (except as permitted under applicable academic policies); personal use inconsistent with Section VI. A. 8; or uses that violate other University policies or guidelines. The latter include, but are not limited to, policies and guidelines (see Appendix B, References) regarding intellectual property, or regarding sexual or other forms of harassment.

5. **Representation**. Electronic mail users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the University or any unit of the University unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer shall be included unless it is clear from the context that the author is not representing the University . {An appropriate disclaimer is: "The opinions or statements expressed herein are my own and should not be taken as a position, opinion, or endorsement of the University of California."}

6. **False Identity**. University email users shall not employ a false identity. Email may, however, be sent anonymously provided this does not violate any law or this or any other University policy, and does not unreasonably interfere with the administrative business of the University.

7. **Interference**. University email services shall not be used for purposes that could reasonably be expected to cause, directly or indirectly, excessive strain on any computing facilities, or unwarranted or unsolicited interference with others' use of email or email systems . {Such uses include, but are not limited to, the use of email services to: (i) send or forward email chain letters; (ii) "spam", that is, to exploit listservers or similar broadcast systems for purposes beyond their intended scope to amplify the widespread distribution of unsolicited email; and (iii) "letter-bomb", that is, to resend the same email repeatedly to one or more recipients to interfere with the recipient's use of email.}

8. **Personal Use**. University electronic mail services may be used for incidental personal purposes provided that, in addition to the foregoing constraints and conditions, such use does not (i) directly or indirectly interfere with the University operation of computing facilities or electronic mail services; (ii)burden the University with noticeable incremental cost; or (iii) interfere with the email user's employment or other obligations to the University. Email records arising from such personal use may, however, be subject to the presumption in Appendix A, definition of a University Email Record, regarding personal and other email records. Email users should assess the implications of this presumption in their decision to use University electronic mail services for personal purposes.

B. Security and Confidentiality

1. The confidentiality of electronic mail cannot be assured. Such confidentiality may be compromised by applicability of law or policy, including this Policy, by unintended redistribution, or because of inadequacy of current technologies to protect against unauthorized access. Users, therefore, should exercise extreme caution in using email to communicate confidential or sensitive matters.

2. Business and Finance Bulletin RMP-8, *Legal Requirements on Privacy of and Access to Information*, prohibits University employees and others from "seeking out, using, or disclosing" without authorization "personal or confidential" information, and requires employees to take necessary precautions to protect the confidentiality of personal or confidential information encountered in the performance of their duties or otherwise. This prohibition applies to email records. In this Policy the terms "inspect, monitor, or disclose" are used within the meaning of "seek, use, or disclose" as defined in RMP-8.

3. Notwithstanding the previous paragraph, users should be aware that on occasion network and computer operations personnel and system administrators may, during the performance of their duties, inadvertently see the contents of email messages. Except as provided elsewhere in this Policy, they are not permitted to do so intentionally or disclose or otherwise use what they have seen. One exception, however, is that of systems personnel (such as "postmasters") who may need to inspect email when re-routing or disposing of otherwise undeliverable email. This exception is limited to the least invasive level of inspection required to perform such duties. Furthermore, this exception does not exempt postmasters from the prohibition against disclosure of personal and confidential information of the previous paragraph, except insofar as such disclosure equates with good faith

attempts to route the otherwise undeliverable email to the intended recipient. Re-routed mail normally should be accompanied by notification to the recipient that the email has been inspected for such purposes.

4. The University attempts to provide secure and reliable email services. Operators of University electronic mail services are expected to follow sound professional practices in providing for the security of electronic mail records, data, application programs, and system programs under their jurisdiction. Since such professional practices and protections are not foolproof, however, the security and confidentiality of electronic mail cannot be guaranteed. Furthermore, operators of email services have no control over the security of email that has been downloaded to a user's computer.

   As a deterrent to potential intruders and to misuse of email, email users should employ whatever protections (such as passwords) are available to them.

5. Users of electronic mail services should be aware that even though the sender and recipient have discarded their copies of an electronic mail record, there may be back-up copies that can be retrieved. Systems may be "backed-up" on a routine or occasional basis to protect system reliability and integrity, and to prevent potential loss of data. The back-up process results in the copying of data onto storage media that may be retained for periods of time and in locations unknown to the originator or recipient of electronic mail. The practice and frequency of back-ups and the retention of back-up copies of email vary from system to system. Electronic mail users are encouraged to request information on the back-up practices followed by the operators of University electronic mail services, and such operators are required to provide such information upon request.

C. Archiving and Retention

University records management policies do not distinguish among media with regard to the definition of University records. As such, electronic mail records are subject to these policies. In particular, such records are subject to disposition schedules in the University of California Records Disposition Schedules Manual, which distinguishes among different categories of records, from the ephemeral to the archival.

The University does not maintain central or distributed electronic mail archives of all electronic mail sent or received. Electronic mail is normally backed up (see Section VI. B. 5), if at all, only to assure system integrity and reliability, not to provide for future retrieval, although back-ups may at times serve the latter purpose incidentally. Operators of University electronic mail services are not required by this Policy to retrieve email from such back-up facilities upon the holder's request, although on occasion they may do so as a courtesy.

Email users should be aware that generally it is not possible to assure the longevity of electronic mail records for record-keeping purposes, in part because of the difficulty of guaranteeing that electronic mail can continue to be read in the face of changing formats and technologies and in part because of the changing nature of electronic mail systems. This becomes increasingly difficult as electronic mail encompasses more digital forms, such as embracing compound documents composed of digital voice, music, image, and video in addition to text. Furthermore, in the absence of the use of authentication systems (see Section I, Caution 4), it is difficult to guarantee that email documents have not been altered, intentionally or inadvertently.

Email users and those in possession of University records in the form of electronic mail are cautioned, therefore, to be prudent in their reliance on electronic mail for purposes of maintaining a lasting record. Sound business practice suggests that consideration be given to transferring (if possible) electronic mail to a more lasting medium/format, such as acid-free paper or microfilm, where long-term accessibility is an issue.

VII. POLICY VIOLATIONS

Violations of University policies governing the use of University electronic mail services may result in restriction of access to University information technology resources. In addition, disciplinary action may be applicable under other University policies, guidelines, implementing procedures, or collective bargaining agreements, up to and including dismissal.

VIII. RESPONSIBILITY FOR POLICY

The Associate Vice President, Information Resources and Communications (IR&C) in the Office of the President is responsible for development, maintenance, and publication of this Policy.

IX. CAMPUS RESPONSIBILITY AND DISCRETION

Each campus shall develop, maintain, and publish specific procedures and practices that implement this Policy and communicate its provisions to campus users of University electronic mail services. The following are assigned to individual campus authority and discretion:

A. Each campus shall decide whether to publish its students' electronic mail addresses as directory information. An electronic mail address assigned by the University to a student is a student record, unless assigned in the student's capacity, if any, as an employee or agent of the University. In accordance with the policies and procedures in the University's "Policy Applying to the Disclosure of Information from Student Records" (Sections 130-134 of the Policies Applying to Campus Activities, Organizations, and Students), campuses are responsible for designating the categories of personally identifiable information about a student that are public. Individual students may, consistent with the above policy, request the campus not to make their email addresses public for other than educational purposes.

B. Each campus shall establish guidelines as to who may use campus electronic mail services, consistent with the provisions of Section VI. A of this Policy.

C. Each campus shall establish regulations and procedures on actions to be taken once an email user's affiliation with the campus is terminated. In particular, the campus may elect to: terminate the individual's email account, redirect electronic mail, or continue the account, subject to the provisions of Section VI. A of this Policy.

D. Each campus shall establish guidelines and procedures for:

1. Restriction of use of University email services pursuant to Section V. C of this Policy;
2. Authorization, notification, and recourse pursuant to Sections V. E and F of this Policy;
3. Response to requests for information from users concerning the back-up of electronic mail, pursuant to Section VI. B. 5 of this Policy; and
4. Any other provisions of this Policy for which procedures are not explicitly stated.

E. Each campus shall designate the appropriate Vice Chancellor to be responsible for the authorization of action pursuant to Sections V. C and E of this Policy. This authorization responsibility may not be further re-delegated.

F. Each campus shall establish appropriate notification procedures regarding this Policy to all email users, including positive acknowledgment by email users of receipt and understanding. Such notification and acknowledgment can be electronic to the extent that the email user's identity can be assured. It is recognized that it may take time to phase in such procedures; however, the lack of comprehensive procedures shall not, in the interim, invalidate the provisions and applicability of this Policy.

G. Each campus may establish its own procedures that further refine and conform with this Policy.

H. For purposes of this Section IX, the Office of the President shall be regarded as a campus with respect to its own internal operations, except that for this purpose Vice President shall replace Vice Chancellor in Sections V. C and E.

APPENDIX A - DEFINITIONS

Computing Facility(ies): Computing resources, services, and network systems such as computers and computer time, data processing or storage functions, computer systems and services, servers, networks, input/output and connecting devices, and related computer records, programs, software, and documentation.

Electronic Mail System or Services: Any messaging system that depends on computing facilities to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print computer records for purposes of asynchronous communication across computer network systems between or among individuals or groups, that is either explicitly denoted as a system for electronic mail; or is implicitly used for such purposes, including services such as electronic bulletin boards, listservers, and newsgroups.

University Email System or Services: Electronic mail system or services owned or operated by the University or any of its sub-units.

Email Record or Email: Any or several electronic computer records or messages created, sent, forwarded, replied to, transmitted, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several email systems or services. This definition of email records applies equally to the contents of such records and to transactional information associated with such records, such as headers, summaries, addresses, and addressees. This Policy applies only to electronic mail in its electronic form. The Policy does not apply to printed copies of electronic mail.

University Record: A "public record" as defined in Business and Finance Bulletin RMP-8, Legal Requirements on Privacy of and Access to Information and the California Public Records Act. "Public records" include any writing containing information relating to the conduct of the public's business prepared, owned, used, or retained (by the University) regardless of physical form or characteristics. [California Government Code Section 6252(d)]. With certain defined exceptions, such University records are subject to disclosure under the California Public Records Act.

> *Records held by students, including email, are not University records unless such records are pursuant to an employment or agent relationship the student has or has had with the University. This exemption does not, however, exclude student email from other aspects of this Policy, regardless of whether such email is a University record.*

University Email Record: A University record in the form of an email record regardless of whether any of the computing facilities utilized to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print the email record are owned by the University. This implies that the location of the record, or the location of its creation or use, does not change its nature as: (i) a University email record for purposes of this or other University policy (see, however, Sections V. D and E), and (ii) having potential for disclosure under the California Public Records Act.

> *Until determined otherwise or unless it is clear from the context, any email record residing on university-owned computing facilities may be deemed to be a University email record for purposes of this Policy. This includes, for example, personal email (see Section VI. A. 8). Consistent, however, with the principles asserted in Section V. E. of least perusal and least action necessary and of legal compliance, the University must make a good faith a priori effort to distinguish University email records from personal and other email where relevant*

> *to disclosures under the California Public Records Act and other laws, or for other applicable purposes of this Policy.*

Use of University or other Email Services: To create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print email (with the aid of University email services). A (University) Email User is an individual who makes use of (University) email services.

> *Receipt of email prior to actual viewing is excluded from this definition of "use" to the extent that the recipient does not have advance knowledge of the contents of the email record.*

Possession of Email: An individual is in "possession" of an email record, whether the original record or a copy or modification of the original record, when that individual has effective control over the location of its storage. Thus, an email record that resides on a computer server awaiting download to an addressee is deemed, for purposes of this Policy, to be in the possession of that addressee. Systems administrators and other operators of University email services are excluded from this definition of possession with regard to email not specifically created by or addressed to them.

> *Email users are not responsible for email in their possession when they have no knowledge of its existence or contents.*

Holder of an Email Record or Email Holder: An email user who is in possession of a particular email record, regardless of whether that email user is the original creator or a recipient of the content of the record.

Substantiated Reason: Reliable evidence indicating that violation of law or policy probably has occurred, as distinguished from rumor, gossip, or other unreliable evidence.

APPENDIX B - REFERENCES

The following list identifies significant sources used as background in the preparation of this Policy, whether or not they are directly referenced by this Policy. It does not, however, include all federal and state laws and University policies that may apply to electronic mail. These policies and laws change from time to time, therefore users of this Policy are encouraged to refer to on-line versions of this and other University policies accessible on the Office of the President home page on the World Wide Web.

- □ **University Policies and Guidelines**
    - □ Business and Finance Bulletins:
        - ■ A 56, Academic Support Unit Costing and Billing Guidelines
        - ■ BUS 29, Management and Control of University Equipment
        - ■ BUS-43, Materiel Management
        - ■ BUS-65, Guidelines for University Mail Services
        - ■ IS-3, Guidelines for Security of Computing Facilities
        - ■ IS 6, Campus Communications Guidelines
        - ■ RMP-1, University Records Management Program
        - ■ RMP-2, University Records Disposition Program
        - ■ RMP-7, Privacy of and Access to Information Responsibilities
        - ■ RMP-8, Legal Requirements on Privacy of and Access to Information
    - □ Personnel Manuals and Agreements:
        - ■ Academic Personnel Manual
        - ■ Personnel Policies for Staff Members

        - ■ Administrative and Professional Staff Program Personnel Policies
        - ■ Staff Personnel Policies
        - ■ Collective Bargaining Contracts (Memoranda of Understanding)

    - □ Other Related Policies and Guidelines:

        - ■ Campus Access Guidelines for Employee Organizations (Local Time, Place, and Manner Rules)
        - ■ Policies Applying to Campus Activities, Organizations, and Students
        - ■ Policy and Guidelines on the Reproduction of Copyrighted Materials for Teaching and Research
        - ■ Policy on Copyright Ownership
        - ■ University of California Records Disposition Schedules Manual

- □ **State of California Statutes**

    - □ State of California Education Code, Section 67100 et seq.
    - □ State of California Information Practices Act of 1977 (Civil Code Section 1798 et seq.)
    - □ State of California Public Records Act (Gov. Code Section 6250 et seq.)
    - □ State of California Penal Codes, Section 502

- □ **Federal Statutes**

    - □ Federal Family Educational Rights and Privacy Act of 1974,
    - □ Federal Privacy Act of 1974
    - □ Electronic Communications Privacy Act

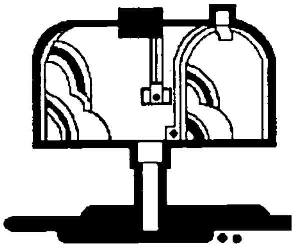
Last updated August 1, 1996

Digit

University of Colorado at Boulder
Computing and Network Services
March/April 1996
Volume 31, Number 2

University Adopts Policy on E-mail Use

Electronic mail has become an essential tool for faculty, staff, and students of the University. Yet like all powerful tools, it has the ability to damage as well as to assist. In 1993, the Policy Board for Information Technology asked the assistant vice president for computing and information systems to draft a University e-mail policy to promote constructive, rather than destructive, use of e-mail. A working group including representatives of information technology, internal audit, legal counsel, personnel, and faculty prepared the policy after reviewing comparable documents from around the country.



The policy addresses issues of privacy and responsible use. It defines permissible and prohibited use and gives examples. It states the University's right to access and disclose the contents of electronic communications, but also sets forth the requirements for prior approval of such access.

After extensive review on all the campuses, the following statement has been adopted as an official administrative policy statement of the University. If you have questions about the policy, contact Lindsay Winsor at University Management Systems (Winsor_1@wizard.Colorado.EDU).

(Continued on page 5)

In this Issue . . .

General

CNS Notes

Around the Campus

Computing Classes and Workshops

Please fill out our Reader Survey on page 21. We want to hear from you.

Contributors to this issue: Lori Arp, Barbara Black, John Dennett, Wendy DuBow, Heidi Dudek, Bruce Fast, Keith Gresham, Pat Jensen, Brad Judy, Suzanne Kincaid, Ken Klingenstein, Peter Marshall, Tim Neese, Lindsay Winsor, Bill Wyman.

University E-mail Policy

(Continued from page 1)

I. Introduction

In 1986, Congress passed the Electronic Communications Privacy Act (ECPA) that made it illegal to intercept electronic communications on a public or private network without proper authorization. The ECPA provides electronic transmission of messages the same privacy protection as telephone calls over the public telephone systems. System operators of public networks are not permitted to divulge the contents of messages except under a narrow set of circumstances.

The ECPA also protects internal systems, such as those at the University of Colorado, from unauthorized interception of messages by outside sources. However, the ECPA permits messages that are stored on internal systems to be accessed by authorized personnel without violating the Act.

This statement sets forth the University's policy with regard to use of, access to, and disclosure of electronic communications. For purposes of this policy statement, electronic communications includes but is not limited to electronic mail, Internet services, voice mail, audio and video conferencing, and facsimile messages that are sent or received by faculty, staff, students, and other authorized users of University resources. Attached to the statement are two appendices: one providing concepts for consideration in granting approval to access electronic communications of others, and one discussing e-mail privacy and ethics.

II. Policy

A. Permissible Uses of Electronic Communications

1. Purpose of Use – The use of any University resources for electronic communications should be related to University business including academic pursuits.

2. Authorized Persons – Only faculty, staff, students, and other authorized persons conducting University business may use the electronic communication systems.

B. Prohibited Uses

1. Personal, Commercial Purposes – University resources for electronic communication shall not be used for personal, commercial purposes. Incidental and occasional personal use of electronic mail and voice mail may occur when such use does not generate a direct cost for the University, but such messages will be treated no differently from other messages. (An example of a use that does not create a direct cost is placing a local telephone call: the University will pay no more for telephone service than it would have paid had the call not been made. An example of a use that does create a direct cost is placing a long-distance telephone call: the University will pay a direct charge for that call. Likewise, any activity that involves printing creates a direct cost.)

2. Other Prohibited Use – Other prohibited electronic communications include, but are not limited to:

a. Use of electronic communications to send copies of documents in violation of copyright laws.
b. Use of electronic communication systems to send messages, access to which is restricted by laws or regulations.
c. Capture and "opening" of undeliverable electronic communication except as required in order for authorized employees to diagnose and correct delivery problems.
d. Use of electronic communications to intimidate others or to interfere with the ability of others to conduct University business.
e. "Spoofing," i.e., constructing electronic communication so it appears to be from someone else.
f. "Snooping," i.e., obtaining access to the files or communications of others for the purpose of satisfying idle curiosity, with no substantial University business purpose.
g. Attempting unauthorized access to data or attempting to breach any security measures on any electronic communication system, or attempting to intercept any electronic communication transmissions without proper authorization.

(Continued on next page)

University E-mail Policy

(Continued from page 5)

C. University Access and Disclosure

1. Grounds Required for Access – The University reserves the right to access and disclose the contents of faculty, staff, student, and other authorized users' electronic communications, but will do so only when it has a legitimate business need such as those listed in number 2 below, and only with explicit authorization. The University's electronic communication systems should be treated like a shared filing system—i.e., with the expectation that messages sent or received on University business or with the use of University resources may be made available for review by any authorized University official for purposes related to University business.

2. Monitoring of Messages – The University will not monitor electronic messages as a routine matter.

The University will inspect the contents of electronic messages in the course of an investigation triggered by indications of misconduct, as needed to protect health and safety, as needed to prevent interference with the academic mission of the institution, or as needed to locate substantive information required for University business that is not more readily available by some other means. The University will respond to legal processes and fulfill its obligations to third parties.

3. Limitations on Disclosure and Use of Information Obtained by Means of Access or Monitoring – The contents of electronic communications, properly obtained for legitimate business purposes, may be disclosed without permission of the employee. The University will attempt to refrain from disclosure of particular messages if disclosure could create personal embarrassment, unless such disclosure is required to serve a business purpose or satisfy a legal obligation.

4. Special Procedures to Approve Access, Disclosure or Use of Electronic Messages – Individuals needing to access the electronic communication of others, to use information gained from such access, and/or to disclose information from such access must obtain approval for such activity in advance. The chancellor of each campus shall develop a written statement of procedure to be followed to request such approval. That procedure shall take into consideration ways to minimize the time and effort required to submit and respond to requests, the need to minimize interference with University business, and the rights of individuals.

D. Disciplinary Action

Appropriate disciplinary action will be taken against individuals found to have engaged in prohibited use of the University's electronic communications resources.

Attachment I: Concepts for Granting Approval to Access Electronic Communications of Others

The following are suggestions for elements to be considered in designing the process for granting approval to access electronic communications addressed to others:

1. What information is needed to determine whether a request should be approved? Possibilities include:

- Name and title of the person whose communications will be accessed;
- Name and title of the person who will do the accessing;
- Why the access is needed;
- What forms of communication will be accessed (e.g., voice mail, e-mail, FAX);
- Required duration of the access;
- What will be done with the accessed messages? With whom will they be shared?

2. Who should be able to request access? Who should be able to approve requests? Possibilities include:

- Department chairpersons and unit directors should be able to request access;
- Deans or vice chancellors should be able to approve requests.

3. Who needs to be informed when a request is approved to implement the access? The approved request must be routed to those people who should keep a copy of the request.

4. What advice or reminders should be given to the person requesting the access? Possibilities include:

- A reminder that concerns about fiscal misconduct or criminal activity should not be investigated by individuals or departments but should be referred to University police or internal audit staff in accordance with the University administrative policy titled "Reporting Fiscal Misconduct."
- A reminder that the contents of electronic communications obtained after appropriate authorization may be disclosed without the permission of the employee. At the same time, the University will attempt to refrain from disclosure of particular messages if disclosure could create personal embarrassment, unless such disclosure is required to serve a business purpose or satisfy a legal obligation.

Attachment II: Statement on E-mail Privacy and Ethics

Electronic mail, or e-mail, is a very useful tool for doing your University work. But you need to understand the nature of e-mail and use it wisely to avoid unpleasant consequences. Please read the following facts and tips about e-mail before you send your next e-mail message.

I. Privacy

A. The Facts of E-mail Privacy – E-mail is not exactly like a phone call. More information, including copies of the content of your messages, is routinely recorded about your use of e-mail than about your use of the telephone. Moreover, a broader, less controlled set of people have access to that information. E-mail is not like a letter in an envelope. The contents of your message are out in the open, and there's no easy way to mark a message "confidential." E-mail is most like a postcard. The contents of your message may be viewed during the mailing process. If it is inadequately addressed, or if there is a problem with routing equipment, a "postmaster" may read your message to try to redirect it correctly. Your message may be delivered to the wrong address. Your message can be forwarded or printed. Your message will probably be stored, perhaps in your directories, perhaps in the directories of the person who receives the message, and probably on system back-up tapes, which may be retained for very long periods of time.

We suggest you keep this "picture" of e-mail in mind as you compose e-mail messages. Don't put anything in an e-mail message that you wouldn't want posted on a bulletin board or used in a lawsuit or shared with the wrong person. Do use professional, courteous language that will not embarrass you later. People who may never meet you will be forming impressions about you based on the way you compose your e-mail messages. It's much easier to edit a message before you send it than to send an apology later. If you receive mail that obviously was not intended for you, send a reply to the sender notifying them that they need to revise the address.

The technology of the University's e-mail systems is constantly being upgraded. Over time, the technical ability to ensure privacy of e-mail communication will increase. But it is best to assume that e-mail is a public medium and to avoid using it for confidential communication.

B. The Policy of the University: The University has formally adopted a policy regarding use of the University's electronic communications resources, which includes electronic mail. You need to be aware of this policy as you use any of the electronic communications resources.

II. Ethics

The University's e-mail systems are developed and maintained to accomplish the work of the University. You should use them for academic pursuits and University-related administrative tasks, abiding by all applicable guidelines and policies. Naturally, you may want to use e-mail for personal communication that is not directly related to your role at the University. A minimal amount of such use is acceptable. Use good judgment and limit the amount and frequency of such use. Never use University e-mail systems for personal gain. Help conserve e-mail resources. If you flood the system with trivia, it won't be available for other more

(Continued on next page)

University E-mail Policy

(Continued from page 7)

worthwhile uses. Never send junk mail, random mail, or "Who are you?" messages.

Limit your use of lists as much as possible: Many of the global e-mail lists are available in other forms, Network News, Gopher, etc., and using those other means of accessing lists will require fewer computer resources than subscribing to a list. If you subscribe to a list, always make sure that you know how to unsubscribe from that list, and do so when you no longer have a use for the information from the list, or when you are ready to stop using e-mail at the University. Be careful when sending to e-mail lists. Sending large messages to lists that may have hundreds of users can dramatically impact both the e-mail system you are using to send the message and the e-mail systems receiving the message. Before sending to any list or replying to any message from a list, make sure that you know the guidelines and policies of that list and that you are aware of where your message is going (to the whole list, or just the person that sent the original message). Let integrity and honesty guide your use of e-mail and it will be an effective, useful tool for your work at the University. ◆

Brown Bag Seminars

Turn your lunch hour into a chance to learn more about the computing environment at UCB. All Brown Bags are scheduled from noon until 1 p.m. in the UMC, Room 235. No registration is necessary; feel free to drop by and bring your lunch.

Introduction to Electronic Mail

Tuesday, March 12, UMC 235

This seminar will provide new users with an introduction to e-mail. Topics covered will be methods of sending and receiving e-mail, electronic mail addresses, and how to get help.

Making Web Pages at UCB

Tuesday, March 19, UMC 235

For those who would like to create or edit their own Web home pages, this presentation explains the most basic steps, from getting the necessary Unix computer account to learning HTML.

Introduction to Pine

Tuesday, April 2, UMC 235

This Brown Bag seminar will cover a range of features in Pine including the basics of composing a message; organizing your saved mail messages; tips and tricks for using Pine more efficiently; and using the address book.

An Introduction to the Internet

Tuesday, April 16, UMC 235

If you're curious about the Internet and want to know how to get started, attend this session. The Internet has many services for education, business, and recreation. This Brown Bag will describe the Internet, discuss ways to connect, and demonstrate some of the more popular services. Bring your questions!

An Introduction to the World Wide Web

Wednesday, April 17, UMC 235

Would you like to find out how to access the wealth of information on the World Wide Web? This Brown Bag will show you how. We will explore techniques for finding information on the Web via popular browsers such as Netscape and Lynx. We will also cover some background information on the basics of browser/server interaction, and current concerns such as security, controversial content, and privacy. ◆

UNIVERSITY OF ILLINOIS
AT URBANA-CHAMPAIGN

CAMPUS ADMINISTRATIVE MANUAL
Public Relations, Records and Information
Section III - 18

Date Issued: May 20, 1993
Approved by: Vice Chancellor for Administration and Human Resources

ELECTRONIC MAIL ADVISORY

> Electronic mail documents in public files are protected by the same laws and policies and are subject to the same limitations as communications in other media.

The University of Illinois at Urbana-Champaign participates in a range of computing networks and many members of the community also regularly use computers in their work. Statements in public files in this medium are protected by the same laws and policies and are subject to the same limitations as communications in other media. The same holds true for electronic personal files and communications.

However, users should exercise caution when committing confidential information to electronic media because the confidentiality of such material cannot be guaranteed. For example, routine maintenance or system administration of a computer may result in the contents of files and communications being seen.

Also, under the Illinois Freedom of Information Act, electronic files are treated in the same way as paper files. The documents in the files of employees of the State of Illinois are considered to be public documents, and may be subject to inspection through FOIA. In such cases, the campus Freedom of Information Officer must inspect files to determine which portions may be exempt from disclosure.

Network and system administrators are expected to treat the contents of electronic files as private and confidential. Any inspection of electronic files, and any action based upon such inspection, will be governed by all applicable U. S. and Illinois laws and by University policies.

A network or system administrator who is unsure about how to deal with questions about the content of computer files or access to such files should contact George F. Badger, Associate Vice Chancellor for Computing and Communications, at 333-4103 (e-mail: g-badger@uiuc.edu).

SPEC
SYSTEMS AND PROCEDURES EXCHANGE CENTER

WWW POLICIES

ASSOCIATION OF RESEARCH LIBRARIES OFFICE OF MANAGEMENT SERVICES

Draft document

UCI WWW Style Guide

University of California, Irvine

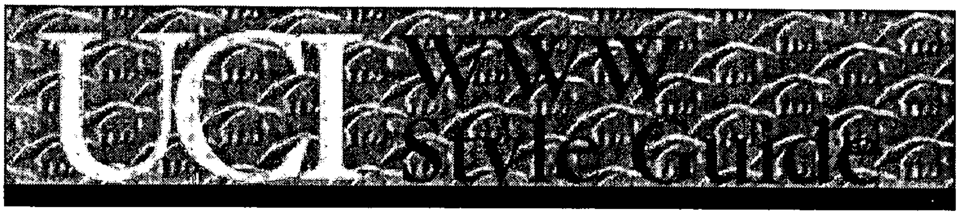
WWW Publications Guide

Table of Contents

Robert Daly
Director, Analytical Studies and Information Management
Comments to the author: bobdaly@uci.edu

Revised: June 28, 1995

Draft document

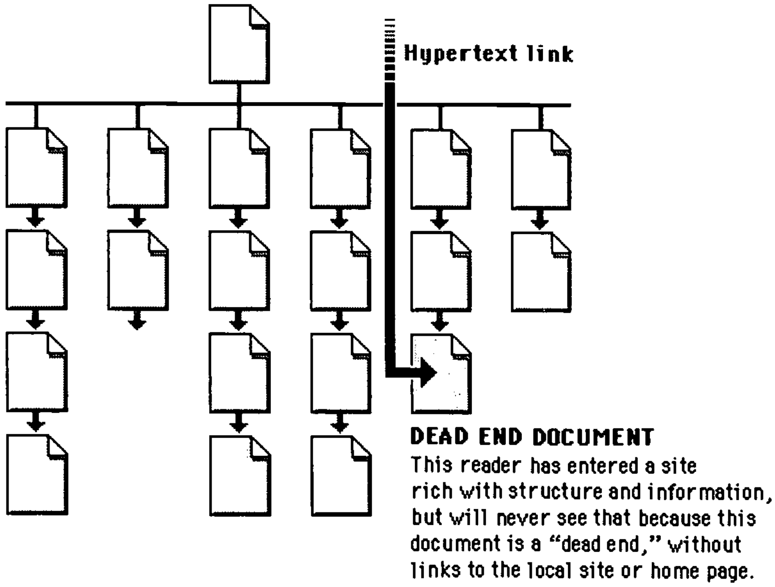


University of California, Irvine WWW Publications Guide

Page Identification

The footer area, at the bottom of WWW pages, are extremely important in identifying the origin, authorship, legal status, and last revision date of the page, and are often the best place to locate local links to the UCI and your local home page.

Links Are Essential
World Wide Web hypertext links are powerful things, but they can also confuse the reader and obscure the origin of linked pages. The power of WWW systems, where you can link directly to any single page in any Web system on the Internet, is a potential problem unless there is clear information about who wrote the page, where it came from, and on the legal status of the text and graphic content of the page. WWW users often link directly into documents several levels below the home page of a Web site:



DEAD END DOCUMENT
This reader has entered a site rich with structure and information, but will never see that because this document is a "dead end," without links to the local site or home page.

WWW designers often forget that links within a Web site must be **bi-directional**, allowing the reader to move up to the home page or major menu pages of a site as well as downward through chains of linked documents. If the links only flow downward away from the home page, most documents in your web will become dead ends.

Recomended page identification elements for UCI's WWW pages include:

Author's name
Author's institutional affiliation (if any)
Copyright marks and language, copyright year.

Last revision date of the page.
Official mark to signal UCI affiliation and authenticity or language designating the page as an official communication of UCI.
Author's e-mail address.
Author's mailing address.

UCI Home | Up | Feed Back

Robert Daly
Director, Analytical Studies and Information Management
Comments to the author: bobdaly@uci.edu

Revised: October 12, 1995

Draft document

UCI WWW Style Guide

University of California, Irvine WWW Publications Guide

Using the Official UC Seal and UCI Logo

The use of the unofficial UC seal in UCI web documents requires the approval of the Chancellor's office. The applicable policy is in the UCI Policy and Procedures Manual in Section 103. Choose Wais search and search on "seal." Section C is the appropriate section, and it is reproduced below:

C. UNOFFICIAL UNIVERSITY SEAL

1. Use of Unofficial University Seal-UCI Application

> a. Use of the unofficial University seal as a symbol of the University for any official UCI-related purpose or in connection with UCI alumni, student, or public project must be approved by the Office of the Chancellor.
> b. The two versions of the unofficial seal which may be used on printed matter are shown in image 700-02A. The seal must be used alone; it may not be incorporated with other symbols in a logo.
>
> c. Approval to use the seal must be granted prior to initiating an order to reproduce it.
>
> d. To obtain approval to use the unofficial University seal:
>
> Address an e-mail message to the Office of the Chancellor explaining the proposed use of the seal and, when possible, include a copy of the material on which the seal is to be used.

UCI Home | Up | Feed Back

Robert Daly
Director, Analytical Studies and Information Management
Comments to the author: bobdaly@uci.edu

Revised: December 20, 1995

Policy for the Electronic Publication of Official UCI Information

University of California, Irvine

Reason for Policy

The quality of information published by the University of California, Irvine plays an important role in determining its reputation and image. The policy presented here has been developed to ensure that official UCI information published electronically (via the Internet--WWW, Web, Gopher, etc.) is (1) correctly representative of UCI and the University of California; (2) accurate, well-written, and visually appealing; and (3) on par with the same high standards as other official publications which appear in print or other formats (audiovisual, etc.).

Definitions

Electronic Publication: An electronic publication is any document that is stored in any electronic device and transmitted via any electronic method, currently such as the World Wide Web (WWW), FTP, or Gopher.

Official UCI Publications: Official UCI publications are those published by academic and administrative units that

1. Present or represent UCI's official academic and/or administrative programs, plans, and/or policies.
2. Present or represent policies of the Regents of the University of California.

WWW (Web) Page: A WWW (Web) page is defined as one HTML file.

Scope of Policy

The policy presented here relates to official UCI publications disseminated electronically via any computerized or electronically oriented method.

Responsibilities

It is the responsibility of the designated representatives in academic and administrative units to ensure that all information in their unit's official electronic publications are accurate and current. Representatives are designated by the vice chancellor, dean, director, or head of each unit and work with the University Editor to ensure the represenativeness and accuracy of the proposed electronic publication.

Policy Statement

Contents of official electronic publications must follow University standards regarding nondiscrimination and copyright. Official electronic publications may not contain or link to electronic documents which contain offensive material. Any official UCI electronic publication which itself contains no offensive information is considered offensive if it links to an electronic document which does contain offensive material.

All official electronic publications must clearly state their affiliation with UCI -- either the UCI logo/wordmark or the full name, "University of California, Irvine." The affiliation must appear on each official electronic publication. In addition, each official WWW page must include a graphic insignia or the text "Official UCI Information ‹ Click to Verify." These signify that the publication is approved and registered as an official UCI document. The graphic insignia may be obtained from Analytical Studies and Information Management (oasim@uci.edu), which also administers and maintains the registry of official campus WWW pages.

Policy for Personal WWW Pages

UCI encourages the concept of faculty, staff, and students creating personal WWW pages that provide information relevant to the individual's role at the University. However, faculty, staff, and students may not use UCI resources to create personal WWW pages for personal business or personal gain, except as permitted by other University policies.

Official UCI WWW pages (and other electronic publications), as defined above, may be linked to UCI-related personal WWW pages but will not be linked to non-UCI-related personal pages. All administrative and academic units which publish links to faculty, staff, or student personal WWW pages must, when requested by a designated representative as defined under "Responsibilities," either deactivate links in those pages or they must remove those pages from University-owned computing equipment.

Review and Approval

The URL (e.g., http://www. .....) of the final drafts of the proposed document should be e-mail to the University Editor (uniedit@uci.edu) for review and approval to publish.

The University Editor is authorized on behalf of the Executive Vice Chancellor to ensure that all official UCI publications adequately and appropriately reflect UCI's programs, plans, and policies. The University Editor has final authority for approving the publication of official electronic (and print) documents and for certifying those documents as official.

Academic and administrative unit representatives who want eletronic documents published on the primary campus Web server, www.uci.edu, or who want link(s) established from Web pages on the primary campus Web server to other pages or information resources for which they are responsible, should contact the Office of Analytical Studies and Information Management (oasim@uci.edu).

Revised: July 12, 1996

UCI Home Feed Back

OFFICIAL UCI INFORMATION
CLICK TO VERIFY

Indiana University

Publishing with World Wide Web

How You Can Deliver Information via WWW

You have a variety of options for making information available via WWW, from creating a personal homepage to developing a complete publication environment on our central server or on your own computer. The selections below describe the services UCS offers for each of these options. You may want to look at Which one of these options is right for me?

- □ Publishing on the central UCS WWW Server"
- □ Running Your Own WWW Server
- □ Creating a Personal WWW Homepage

Installing access to your information

Find out how to get pointers to your information installed in the central environment.

General WWW information

An introduction to WWW

Access general information about WWW, including Frequently Asked Questions about WWW.

Learning about HTML (Hypertext Markup Language)

Find out how to use HTML to markup your documents for WWW. Also see A Beginner's Guide to URLs which describes how how to write URLs (Uniform Resource Locators), the pointers you include in your HTML documents to provide access to other files.

WWW Publication Support Tools

Many tools have been developed to help in creating HTML including HTML editors, wordprocessing macros, and tools which convert from various file formats to HTML.

WWW Advanced Features

Learn about advanced WWW features, including the creation of forms, common gateway interface applications and graphical information maps.

Indiana University - Bloomington
LIBRARIES

IUB Libraries World Wide Web Information Providers Rights and Responsibilities

The IUB Libraries WWW Implementation Committees invite interested library units to participate in the development of the IUB Libraries WWW. The IUB Libraries WWW will be the primary "window" to IUB Libraries electronic services and internet resources for faculty, students and staff of Indiana University, and for scholars and researchers worldwide. It will also develop as an important tool for internal staff communications. We believe that the IUB Libraries WWW will be truly useful only if librarians and staff from throughout the libraries contribute their creativity and expertise to it.

As a foundation on which to build WWW applications throughout the IUB Libraries, ERSD (Electronic Resources and Services Department) and the IUB Libraries WWW Implementation Committees are developing and maintaining central WWW home pages for the IUB Libraries, and will provide training and support for IUB Libraries units to design and maintain their home pages. As library units become interested in becoming Information Providers with their own home pages, ERSD will manage accounts, provide initial training and ongoing support, and provide a centrally-managed IUB Libraries homepage and links to common library resources such as IUCAT.

The following "Rights and Responsibilities" are intended to ensure a useful web environment for users across disciplines, and to support and encourage IUB Libraries units to become WWW Information Providers.

IUB LIBRARIES INFORMATION PROVIDERS: RIGHTS

1. Information Providers will receive accounts, computer storage space, technical support and training, and design consultation as needed.

2. Information Providers will control the design, content and presentation of information contained in their Web site, within the contraints of the IUB Libraries WWW standards and guidelines.

IUB LIBRARIES INFORMATION PROVIDERS: RESPONSIBILITIES

1. All IUB Libraries home pages:
   - A. bear the "IUB Libraries" banner at the top left of the page:
   - B. are dated:
   - C. include a comment facility:
   - D. point back to the IUB Libraries home page.

All IUB Libraries pages:
   - A. include a meaningful title in the html <title> field of the header.

2. Information Providers are defined as IUB Libraries units, (departments or other formal organizational entities.) Department heads who receive an IUB Libraries WWW account accept responsibility for the creation and ongoing maintenance of the information contained in their Web pages, even if development is actually accomplished through the efforts of one or more individuals in the unit.

3. Information Providers are responsible for seeing that the information in their pages is consistent with the goals of the IUB Libraries WWW: (1) to provide information in support of research and instruction to faculty, staff and students of Indiana University Bloomington, and to scholars worldwide, and (2) to facilitate internal communications for IUB Libraries' faculty and staff. Home pages describing personal interests of individuals should be developed in the place provided by UCS for that purpose.

4. Information Providers are also responsible for understanding that the information they put in their pages will be read by many different constituencies and groups. Information that may be completely accurate, appropriate, and useful for a particular group of users may sometimes result in questions or unintentional controversy when viewed by users with different perspectives. The WWW Steering Committee will work with Information Providers to ensure that information that appears in IUB Libraries WWW is consistent with the general goals and statements of the IUB Libraries as an institution.

Julie Bobay and Carolyn Sherayko, ERSD (Electronic Resources and Services)

To ERSD Home Page

Last updated: 25 May 1995
URL: http://www.indiana.edu/~libcbrst/rights.html
Comments: bobay@indiana.edu

Indiana University - Bloomington
LIBRARIES

Standards & Guidelines for IUB WWW Information Providers

Standards (required)

All IUB Libraries home pages:
A. bear the "IUB Libraries" banner at the top left of the page;
B. are dated;
C. include a comment facility;
D. point back to the IUB Libraries home page.

All IUB Libraries pages:
A. include a meaningful title in the html <title> field of the header.

Guidelines (optional)

I. Page Layout

A. Header

<Title> Tag

Use a meaningful title as the title of your document

The title serves as a cue to help users to know where they are. In Lynx the title is displayed in the upper-right of the screen. In Netscape the title appears at the very top of the screen.

The information in the <title> tag becomes the bookmark entry when saved. Meaningful information here will make the bookmark more useful and easier to remember.
Title words are used by many web search engine to index documents.

Aim for consistency among the Libraries' pages.

Using standard language in the <title> tag can help present a unified feel to library web pages even though created by many different information providers.

Suggested text for the <title> tag: <title>IUB Libraries: ... </title>

B. Body

Headings

Use meaningful headings to introduce your document or sections of your document.

Each page you write should be able to stand alone, yet provide "location" or "context" cues for users. A page beginning with a heading such as "List" might not be helpful if the user arrived to it via a link from some other source.

Many search engines weight the relevance of the document retrieved based on words in the headings. Using descriptive headings take advantage of this feature.

C. Footer

Date

Include a date indicating when the page was last updated.

Feedback/Comments

It is important that users of our pages have a way to provide feedback and comments to the developer(s) of the page. A simple way to do this is within the footer with a "mailto" link.

Signature

A signature, either a personal name or a unit name is a good way to reflect the responsibility for the page and also acknowledge the creative effort of the developer(s).

Copyright

Include a copyright statement, if applicable.

IUB Standard Footer

The redesign committee for the Bloomington Campus homepage developed a standard footer which it recommends to information providers. It includes the basic information required by the IUB Libraries Standards & Guidelines and provides a basic copyright statement. The footer may be centered or flush left.

Standard footer:

Last updated:`day month four-digit year`
URL: http://www.indiana.edu/`your_directory`/`your_ filename`.html
Comments: `your_username`@indiana.edu
Copyright 1995, The Trustees of Indiana University

II. Navigation

Provide navigation links in addition to the "back" capabilities of the browser so that users may move around within your web pages easily.

Provide a link to point back to the IUB Libraries' Home Page.

If appropriate, also provide a link to the Libraries' "Behind the Scenes" home page.

III. Graphics/Images

Use the IUB Libraries' banner at the top left of your home page.

Use graphics or images that enhance the information content of your pages.

Keep in mind the length of time it takes to load multiple graphics or images.

Provide alternative text to describe graphics or images in text-based browsers or use the <img ....alt""...> attribute to suppress automatically supplied text.

IV. Permissions

Ask permission from the creator of the resource before using text, photographs or graphics from other web documents in your web pages.

In some graphics files, the creator will have given permission for the images to be used freely. In others the page creator may have indicated that the images have been gathered from all over the web and are displayed without regard to the protected status of the image. (Use these files with caution.)

Web Style Guide for Indiana University, Bloomington Campus

During the summer of 1995 a campus-wide committee met to redesign the Bloomington Campus homepage. A product of that effort was the Web Style Guide for Indiana University, Bloomington Campus which includes many good ideas for the design of web pages. When developing your pages you may want to consult this guide as well.

To ERSD Home Page

Last updated: 7 December 1995
URL: http://www.indiana.edu/~libcbrst/standard.html
Comments: lamoreau@indiana.edu

University of New Mexico

The University of New Mexico

Web Data Providers

The purpose of this document is to help UNM departments and organizations create World Wide Web presentations.

Table of Contents

Web page standards

When designing department home pages, the University of New Mexico requires five elements to link their home pages to the UNM Home Page;

- □ UNM must appear in the HTML Title tag.
- □ The words "University of New Mexico" must appear on the home page.
- □ The offical UNM logo must appear on the home page.
- □ A link back to the UNM home page must appear on the home page.
- □ A link to contact information for the department must appear on the home page. Include an e-mail address, phone number, fax number and U.S. postal address.

Return to table of contents

UNM Policies and U.S. Copyright laws

All college, department, or organization pages must adhere to the policies and copyright laws listed below;

- □ Like traditional departmental publications, Web pages must follow UNM design standards. Although still in revision, *The University of New Mexico Guide to Graphic Identification* can help designers plan Web pages. For more information contact the Publications office at 277-4957.
- □ The University of New Mexico Copyright, Fair Use and Patent Guidelines. To request a copy of this document contact the UNM Patent Administration Office at 277-7646.
- □ The U.S. Copyright Office
- □ The UNM Ethics Code and Policy for Computer Use.

Return to table of contents

Guidelines

- □ Review your work before placing it on-line. Ask co-workers to check for completeness and readability.

- Include a disclaimer on any personal home page listings. A standard disclaimer can be found on the UNM faculty and staff home page.
- Create pages that will function using both graphical browsers (e.g., Netscape) and text browsers (e.g., Lynx).

Return to table of contents

Creating a web presentation

- **Requirements**

  First, you will need a department computer account on CIRT's UNIX systems. The "Request for Departmental/Organizational CIRT Computer Account" document describes how to obtain such an account. For questions, contact the CIRT User Accounts office at 277-8131.

  Departments committing to a web presentation will need to designate a certain amount of resources to create and maintain the information offered on their pages. Information will need to be checked on a regular basis to ensure that it is current. Any links to other web locations will also need to be checked to ensure that they are still active.

  If disk space requirements for your web presentation exceed 12MB, the maximum allowed by CIRT, you will need to consider running your own WWW server. There are many WWW servers available, and they run on a wide variety of computer platforms including the PC and Macintosh. For more information, see Yahoo's list of WWW servers.

- **Learning HTML**

  Some knowledge of HyperText Markup Language (HTML) will be needed to create and maintain your department's web presentation. HTML is a collection of styles (indicated by markup tags) that define the various components of a World Wide Web document. Creating an HTML document can be done in an editor or word processing program by adding the HTML "tags" to the text and saving the file as text. HTML documents can also be created using HTML editors, which work like word processing software and create the tags for you. For files already created in a word processor, like WordPerfect, conversion programs are available on the Internet. For more information on editors and converters, see Yahoo's HTML Editor and HTML converter listings.

  Below is a collection of HTML resources:
  - A Beginner's Guide to HTML
  - The HTML Quick Reference Guide
  - HyperText Markup Language (HTML) Guide
  - WWW & HTML Developer's JumpStation
  - UNM Inline Image Collection

- **Creating pages on the UNM WWW server**
  - Setting up a WWW Home Page on the UNM WWW Server
  - Creating a home page with webgen, UNM's automated page generator.

Return to table of contents

Registering University college, department and organization web pages

Departments, colleges and organizations

To have your page added to the UNM Home Page, send a memo or e-mail message to the CIRT Unix Coordinator. Memos must be signed by the dean, director or chair. E-mail must be sent by the dean, director or chair to ucoord@unm.edu. Include in the memo or e-mail where you would like the link to your Web pages placed, and the address of the Web pages. Select a destination for the Web page from the following six categories from the UNM Web page:

□ Welcome
□ Student Info
□ Colleges and Schools
□ Research
□ Libraries
□ Campus Services

After you submit your registration request it will be processed by the UNM Webmaster at CIRT. You will receive a reply when the link has been created.

Student Organizations

For University-recognized student organizations, the faculty or staff sponsor must send a memo or e-mail message to the CIRT Unix Coordinator agreeing to the linking of the organization's page. E-mail messages must be sent by the faculty or staff sponsor to ucoord@unm.edu.

Faculty and Staff Organizations

For University-recognized faculty and staff organization, the chair or president of the organization must send a memo or e-mail message agreeing to the linking of the organization's page. Official status of the organization will be determined from the University Secretary's office.

Ad-hoc Committees and Organizations

These entities may have a linked Web page if a department is willing so sponsor them. The sponsoring department must be acknowleged on the Web page, and a memo from the chair of the sponsoring department must be sent to the CIRT Unix Coordinator agreeing to linking the organization's page to UNM's page.

Return to table of contents

The University of New Mexico
Albuquerque, New Mexico, USA

Comments to webmaster@unm.edu

SPEC
SYSTEMS AND PROCEDURES EXCHANGE CENTER

LIBRARY POLICIES

CANCOPY at the University of Alberta:

Copyright Information for Faculty, Staff and Students

□ *Copying right*
A simplified guide to copyright, fair dealing and collective licensing (September 1994)
□ *A Guide to Copying at the University of Alberta under the CANCOPY License*

□ Canadian Copyright Licensing Agency (CANCOPY) Home Page
□ Canadian Information Policy Resources (IFLA)

Information on Copyright Worldwide

□ Copyright and Intellectual Property Resources
□ Copyright and Universities: WWW and Gopher Sites
□ Intellectual Property Web Sites (Copyright Management Center)

U of A Library Home Page

Author: Susan.Stein@ualberta.ca
Last update March 12, 1996
URL: http://www.library.ualberta.ca/library html/copyright.html

University of California, Riverside
University Library

PERSONNEL ADMINISTRATION MEMORANDUM NO. 1.1

Issued: January 1983
Revised: August 1993

USE OF ELECTRONIC INFORMATION SYSTEMS

The purpose of this memorandum is to make Library employees aware of their obligations and responsibilities in the use of electronic information systems. Electronic information systems include all data bases, both internal (such as CLSI, INNOVACQ, etc.) and external (such as OCLC, MELVYL, etc.), electronic mail systems (such as bitnet and internet), GOPHER and other Campus Wide Information Systems (CWIS), CD-Rom Systems, and Library Local Area Networks.

Library employees authorized to use electronic information systems are entrusted with the responsibility to use them for library purposes and to protect the integrity of these systems. Because the Library contributes to national and University databases on which libraries throughout the country depend, it is of critical importance that data input to these databases is accurate and correct.

At the UCR Library, it is a condition of employment that electronic information systems not be misused. Willful violation of the use, accuracy, or integrity of electronic information systems or the deliberate input of misinformation is a violation of Library policy and constitutes misconduct. Such misconduct may result in the employee receiving corrective action, including investigatory leave, suspension without pay, or dismissal, depending on the nature of the offense. Furthermore, under existing California state law, any person who maliciously accesses, alters, deletes, damages, or destroys any computer system, network, computer program, or data is guilty of a felony.

In order to protect the integrity of electronic information systems, the library employee is expected to:

1. Keep confidential any assigned passwords and not reveal them to any unauthorized person.

2. Be responsible for all information entered by the employee under his or her logon ID.

3. Input data accurately and correctly to the best of his or her ability.

4. Maintain proper physical security of the systems for which he or she has responsibility.

5. Use electronic information systems only for legitimate University business for which he or she is authorized.

6. Keep confidential any information which is so designated, and only disclose it under proper authorization.

7. Report any suspected security violations to the appropriate supervisor, department head, and or division head.

As part of the orientation process, new library employees will be given a copy of this memorandum and asked to sign it. The signed copy will be filed in the employee's personnel file.

By signing below, the employee indicates that he or she has read and understood this memorandum, and agrees to abide by the polices stated above.

______________________________ Signature

______________ Date

University of California, San Diego
COMPUTER SECURITY AND USE STATEMENT
The University Library

Employee Name ______________________ Employee Number ___________

I have been informed that, in the performance of my duties in the University Library, University-provided computer hardware, software, data files, and networks are the property of or licensed to the Regents of the University of California, and are to be used solely for official University Business. I have reviewed and understand the *Rules of Conduct for University Employees Involved with Information Regarding Individuals* on the reverse side of this agreement.

I have been informed that my intentional and unauthorized disclosure of personal/confidential information is an invasion of privacy and may result in disciplinary, civil and/or criminal actions against me.

I also understand that it is against University policy to seek out or use university records including, but not limited to, personal/confidential information relating to others for my personal interest or advantage.

I have been informed that under existing California State Law any person who maliciously accesses, alters, deletes, damages or destroys any computer system, network, computer program, or data shall be guilty of a felony.

I am advised that my account and password constitute my signature and I will be responsible for all entries made under my account. I also understand that either use of another person's account and password, or the delegation of my account and password to another person, would not absolve me of responsibility for actions taken under that account and password. Delegation of my account and password for the sole purpose of electronic mail retrieval may be made upon prior approval of my supervisor.

I am aware that the References on the reverse side include, but may not specify all, the computer use standards, policies, rules and procedures and State and Federal laws which I am governed by.

I am advised that failure to comply with these policies, rules and regulations may result in disciplinary action, up to and including dismissal. Any violation of local, state or federal laws may carry the additional consequence of prosecution under the law, where judicial action may result in specific fines or imprisonment, or both; plus the costs of litigation or the payment of damages or both; or all.

Date ____________ Signature ________________________________

COMPUTER SECURITY AND USE STATEMENT

DEFINITION FOR CLASSIFICATION OF RECORDS

A. PERSONAL INFORMATION

Home Telephone Number
Social Security Number
Home Address
Employee Evaluations
Employee Medical Records

B. NONPERSONAL INFORMATION

Employee Name
Campus Address
Campus Telephone Number
Library Card Catalog

NOTE:
These are only examples of the information that constitute these types of records. This should not be construed as a comprehensive or complete itemization of records that are included in the above categories.

RELATED POLICIES/COLLECTIVE BARGAINING AGREEMENTS

1. POLICY AND PROCEDURE MANUAL (PPM)

A. 150-15 Protection of Human Subjects
B. 160-2 Disclosure of Information from Student Records
C. 230-11 Maintenance of, Access to, and Opportunity to Request Amendment of Academic Personnel Records
D. 230-29 Policies and Procedures to Assure Fairness in the Academic Personnel Review Process
E. 480 University Policy Regarding Records, Access and Disclosure

2. POLICY & PROCEDURE MANUAL/STAFF PERSONNEL MANUAL (PPM/SPM)

A. 250-605 Staff Employee Personnel Records
B. 250-605 (L-1) Staff Employee Personnel Records

3. COLLECTIVE BARGAINING AGREEMENTS

RULES OF CONDUCT FOR UNIVERSITY EMPLOYEES INVOLVED WITH INFORMATION REGARDING INDIVIDUALS

A. Employees responsible for the collection, maintenance, use and dissemination of information about individuals which relates to their personal life, including their employment and medical history, financial transactions, marital status and dependents, shall comply with the State of California Information Practices Act, PPM 480-3 Privacy of Access to Information, Legal Requirements and Implementing procedures, shall be used as a basic source of guideline in administering the Act's provisions.

B. Employees shall not require individuals to disclose personal information which is not necessary and relevant to the purposes of the University or to the particular function for which the employee is responsible.

C. Employees shall make every reasonable effort to see that inquiries and requests relating to personal records of individuals are responded to quickly and without requiring the individual to unnecessarily repeat his or her inquiry to others. In other words, reasonable efforts will be made to place the responsibility on the Department for responding to the individual after his/her initial contact.

D. Employees shall assist individuals who seek information pertaining to themselves in making their inquiries sufficiently specific and descriptive so as to facilitate locating the records.

E. Employees shall respond to inquiries from individuals and requests from them to review, obtain copies of, amend, correct, or dispute their personal records in a courteous and business-like manner, and in accordance with PPM 480-3.

F. Employees shall not disclose personal and confidential information relating to individuals to unauthorized persons or entities. The intentional disclosure of such information to such persons may be cause for disciplinary action.

G. Employees shall not seek out or use personal or confidential information relating to others for their own interest or advantage. The intentional violation of this rule may cause disciplinary action.

H. Employees responsible for maintenance of personal and confidential records shall take all necessary precautions to assure that proper administrative, technical and physical safeguards are established and followed in order to protect the confidentiality of records containing personal information and to assure that such records are not disclosed to unauthorized individuals or entities.

INFOPATH MEMORANDUM OF UNDERSTANDING

This document is an agreement between the UCSD University Library and the campus department or organization specified below to provide an information resource through InfoPath, UCSD's Campuswide Information System.

The department or organization agrees to make its information resource available through InfoPath, to update the information on an agreed frequency, and to provide maintenance and user support for this information.

The department or organization understands the implications of making this information resource available through networked access and agrees to assume responsibility for ownership and sponsorship including compliance with Federal and State law and with University of California policies and regulations. The University Library is not liable for potential uses of this information resource.

The University Library reserves the right to remove access to the file or system through InfoPath without notice in the case of non-compliance with this agreement.

(Please Complete the following items)

NAME OF INFORMATION RESOURCE:
(Suggested name for InfoPath menu)

TECHNICAL CONTACT:
(Responsible for providing/updating the information resource)
Name and Title:
Department:
Mail Code:
Telephone:
Email address:

PUBLIC CONTACT:
(For users to contact with questions)
Name and Title:
Telephone:
Email address:

AUTHORIZED BY:

For the Provider
Department/Organization:
Name (Chair/Director):
Signature:
Date:

For the University Library
Director of Infopath Services:
Signature:
Date:

POLICY ON APPROPRIATE USE OF LIBRARIES COMPUTERS BY LIBRARIES PERSONNEL

Computers shall include hardware, software, and access to local and remote systems. Staff members shall include Libraries faculty, staff, and student employees. Staff members have the responsibility to make use of the Libraries computers in an effective, ethical, and legal manner.

Computers shall be used in a manner consistent with the objectives of the Libraries.

As a condition of use of Libraries facilities the staff member agrees:
To respect the intended purposes of Libraries computers.
To respect the privacy of other users.
To respect the integrity of the Libraries computers.

Staff members shall not intentionally seek information on, obtain copies of, or modify files, tapes, passwords, or any type of data belonging to other users unless specifically authorized to do so Staff members shall not develop or execute programs that could harass other users, infiltrate computer systems, or alter software component of the systems.

Software programs are protected by Section 117 of the 1976 Copyright Act. Unless they have written the program themselves, staff members do not have the right to make and distribute copies of programs without specific permission of the copyright holder.

Staff members shall not make copies of Libraries-owned software unless specifically authorized to do so.

Staff members shall not load personal copies of software on Libraries computers unless specifically authorized to do so.

Violations of these conditions may result in the suspension of computing privileges; disciplinary review; termination of employment; or legal action. The Libraries reserves the right to examine users' stored information when investigating cases of computing abuse.

The physical abuse of any computing equipment or supplies will be reported to the University Police and to the appropriate administrative office.

SPEC

SYSTEMS AND PROCEDURES EXCHANGE CENTER

INSTITUTIONAL POLICIES

ASSOCIATION OF RESEARCH LIBRARIES OFFICE OF MANAGEMENT SERVICES

University of Alberta

CNS Conditions of Use 20 September 1994

Computing and Network Services

The University of Alberta works to create an intellectual environment in which students, faculty, and staff may feel free to create and to collaborate with colleagues both at the University and at other institutions without fear that the products of their intellectual efforts will be violated, misrepresented, tampered, destroyed, or stolen. This intellectual environment is fostered by an atmosphere of trust and confidentiality that in part is encouraged by the computing environment that exists at the University.

Authority to Use

The information resources at the University of Alberta are for your use as a student, faculty, or staff member of the University. It is a policy of the University that these information resources be used by you respecting the public trust through which they have been provided and in accordance with policy and regulations established from time to time by the University and its operating units.

The University agrees to make reasonable effort to provide you with computing facilities appropriate to the tasks you have been asked to undertake, and that these facilities will be available as required. In return, you agree to use the facilities provided to you for the purposes they were intended, knowing that you are accountable for their use.

The computing facilities you use are provided for you by one of the University's teaching, administrative, or service units. In some cases you will be provided with a computer account on a University computer system, whereas in other cases you will be provided with access to facilities such as workstations or computing laboratories. You may be given access to the facilities as an individual or as part of a group, such as a class. Under any of these alternatives, your responsibilities and the University's responsibilities are the same.

The University reserves the right to withhold access to the computing facilities provided to you if there are reasonable grounds to suspect that your continued access to the facilities would pose a threat to the operation of the facilities or the good name of the University. Where there is substantiated abuse of computing privileges, the University will consider the removal of your access to facilities in balance between the threat perceived to the community and the inconvenience you will face. In the event that your access to any or all computing facilities is removed, the University will inform you of the options available to you to have that access reinstated.

Privacy

The University will treat your data and programs as both private and confidential and will not examine your information without just cause or due process, nor disclose that information to a third party unless it is for use in a disciplinary or criminal investigation.

The University will not normally monitor individual usage of any general computing facility, although all usage of a general facility may be monitored to enable accurate auditing. However, the University reserves the right to monitor and record the usage of any facility if threatening or abusive behavior has been reported and the University has the right to use information gained in this way in disciplinary or criminal proceedings.

To acknowledge the right of others to privacy, you agree to stay within the limits of your authorization to use the facilities provided for your use, to copy information only from pre-authorized sources, and never to delete or change information without permission from its holder.

Never consider electronic communications either private or secure. Remember that electronic mail messages can be saved indefinitely on the receiving computer, copies can be easily made and forwarded to others either electronically or on paper, and that messages sent to nonexisting or incorrect usernames are not returned directly to you but are delivered to a person designated as the Postmaster for either the remote or local site.

Ethical Use of Facilities

You will refrain from illegal activity, including software piracy or unauthorized profit-making activities using University resources.

You will be sensitive to the public nature of shared facilities and take care not to display on screens in such public locations images, sounds or messages which could create an atmosphere of discomfort of harassment for others. You will refrain from transmitting to others in any location inappropriate images, sounds or messages which might reasonably be considered harassing.

Electronic mail is a personal medium; it represents a conversation between you and another user. As such, the University will not attempt to monitor or regulate the content of your electronic mail. Notwithstanding this, within the broad context of free academic discussion and debate, communications between members of the University community are expected to reflect high ethical standards and mutual respect and civility. It makes no difference whether the communication medium is face-to-face oral exchange or a local or a national computer network. The use of obscene, racist or sexist language, for example, clearly violates the ethical standards of our University community and is as inappropriate for computer mediated communications as it is for other forms of University discourse.

Security and Integrity

The University is responsible for operating the computing facilities it provides in a manner that offers you and others security and integrity of computing.

The University reserves the right to inspect, copy, remove, or otherwise alter data files, system resources, or user files in the regular conduct of its duty to maintain efficient and well run computing facilities.

Entry into a system, including the network system, by individuals not specifically authorized shall be viewed as trespass. Attempts to circumvent the protective mechanisms of any University system shall be considered attempted theft or trespass. Deliberate attempts to degrade system performance or capability, or attempts to damage systems, software or intellectual property of others shall be viewed as criminal activity. Irresponsible use (that which needlessly affects the work of others) will be treated as a mischief.

Investigation of Abuses of Computing Privileges

System administrators of computing services have the responsibility to take remedial action in the case of possible abuse of computing privileges. Nothing in this policy diminishes that responsibility and system administrators, with the approval of their supervisor and with due regard for the right of your privacy and the confidentiality of your data, have the right to suspend or modify your computer access privileges, examine files, passwords, accounting information, printouts, tapes, and any other material which may aid in an investigation of possible abuse. Whenever possible, your cooperation and agreement will be sought in advance.

Investigation into suspected violation of this policy will be governed by the same regulations as other investigations on campus. For example, where academic offenses such as plagiarism or professional misconduct involve the use of computing facilities, the same faculty officers involved in a more traditional case will be involved in the computer based case with computer specialists likely being used as resources.

This policy has been drafted and approved under the authority of the Director of Computing and Network services. Any questions regarding the application or interpretation of these Conditions of Use should be directed to Computing and Network Services.

POLICIES

The Division of University Computing (DUC) provides central computing and networking services to Auburn University faculty, employees, and students on an IBM mainframe and a Sun SPARCcenter. DUC also operates several computing labs that contain PC and Macintosh microcomputers and Sun workstations.

Accessing the Computers

Access to the IBM mainframe and Sun workstations is authorized by means of computing accounts or userids. To obtain an account, faculty and employees must complete an Employee User ID Action Request form, available from the DUC Support Services office in 26 L Building or from their Computing Coordinator. Students have the option to activate their own DUC Sun and IBM mainframe accounts from any DUC computing lab or from the DUC Support Services office. Accounts are offered free of charge to all students and to qualified faculty and employees whose activities are funded by the AU general fund (for more information, see section on Funding). Accounts remain active as long as the person is employed by the University or enrolled in the current quarter. For more information about establishing an account, call the DUC Hotline at 844-5555.

Walk-in access to the PC and Macintosh microcomputers in the DUC computing labs is available to all University faculty, employees, and students.

DUC Computing Lab Reservations

The primary use of the DUC computing labs is for student walk-in instructional computing. While some labs may be reserved by University departments for instructional purposes, the hours available for reservation are limited. Departments and colleges with strong demands for instructional computing labs are urged to establish their own facilities to meet their own specialized needs. DUC computing labs may not be reserved for events that charge a registration fee that is not included in University tuition.

To reserve a DUC computing lab for instructional use, notify the Manager of DUC Computing Lab Support at least one week in advance. If the requested use of the lab involves the installation of software, the request should be made at least two weeks in advance.

If the use of a teaching lab requires the installation of discipline-specific software not currently available in the lab, the following policies apply:

1. The software must be installed by DUC personnel (the assistance of the requesting instructor may be required).
2. The software must be legal. It is the responsibility of the individual reserving the lab to obtain the correct number of legal copies or an appropriate site license.
3. The software must not conflict with any software on the DUC support list (i.e., if software on the DUC support list would serve the same purpose, alternative software will not be installed).
4. DUC will provide no instructional or technical support in the use of the software.

5. DUC reserves the right to refuse any request for software installation.

An instructor or individual who reserves a DUC computing lab is responsible for the lab during that time. All DUC rules and policies must be followed. No tobacco products, food, or drinks are permitted in DUC labs. For more information about the computing lab reservation policy, contact DUC Computing Lab Support at 844-9904.

Software Support

DUC supports a wide variety of software available on the PC and Macintosh microcomputers, the Sun workstations, and the IBM mainframe. There are two levels of support: Level I--Full Support and Level II--Minimal Support.

Software classified for Level I support is installed on DUC host computers and microcomputers, and maintained and upgraded by DUC personnel on a high priority basis. Full user services (general and expert consulting assistance, complete vendor and locally written documentation, introductory and advanced training, news announcements, and testing) are provided for these packages. Telephone and walk-in help for Level I software is available by dialing the DUC Hotline at 844-5555 or by coming to the DUC offices in 26 L Building. You may also e-mail questions to hotline@mail.auburn.edu.

Software at Level II is installed, maintained, and upgraded on DUC computers by DUC personnel and installed on departmental computers by the user. Limited user services (general consulting assistance, basic vendor documentation, brief writeups, and news announcements) are available from DUC.

The list of supported software and support levels for the Sun workstations and IBM mainframe can be found in the Computers section of this booklet.

Procedures have been defined within DUC to encourage user input in the process of establishing DUC supported software. The steps in this process include recommendations from users, testing of the software by DUC personnel, and evaluation of the software by DUC personnel in cooperation with the user. For more information about the procedures for adding a product to the supported software list, contact DUC at 844-5555.

Hardware Support

DUC supported products have been selected in order to provide users with high-quality computer services and pricing discounts. These products are also supported by the Digital Repair Facility (DRF) and the Division of Telecommunications and Educational Television (Telecom).

For a list of DUC supported microcomputers, see the SUPPORT writeup.

Data Set Maintenance and Backup Policy

IBM mainframe and Sun workstation users are responsible for maintaining backup copies of their data sets and files. DUC regularly backs up disk data sets on the host computers but keeps these backups for a limited time only. No one should depend upon this procedure for backup.

No backup is maintained for mainframe tape data sets. Irreplaceable data sets or those difficult and costly to re-create should be backed up by the user. See the writeup DMS for a description of disk data set maintenance procedures on the mainframe.

DUC provides and supports ADSM (Adstar Distributed Storage Manager), a backup utility that allows desktop computers to back up files to the University host system. An ADSM host account and access to the campus network is required. ADSM is a commercial product site-licensed from IBM and is available free of charge to anyone associated with Auburn University. For more information or suggestions about personal backup procedures, contact the DUC Hotline.

The microcomputers in the DUC computing labs are reformatted regularly, and any data saved to the hard drive will be lost. Users must save copies of their data files on floppy disk.

Funding

Use of DUC facilities is available to Auburn University faculty, employees, and students. Units and projects that are funded from sources other than the University's General Fund (such as direct state appropriation lines, auxiliary enterprises, and research contracts) are charged for use of DUC computing resources.

DUC is funded through the Auburn University main-campus general fund and provides computing and networking services for departments and activities funded by the University's general fund. Such services include computing done in ordinary University operations such as administration, instruction, and research not subsidized through a grant or contract.

DUC's budget is not intended to supply services to those whose work is not covered by the University's general fund. Departments, units, or individuals using DUC facilities for any computing activity not funded by the general fund must pay for computing services in hard dollars. Hard dollar users include units funded by a grant or contract (federal, state, local, or private), earmarked fees, other state line-item appropriations, gifts, donations and endowments, income from the sale of goods and services, income generated by auxiliary enterprises, indirect cost recoveries, and other external or private funding sources.

Each University department or division head must see that all of the unit's computing accounts are being used in accordance with this funding policy. The DUC form requesting a computing account requires the department head who signs it to provide an appropriate account number. This account number must be the correct funding source for the computing activity that the requested computing account will support; from this account number, DUC determines whether or not the computing account must pay for computing services with hard dollars. The department head's responsibilities include providing the appropriate account number for each computing account requested and insuring that all computing work is actually logged to the correct computing account. Compliance with this policy is subject to review by Internal Auditing.

Security and Ethics

DUC addresses the issues of computer security in part by assigning userids and passwords and by making regular backups of data sets, directories and files on its mainframe and workstations. However, the primary responsibility for computer security rests with the user. DUC recommends that users change passwords regularly and protect important data sets, files, or directories by assigning passwords to them. Anyone who believes that his or her userid has been illegally used or that their data sets, files, or directories have been illegally accessed should call the DUC Hotline (844-5555) immediately.

Computer userids and passwords enable users to access the mainframe and workstations provided by DUC. Any abusive activities initiated from an account are the responsibility of the account owner. Therefore, it is the policy of DUC that accounts are not to be shared. If users wish to share information or otherwise collaborate in a group, they should set the appropriate file permissions combined with appropriate group membership. Abuses and misuses of the computing facilities include attempting to destroy or modify another user's data sets, directories or files, attempting to modify the system or cause it to fail, and using a computing resource for purposes for which it was not intended such as game playing or unapproved private applications. Failure to comply with this policy may result in suspension of the user's account. Persons who seriously violate network security and otherwise misuse the computing facilities will have their accounts terminated, will be referred to the Discipline Committee (see Section II-A-2-f of the University's Code of Student Discipline), and may be held responsible under State and Federal laws.

Users should be aware that electronic mail is not private or secure although DUC does make an effort to ensure confidentiality. Electronic mail should not be used to transfer secure or confidential information.

Computer software and documentation are protected under the U.S. Copyright Act just as books and articles are protected; that is, copying such software is unlawful. Accordingly, the University prohibits the use of its equipment to make unauthorized copies of copyrighted software. The software in the DUC computing labs is to be used only in the labs; except where specifically allowed under the provision of a site license, copying it is prohibited.

For more information on Auburn University's computer security policy, see the DUC Network Policies and the Security Policy Manual.

Please send questions or comments to hotline@mail.auburn.edu.
Last modified: Wednesday, 12-Jun-96 11:20:58 CDT

University Directory

Return to AU Home Page

Computer and Network Use Policy

Revised June 16, 1995
http://www.ucdavis.edu/AUP.html

Part 1

I. Introduction
This acceptable use policy governs the use of computers and networks on the UC Davis campus. As a user of these resources, you are responsible for reading and understanding this document. This document protects the consumers of computing resources, computing hardware and networks, and system administrators.

II. Rights and Responsibilities
Computers and networks can provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. Such open access is a privilege and requires that individual users act responsibly. Users must respect the rights of other users, respect the integrity of the systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations. Since electronic information is volatile and easily reproduced, users must exercise care in acknowledging and respecting the work of others through strict adherence to software licensing agreements and copyright laws.

III. Existing Legal Context
All existing laws (federal and state) and University regulations and policies apply, including not only those laws and regulations that are specific to computers and networks, but also those that may apply generally to personal conduct.

Users do not own accounts on University computers, but are granted the privilege of exclusive use. Under the Electronic Communications Privacy Act of 1986 (Title 18 U.S.C. section 2510 et. seq.), users are entitled to privacy regarding information contained on these accounts. This act, however, allows system administrators or other University employees to access user files in the normal course of their employment when necessary to protect the integrity of computer systems or the rights or property of the University. For example, system administrators may examine or make copies of files that are suspected of misuse or that have been corrupted or damaged. User files may be subject to search by law enforcement agencies under court order if such files contain information which may be used as evidence in a court of law. In addition, student files on University computer facilities are considered "educational records" under the Family Educational Rights and Privacy Act of 1974 (Title 20 U.S.C. section1232[g]).

Misuse of computing, networking or information resources may result in the loss of computing and/or network access. Additionally, misuse can be prosecuted under applicable statutes. Users may be held accountable for their conduct under any applicable University or campus policies, procedures, or collective bargaining agreements. Illegal production of software and other intellectual property protected by U.S. copyright law is subject to civil damages and criminal punishment including fines and imprisonment. The Davis campus of the University of California supports the policy of EDUCOM on "Software and Intellectual Rights."

Other organizations operating computing and network facilities that are reachable via the UC Davis network may have their own policies governing the use of those resources. When accessing remote resources from UC Davis facilities, users are responsible for obeying both the policies set forth in this document and the policies of the other organizations.

IV. Enforcement
Minor infractions of this policy, when accidental, such as consuming excessive resources or overloading computer systems, are generally resolved informally by the unit administering the accounts or network. This may be done through electronic mail or in-person discussion and education.

Repeated minor infractions or misconduct which is more serious may result in the temporary or permament loss of computer access privileges or the modification of those privileges. More serious violations include, but are not limited to unauthorized use of computer resources, attempts to steal passwords or data, unauthorized use or copying of licensed software, repeated harassment, or threatening behavior. In addition, offenders may be referred to the their sponsoring advisor, department, employer, or other appropriate University office for further action. If the individual is a student, the matter may be referred to the Office of Student Judicial Affairs for disciplinary action.

Any offense which violates local, state, or federal laws may result in the immediate loss of all University computing privileges and will be referred to appropriate University offices and/or law enforcement authorities.

Part 2

Conduct which violates this policy includes, but is not limited to the activities in the following list.

- □ Unauthorized use of a computer account.
- □ Using the Campus Network to gain unauthorized access to any computer systems.
- □ Connecting unauthorized equipment to the campus network.
- □ Unauthorized attempts to circumvent data protection schemes or uncover security loopholes. This includes creating and/or running programs that are designed to identify security loopholes and/or decrypt intentionally secure data.
- □ Knowingly or carelessly performing an act that will interfere with the normal operation of computers, terminals, peripherals, or networks.
- □ Knowingly or carelessly running or installing on any computer system or network, or giving to another user a program intended to damage or to place excessive load on a computer system or network. This includes, but is not limited to, programs known as computer viruses, Trojan Horses, and worms.
- □ Deliberately wasting/overloading computing resources, such as printing too many copies of a document.
- □ Violating terms of applicable software licensing agreements or copyright laws.
- □ Violating copyright laws and their fair use provisions through inappropriate reproduction or dissemination of copyrighted text, images, etc.
- □ Using university resources for commercial activity such as creating products or services for sale.
- □ Using electronic mail to harass or threaten others. This includes sending repeated, unwanted e-mail to another user.
- □ Initiating or propagating electronic chain letters.
- □ Inappropriate mass mailing. This includes multiple mailings to newsgroups, mailing lists, or individuals, e.g. "spamming," "flooding," or "bombing."

- □ Forging the identity of a user or machine in an electronic communication.
- □ Transmitting or reproducing materials that are slanderous or defamatory in nature, or that otherwise violate existing laws or university regulations.
- □ Displaying obscene, lewd, or sexually harassing images or text in a public computer facility or location that can be in view of others.
- □ Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.

It is the intention of the Joint Campus Committee on information technology in adopting this policy, that it should be reviewed annualy by a Subcommittee of the Joint Campus Committee on information technology. It is further our intention that this policy should be incorporated into the UCD Policy and Procedure Manual as soon as possible.

For further information refer to:

UC Davis Directive #90-108 "Principles of Community"
UC Davis Policy & Procedure Manual Section 210-70 "Copyright"
UC Davis Policy & Procedure Manual Section 280-05 "Prohibited Discrimination"
UC Davis Policy & Procedure Manual Section 320-20 "Privacy and Access to Information"
UC Davis Policy & Procedure Manual Section 380-12 "Sexual Harassment"
UC Davis Code of Academic Conduct
University of California: Standards of Conduct for Students
UC Davis Administration of Student Discipline
The EDUCOM Code: Software and Intellectual Rights
Office of Student Judicial Affairs (463 MU, 752-1128)
Information Technology Campus Access Point (Shields Library, 752-2548)

UC DAVIS HOME SEARCH HELP

Questions or Comments

University of California-Irvine

COMPUTER USE POLICY

The University of California, Irvine (UCI) provides computing resources and worldwide network access to members of the UCI electronic community for legitimate academic and administrative pursuits to communicate, access knowledge, and retrieve and disseminate information. As members sharing these resources, we also share the rights and responsibilities of their use. This document describes the shared rights and responsibilities as well as the consequences of misuse. Please read it as YOU ARE RESPONSIBLE FOR KNOWING AND FOLLOWING THESE POLICIES. We welcome your use of campus computing resources and your cooperation.

Rights and Responsibilities

Worldwide, open access electronic communication is a privilege and continued access requires that users act responsibly. Users should be able to trust that the products of their intellectual efforts will be safe from violation, destruction, theft, or other abuse. As a users sharing computing resources, you must respect and value the rights and privacy of others, respect the integrity of the systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations. You are responsible to refrain from acts that waste resources, prevent others from using them, harm resources or information, or abuse other people. To help protect your files, you are responsible for setting passwords appropriately and keeping your password confidential by not giving it to another person.

Most UCI owned computers are under the control of a system administrator or lab manager. Like you, these administrators are expected to respect the privacy of computer system users. However, UCI computer system administrators may access user files or suspend services on the systems they manage without notice as required to protect the integrity of computer systems or to examine accounts that are suspected of unauthorized use, misuse, or have been corrupted or damaged. This includes temporarily locking vulnerable accounts, removing hung jobs, reprioritizing resource intensive jobs, etc.

Many UCI departments have their own computing and networking resources and policies. When accessing computing resources, users are responsible for obeying both the policies set forth in this general computing document and the policies of the other departments.

Examples of Misuse

Examples of misuse include, but are not limited to, the activities on the following list:

- □ Knowingly running or installing on any computer system or network, or giving to another user, a program intended solely for the purpose of damaging or placing excessive load on a computer system or network. This includes, but is not limited to, computer viruses, Trojan horses, worms, or password cracking programs.
- □ Attempting to circumvent data protection schemes or uncover security loopholes without prior written consent of the system administrator. This includes creating and/or running programs that are designed to identify security loopholes and/or intentionally decrypt secure data.
- □ Using computers or electronic mail to act abusively toward others or to provoke a violent reaction, such as stalking, acts of bigotry, threats of violence, or other hostile or intimidating "fighting words". Such words include those terms widely recognized to victimize or stigmatize individuals on the basis of race, ethnicity, religion, sex, sexual orientation, disability, etc.
- □ Posting on electronic bulletin boards materials that violate the University's codes of conduct. This includes posting on Internet services information that are slanderous or defamatory in nature or displaying graphically disturbing or sexually harassing images or text in a public computer facility

or location that are in view of other individuals.

- □ Attempting to monitor or tamper with another user's electronic communications or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.
- □ Violating terms of applicable software licensing agreements or copyright laws.
- □ Using the campus network to gain unauthorized access to any computer system.
- □ Using a computer account or obtaining a password that you are not authorized to use.
- □ Masking the identity of an account or machine. This includes sending mail that appears to come from someone else.
- □ Knowingly performing an act without authorization which will interfere with the normal operation of computers, terminals, peripherals, networks, or which will interfere with others' ability to make use of the resources.
- □ Using your account for any activity that is commercial in nature not related to your work at UCI, such as consulting services, typing services, developing software for sale, advertising products, and/or other commercial enterprises for personal financial gain.
- □ Deliberately wasting computing resources, such as playing games (MUDS, etc.) while someone else is waiting to use the computer for UCI related work, sending chain letters, treating the printer like a copy machine, storing or moving large files which could compromise system integrity or preclude other users right of access to disk storage, etc.

Consequences of Misuse

Misuse of computing, networking, or information is unacceptable, and users will be held accountable for their conduct. Serious infractions can result in temporary or permanent loss of computing and/or network privileges, student judicial affairs review and discipline, and/or Federal or State legal prosecution. California Penal Code Section 502 makes certain computer abuses a crime, (such as illegal reproduction of software protected by U. S. copyright law) and penalties can include a fine and/or imprisonment. Files may be subject to search under proper authorization.

Minor infractions of this policy, such as poorly chosen passwords, overloading systems, excessive disk space consumption, are typically handled internally to the department in an informal manner. More serious infractions such as abusive behavior, account invasion or destruction, attempting to circumvent system security, etc. are handled formally through the Dean of Students Office or by other appropriate officials.

Acknowledgements
This document has been adapted in part from the UCI ICS Department, UC Berkeley, and UC Davis computer use policies.

OAC Home Page

Updated: 31 JULY 1995
oac@uci.edu

Home Index

BUSINESS AND FINANCIAL AFFAIRS: Information Systems and Computers
SEC. 714-15: Policy on Access to University Information Systems

References:

State of California Information Practices Act of 1977 (IPA)

Business and Finance Bulletins:

RMP-7, Privacy of and Access to Information Responsibilities

RMP-8, Legal Requirements of Privacy of and Access to Information

RMP-9, Guidelines for Access to University Personnel Records by Government Agencies

Campus Policy and Procedures:

720-10, Information Access and Disclosure: Information from Public Records

720-11, Information Access and Disclosure: Privacy and Access to Information (Excluding Student Records)

720-14, Information Access and Disclosure: Use of Social Security Number

720-15, Information Access and Disclosure: Directories and Mailing Lists

A. Introduction

Administrative Computing Services (AdCom Services) is responsible for providing information to achieve departmental and campus administrative goals. Major systems responsibility includes payroll/personnel, purchasing, accounts payable, general ledger and associated financial systems. On-line access is available via individual desktop computers for most systems. Training is available on an ongoing basis.

B. Policies for Access

Access to the University's information systems and data is limited to those employees who have a demonstrated need for access based on their job duties. Department heads may request access to administrative information systems for individuals who report to them.

C. Data Privacy

Some of the data contained in the University's information systems may be defined as personal or confidential under the University's policy and the State of California Information Practices Act of 1977 (IPA).

The references to personal and confidential information in the Irvine Campus Policy and Procedures Manual are for the employee's information but may not specify all the computer use standards, the University's policy and procedures, and state and federal laws by which an employee is governed.

It is the responsibility of individual users to access and use data in accordance with the University's policy and the State of California Information Practices Act of 1977. For more specific information, refer to the references shown above or contact the Campus Information Practices Coordinator at 824-7500.

D. User's Responsibilities

Individual users certify understanding, and agree to adhere to Administrative Computing Services' policies by signing the Logon ID Request/Computer Security and Use Agreement. Specifically, an employee acknowledges an understanding of and agreement to adhere to the following:

- □ The logon ID is considered equivalent to a signature and the individual is responsible for all entries made under that logon ID.
- □ Updates to the system and changes in system data are to be made in a manner that is consistent with the University policies and

procedures that govern the particular action to be changed.

- Computing resources are to be used only for the legitimate University business that an employee has been explicitly authorized to perform as stated in his/her job description.
- It is against the University's policy to pursue or use the University's records including, but not limited to, confidential information for personal interest or advantage.
- Proper password security is to be maintained by not revealing passwords to anyone.
- Security is to be maintained by not providing anyone access to or use of the University's information systems maintained by AdCom Services.
- Proper physical security is to be maintained by not leaving a workstation/terminal unattended while logged in to the University's systems.
- The privacy and confidentiality of all accessible data is to be maintained and it is understood that unauthorized disclosure of personal/confidential information is an invasion of privacy and may result in disciplinary, civil and/or criminal actions against an individual.
- Suspected security violations will be reported to the AdCom Services.
- Under existing California state law, any person who maliciously accesses, alters, deletes, damages or destroys any computer system, network, computer program or data shall be guilty of a felony.
- References to personal and confidential information in the Campus Policy and Procedures Manual and the Computer Security and Use Agreement are for the employee's information but may not specify all computer use standards, University policy and procedures, and state and federal laws by which employees are governed.

Failure to comply with these policies, rules and regulations may result in disciplinary action, up to and including dismissal. Any violation of local, state or federal laws may carry the additional consequence of prosecution under the law, where judicial action may result in specific fines or imprisonment, or both; plus the costs of litigation or the payment of damages or both; or all.

The University will take the strongest actions possible in the case of any breach of these agreements.

E. Departmental Responsibilities

Access to the University's information systems is granted to employees with a demonstrable need for access. The employee's department head or delegate certifies that requested access is required for the employee's necessary and proper performance of assigned job duties. Departments authorize an individual's use of the University information systems maintained by AdCom Services by submitting the appropriate access forms.

Revised 7/96

Index Home Feed Back

University of California, Riverside

UCR POLICY AND PROCEDURES MANUAL POLICY/PROCEDURE NO: 400-30

DEPARTMENT: Computing & Communications SECTION NO: 400-30
SUBJECT: ACADEMIC COMPUTING DATE: September 15, 1994
PAGE: 1

A. OPEN ACCESS

The Academic Computing Open Access Policy, approved by the Academic Senate Committee on Computers, is designed to provide:

1. effective use of campus computing resources to support instruction and research
2. realistic access to students and faculty
3. a sound financial base for current operations and growth

Often these objectives must be balanced one against the other. Your suggestions may help to achieve a better balance. Changes will be subject to the final approval fo the Academic Seante Committee on Computers.

B. COMPUTER ACCOUNTS

All individuals who would like to use the AC computers must have a valid account number. Applications for account numbers are available at the C&C Administrative Office, 1626 Statistics - Computer Bldg. The following types of accounts are available (fiscal year allocation shown in parentheses):

1. Student Easy access for registered undergraduates ($150).
2. Instructional Accounts for faculty teaching a particular class with associated student sub-accounts ($125/student).
3. Undergraduate Special Studies or Undergrad Research (requires faculty approval/$1500).
4. Graduate Student Directed Research/Dissertation (requires faculty approval/$3000).
5. Faculty Research ($5000).
6. Staff ($600) (for e-mail, DEXlite & PRlite access).
7. Departmental Storage - large data sets
8. Hard dollar accounts funded by grants, general funds.
9. Outside user accounts (billed by sundry debtors).

Account allocations are issued for the entire fiscal year; prorated accordingly throughout the fiscal year. Individuals who exceed their limit (except student easy access accounts) may submit a request for additional funds. Requests for annual usage over $5000 must be approved by the Academic Senate Committee on Computers through C&C.

C. PASSWORD SECURITY

Passwords are the only protection that users have to insure their accounts are used only with their knowledge. C&C can at no time give out passwords or reset passwords via the telephone. The owner of the account must appear in person at the C&C office (1626 Stat/Comp) with proper ID to have their password reset. We apologize for any inconvenience this may cause. Clients may change their own password at any time and are encouraged to do so frequently to maintain security via the command *$set password*.

For additional questions regarding your account please contact Terri McDonald at the C&C office at x4741.

D. HARDWARE

C&C offers computer time on several computers under different operating systems. The computers available to academic users are: a VAXcluster consisting of a VAX 8820 and 6310, and an IBM 9121-210 (MVS).

The ACNET Ethernet network provides communications to AC timesharing services. Access is also available via dial-up modems to the Cisco terminal servers.

The VAXcluster has 21.7 Gigabytes (GB) of disk space and operates under VMS version 5.5. Connected to the VAXcluster are two CPUs:

> the VAX 8820 has 128 Mb of memory and a floating point accelerator;
> the VAX 6310 has 32 Mb of memory and a floating point accelerator.

All AC VAXes are connected to ACNET, the campus' local area Ethernet network, along with several DEC computers owned by other departments.

D. SOFTWARE

Since software costs are becoming a more significant part of computer center budgets, it is necessary that AC spend its resources (both monetary and personnel) as wisely as possible. Therefore, AC, with the support of the Academic Senate Committee on Computer, has adopted the following policy:

There are two distinct classes of software having different qualifications for acquisition, installation, maintenance, and consulting. Class-1 software will include all programs and packages that AC is obliged to support actively, while Class-2 software will encompass all programs and packages that have been installed on the AC computers, but are not fully supported.

E. SUPERCOMPUTING

UC Riverside is a member of the San Diego Supercomputer Consortium. The San Diego Supercomputer Center (SDSC), located on the UC San Diego campus, is administered and operated by GA Technologies, Inc. The SDSC consortium consists of 25 institutions including all UC campuses. Consortium sites use Remote User Access Centers (RUACs) and DECnet Communications to support remote login to the SDSC and other consortium RUACs for file transfer, electronic mail, and remote output queuing of print and graphics output from the SDSC.

The National Center for Supercomputing Applications (NCSA), located on the University of Illinois Urbana-Champaign (UIUC) campus, is administered by the NCSA Interdisciplinary Research Center. UCR is an affiliate member of NCSA and uses the Internet network (TELNET) for remote login.

F. CONSULTING

Academic Computing maintains an open-door policy of providing consulting assistance. However, clients should be aware that AC cannot maintain a large staff for consulting due to limited funds.

Walk-in consulting for brief questions is available in the Watkins Microcomputer Facility, Room 2103, from 10:00 a.m. - 12:00 noon and 1:00 p.m. - 3:00 p.m., Monday - Friday, during the academic year. Lab monitors are available at the Watkins Microcomputer Facility and the GSM Microcomputer Facility all hours the facilities are open to help with general questions.

The faculty hot-line, 787-HELP (4357), is available for immediate response from an AC staff member. More in-depth consulting is available to students, faculty, and staff by making an appointment at (787) 4744. The user may be charged for this service, depending on the subject and length of the contact.

An AC consultant will provide at faculty request, a workshop to department faculty, graduate students or in-class lecture. Potential topics include operating systems, languages, or statistical packages. AC staff are willing to work with faculty to develop a specific computer-related class handout. If you are interested in a specific topic for a lecture or handout, please contact Alex Ramirez at (787-) 4705. A minimum notice of two weeks is required.

SECTION - 1

GUIDELINES FOR ACCESS TO UNIVERSITY INFORMATION SYSTEMS

A. **INTRODUCTION**
Using the IBM and VAX mainframe computers, Computing & Communications is responsible for providing certain information to achieve departmental and campus administrative goals. Major systems responsibilities include payroll/personnel, general ledger, purchasing, accounts payable, and student information. Access is available via individual workstations/terminals for most systems.

B. **GUIDELINES FOR ACCESS**
Access to the University's information systems and data is limited to those employees who have a demonstrated need for access based on their job duties. Department heads may request access to administrative information systems for individuals who report to them.

C. **DATA PRIVACY**
Some of the data contained in the University's information systems may be defined as personal or confidential under the University's policies and the State of California Information Practices Act of 1977 (IPA).

The references to personal and confidential information in the Riverside Campus Policies and Procedures Manual are for the employee's information but may not specify all the computer use standards, University policies and procedures, and state and Federal laws by which an employee is governed.

It is the responsibility of individual users to access and use data in accordance with the University's policies and the State of California Information Practices Act of 1977. For more specific information, refer to the references shown in **F. ADDITIONAL REFERENCES.**

D. **USER RESPONSIBILITIES**
Individual users certify understanding of and agree to adhere to Computing's guidelines by signing the **LOGON ID REQUEST/COMPUTER SECURITY AND USE AGREEMENT** (see Sec.- 2, Exhibit B) or **VAX ACCOUNT REQUEST FORM** (Exhibit E). Specifically, an employee acknowledges an understanding of and agrees to adhere to the following:

1. Security is to be maintained by not providing anyone else access to or use of University information systems maintained by Computing & Communications.

2. The Logon ID or Username is considered equivalent to a signature and the individual is responsible for all entries made under that Logon ID.

3. Proper password security to all systems, including electronic mail, is to be maintained by not revealing passwords to anyone.

4. Proper physical security is to be maintained by not leaving a workstation/terminal unattended while logged into a University system.

5. Suspected security violations are to be reported to the department head and the Institutional Computing or VAX Security Administrator.

6. Under existing California state law, any person who maliciously accesses, alters, deletes, damages, or destroys any computer system, network, computer program, or data shall be guilty of a felony.

7. Computing resources and University data are to be used only for the University's legitimate business for which an employee is explicitly authorized.

8. The privacy and confidentiality of all accessible data are to be maintained. It is understood that unauthorized disclosure of personal/confidential information is an invasion of privacy and may result in disciplinary, civil, and/or criminal actions against an individual.

9. References to personal and confidential information in the Campus Policy and Procedures Manual and the **LOGON ID REQUEST/COMPUTER SECURITY AND USE AGREEMENT** are for the employee's information but may not specify all computer use standards, University policies and procedures, and state and Federal laws by which employees are governed.

Failure to comply with the above may result in disciplinary action, up to and including dismissal. Any violation of local, state, or Federal laws may carry the additional consequence of prosection under the law - where judicial action may result in one or more of the following:

- specific fines
- imprisonment
- litigation costs
- payment of damages

The University will take the strongest actions possible in the case of any breach of these agreements.

E. **DEPARTMENTAL RESPONSIBILITIES**

Access to the University's information systems is granted to employees with a demonstrable need for access. The employee's department head or delegate certifies that requested access is required for the employee's necessary and proper performance of assigned job duties. The department head initially requests employee access to the University's information systems maintained by Computing & Communications by submitting the following to the Computing's IBM/VAX Security Administrator:

1. A completed **SIGNATURE AUTHORIZATION/DELEGATION** form (see Sec.- 2, Exhibit A). This form establishes the authority to request user access to information systems or to delegate that authority to another individual in the department.

2. A department head/delegate authorized **LOGON ID REQUEST/COMPUTER SECURITY AND USE AGREEMENT** (see Sec.-2, Exhibit B). This form is used by a department to request a logon ID for an employee and for this employee to acknowledge understanding of and agreement to adhere to the Computer Security and Use Agreement.

3. A REQUEST FOR ACCESS TO SYSTEMS (see Sec.- 2, Exhibit C). This form is used to request employee access to specific University online systems maintained by Computing & Communications. This form should be submitted at least five working days in advance of when access is needed.

The Department Head/Authorized Delegate must submit a **CANCELLATION REQUEST** (see Sec.-2, Exhibit D) whenever any of the following apply: 1) an employee terminates employment with the University, 2) an employee transfers to another department, or 3) an employee has a change in departmental responsibilities and no longer requires access to the University's information systems maintained by Computing & Communications.

F. **ADDITIONAL REFERENCES**
Business and Finance Bulletins (available for reference in the Labor Relations Office):

RMP-7	Privacy of and Access to Information Responsibilities
RMP-8	Legal Requirements of Privacy of and Access to Information
RMP-9	Guidelines for Access to University Personnel Records by Government Agencies

Campus Policies and Procedures Manual:

800-70	Privacy and Access to Information

SECTION - 2

PROCEDURES FOR ACCESSING UNIVERSITY INFORMATION SYSTEMS

A. **REQUESTING ACCESS**
To initially request access to information systems maintained by Computing, three forms must be filed with Computing and Communications. Forms from the exhibits in this section should be duplicated, completed, and submitted to the Computing's IBM or VAX Security Administrator.

B. **SIGNATURE AUTHORIZATION/DELEGATION (See Exhibit A)**
A **SIGNATURE AUTHORIZATION/DELEGATION** form is used by a department to establish an individual's authority to request access by departmental employees to the University's information systems or to add a delegate with signature authority.

1. Complete only one form for each organizational unit.

2. Completed forms are maintained by the Institutional Computing Security Administrator.

3. **Resubmit this form only when there is an addition, change, or deletion in department head or delegate.**

C. **LOGON ID REQUEST/COMPUTER SECURITY AND USE AGREEMENT (See Exhibit B for IBM access, Exhibit E for VAX access)**

A **LOGON ID REQUEST/COMPUTER SECURITY AND USE AGREEMENT** form is used by a department to request a logon ID for an employee to be used on Institutional Computing's IBM mainframe computer. Departments should limit logon ID's to employees with a demonstrable need for access.

1. One form should be submitted for each user.

2. Completed forms are maintained by the Institutional Computing Security Administrator.

3. After access is established, individuals are notified of their Logon ID and default password.

D. **REQUEST FOR ACCESS TO SYSTEMS (See Exhibit C)**

A **REQUEST FOR ACCESS TO SYSTEMS** form is used by a department to request access to specific University online systems maintained by Computing. Departments should limit systems access to employees with a demonstrable need for access.

1. One form is required for each employee for up to six systems to be accessed by the employee.

2. The form should be submitted at least five working days in advance of when access is needed.

3. Completed forms are maintained by the Institutional Computing Security Administrator.

4. Requests are forwarded to the appropriate departments (Registrar, Student Business Services, etc...) for approval to access specific functions. Institutional Computing notifies the employee when access is granted

E. **CANCELLATION REQUEST (See Exhibit D)**

A **CANCELLATION REQUEST** form is used by a department to cancel a logon ID and/or access to specific systems. When an employee terminates University employment, transfers to another department, or changes departmental responsibilities and no longer requires access to the University's information systems maintained by Computing, it is the responsibility of the department that requested access to request the cancellation of the logon ID and/or access to systems.

1. Cancellation of the logon ID cancels access to all systems.

2. Signature of the department head or delegate is required.

3. Prior to the release of the terminating employee's last check, a cancellation request should be sent to Computing & Communications.

F. **AUTOMATIC CANCELLATIONS**

1. A logon ID with no activity for three consecutive months will be canceled by Computing unless the logon ID is placed in inactive status - see 2. below.

2. If an employee will be on leave of absence or furlough for three months or longer, arrangements must be made to have the logon ID placed on inactive status until the employee returns. The employee, the department head, or the authorized delegate should send a written memo to the Institutional Computing Security Administrator stating the employee name, logon ID, leave begin date and leave return date. Failure to follow this procedure will result in the logon ID being canceled.

G. **INTERNAL AUDIT**

To accomplish audit objectives, the Internal Audit Department is authorized to have full inquiry access to all University information systems. This open access will facilitate the periodic review of controls over system security, access, and use.

H. **DEPARTMENT INFORMATION SYSTEMS**

Access, use, and security controls over information systems distributed throughout the campus departments are the responsibility of the campus department management. Questions concerning access, use, and security controls for a particular department's information system can be directed to Computing & Communications IBM or VAX Security Administrator or the Internal Audit Department.

Section - 2, Exhibit A

UCR COMPUTING & COMMUNICATIONS SIGNATURE AUTHORIZATION/DELEGATION

Department Name ____________________

Check the desired action(s) below.

____ **Establish Signature Authority**

By signing below I certify that I am the Department Head or Dean with responsibility and authority to manage funds and administrative actions. Further, I understand that I have authority to approve a request for an employee's logon ID - which is considered equivalent to a signature for some system actions.

____________________ ____________

Signature of Department Head or Dean Date

____________________ ____________

Printed name of Department Head or Dean Payroll Title

____ **Add Delegate to Signature Authority**

The delegate specified below is granted the authority to request a logon ID for an employee. By signing below I certify that I have been granted authority to request a logon ID for an employee - which is considered equivalent to a signature for some system actions.

____________________ ____________

Signature of Authorized Delegate Date

____________________ ____________

Printed name of Authorized Delegate Payroll Title

____________________ ____________

Signature of Department Head or Dean Date

____ **Cancel Department Head/Delegate**

____________________ ____________

Printed name to be canceled Date

____________________ ____________

Signature of Department Head or Dean Date

Submit the completed form to Computing & Communications (Security Administrator).

Section - 2, Exhibit B
Page 1

UCR COMPUTING & COMMUNICATIONS
LOGON ID REQUEST/COMPUTER SECURITY AND USE AGREEMENT

Logon ID Request:

Employee Name________________________________ Employee Number__________

Department__________________________________ Phone Number____________

Computer Use and Security Agreement:

I, the undersigned employee, acknowledge that I understand and agree to adhere to the following statements:

* My logon ID is considered equivalent to my signature, and I am responsible for all entries made under my logon ID.

* I will maintain proper password security by not revealing my password to anyone.

* I will maintain Computing & Communications system's security by not providing anyone else access to or use of Computing's systems.

* I will maintain proper physical security by not leaving my workstation/terminal unattended while I am logged into University systems.

* I will report suspected security violations to the Department Head and Institutional Computing Security Administrator.

  I am informed that under existing California state law, any person who maliciously accesses, alters, deletes, damages, or destroys any computer system, network, computer program, or data shall be guilty of a felony.

* I will use computing resources only for legitimate University business for which I, as an employee, am explicitly authorized. I know that it is against University policy to pursue or use University records including, but not limited to, personal or confidential information for my personal interest or advantage.

* I will maintain the privacy and confidentiality of all accessible data and understand that unauthorized disclosure of personal/confidential information is an invasion of privacy and may result in disciplinary, civil, and/or criminal actions against me.

* I am informed that the references to personal and confidential information in the Riverside Campys Policies and Procedures Manual and this document are for my information but may not specify all the computer use standards, University policies and procedures, and state and Federal laws by which I am governed.+

Section - 2, Exhibit B
Page 2

* I am informed that failure to comply with these policies, rules, and regulations may result in disciplinary action, up to and including dismissal. Any violation of local, state, or Federal laws may carry the additional consequence of prosection under the law - where judicial action may result in one or more of the following:

- * specific fines
- * imprisonment
- * litigation costs
- * payment of damages

The University will take the strongest actions possible in the case of any breach of these agreements.

____ ____________________Employee
Signature Date

Department Head/Delegate Authorization:

____ ____________________
Signature of Department Head or Authorized Delegate Date

____ ____________________Printed Name of
Department Head or Authorized Delegate Date

Some of the data in the University's information systems may be defined as personal or confidential under University Policy and the State of California Information Practices Act of 1977 (IPA). The IPA applies to all University records, except those student records specifically exempted from the law, containing personal or confidential information and is intended to protect the privacy of individuals about whom records are maintained. Access to these records, which may be maintained by individual name or other identifier such as employee number or social security number, is authorized when necessary to the performance of duties and if the use of the records is consistent with the purpose(s) for which the information was acquired.

+ State of California Information Practices Act of 1977 (IPA); Riverside Campus Policy and Procedures Manual Section 800-70 (Exhibit A); Business and Finance Bulletin RMP-7 "Privacy and Access to Information Responsibilities"; Business and Finance Bulletin RMP-8 "Legal Requirements of Privacy of and Access to Information"; Business and Finance Bulletin RMP-9 "Guidelines for Access to University Personnel Records by Government Agencies."

Section - 2, Exhibit C

UCR COMPUTING & COMMUNICATIONS
REQUEST FOR ACCESS TO SYSTEMS

Complete a separate form for each employee for up to six system(s) requiring access.

Person for whom access is requested: ____________________

Logon ID: ____________________ or VAX username: ____________________
(If known)

Job Title: ____________________ Department: ____________________

Department Code: ____________________
(if requesting DEXlite access)

Purchase Dollar Limit$ ____________
(if requesting PRlite)

System(s) requested:

System 1: ____________________ System 4: ____________________

System 2: ____________________ System 5: ____________________

System 3: ____________________ System 6: ____________________

By signing below, I request that the above named individual be given access to the system indicated. I consider this access to be necessary and proper, and I understand that I am to notify Computing & Communications in the event this employee transfers or separates.

____________________ Department Phone ____________
Signature of Department Head or Authorized Delegate

____________________ ____________
Printed name of Department Head or Authorized Delegate Date

Submit the completed form to the Computing & Communications (Security Administrator).

COMPUTING & COMMUNICATIONS

Reviewed by Project Leader ____________________ ____________
Signature of Project Leader Date

Access enabled by ____________________ ____________
Signature of Security Administrator Date

Application Profile, etc. ____________________

Copy to VAX Security Administrator ________ Date: ____________

Section - 2, Exhibit D

UCR COMPUTING & COMMUNICATIONS
CANCELLATION REQUEST

______________________	______________________
Department Name	Employee Logon ID/Username
______________________	______________________
Employee Name	Employee Phone Number

Check the box corresponding to the requested cancellation:

____ **Logon ID Cancellation:** Cancellation of logon ID will automatically cancel access to all systems.

____ **VAX Username Cancellation:** Dexlite access is automatically cancelled

____
Effective Date

____ **Access to Systems Cancellation:**

Name of system(s) or functions within a system to be canceled:

____

____

____
Effective Date

______________________________	______________
Signature of Dean/Department Head/Delegate	Date

____
Printed name of Dean/Department Head/Delegate Name

Submit the completed form to the Institutional Computing Security Administrator.

Copy to VAX Security Administrator: ______ Date: ____________

SECTION - 3

USING UNIVERSITY INFORMATION SYSTEMS ON THE IBM MAINFRAME

A. PASSWORD SELECTION

1. Passwords must be five to eight characters long and must begin with an alphabetic (A-Z) or national (@, #, $) character. Blank spaces must not be included.

2. Passwords should be easy to remember.

3. Passwords which combine alphabetic and numeric characters are encouraged.

4. When selecting a password, **DO NOT** use:

    * Names of people (last, first, or middle)
    * Names of pets
    * Birth dates
    * Portions of social security numbers
    * Logon ID
    * License plates
    * Any other information which might be easy for someone to guess.

B. PASSWORD SECURITY

Maintaining confidential passwords is an essential safeguard against misuse, intrusion, and theft. Each user is personally responsible for the use of his/her logon ID and password.

* Passwords should not be displayed or written down.
* Passwords are confidential and should not be shared with anyone, including supervisors, co-workers, family members, or friends.
* Passwords should not be stored on a workstation as part of an automated logon process.
* If there is a reason to suspect that password confidentiality has been compromised, the user is responsible for changing his/her password immediately and reporting the suspicion to the Institutional Computing Security Administrator.

C. PASSWORD EXPIRATION

Passwords automatically expire in 35 days. The user is prompted at that time to enter a newly selected password. 12 generations of previous passwords are maintained. Passwords can not be reused unless they are more than 12 generations old.

D. INVALID LOGON ATTEMPTS

When a user attempts to logon with a valid logon ID and an incorrect password, the system responds with the message "Password invalid". Four such attempts result in revocation of the logon ID. Contact the Institutional Computing Security Administrator at extension 4741 for assistance.

E. TIMEOUTS

After 60 minutes of inactivity, the user is logged off automatically.

F. GETTING HELP WITH SYSTEMS

Online system help is available on most systems by pressing [F1]. System help is available from Institutional Computing at extension 4741 from 8:00 a.m. to 12 Noon, and from 1:00 p.m. to 5:00 p.m., Monday through Friday.

Academic Computing
Computing & Communications, UC Riverside
Application for Computer Allocated Funds

Name: (Last) ______________________ (First) ______________________ (MI) ____

Title or Status: ____

Department: ______________________ Telephone: ______________

Type of Account (check one):

□ Student Easy Access—Student ID No. ______________________

□ Instruction:
Course name/# (this will become the User Name) ______________
Number of student accounts needed ______________
Student Password ______________

□ Undergraduate Special Studies/Research
□ Graduate Directed Research/Dissertation
□ Faculty Research

X ______________________
Faculty Advisor/Professor signature required for student and post-doc accounts

□ Staff

□ Department Funds:
Recording number: ______________
Cost Center (optional): ______________

X ______________________
Signature of person authorized to sign for the account

□ Off-campus
Name ______________________ Deposit $______________
Address ______________________ Phone ______________

Computer(s)

□ VAX(VMS) □ ______________

USER NAME (4 character min/8 max) ______________________

PASSWORD (6 character min/16 max) ______________________

My signature below acknowledges my understanding and willingness to adhere to the policies stated in UCR's Policy & Procedure No. 400-35 Section 1 - D, User Responsibilities.

Date______________________ User Signature X______________ 94

Office Use Only
Account established: ______ Dollars allocated: ______ Account #______

(Copy 2 will be returned for confirmation and filing)

University of Georgia

COMPUTER ETHICS AT GEORGIA

Summary of Policies

December 1994

The University of Georgia is committed to free and open inquiry and discussion, fair allocation of University resources, and the provision of a working environment free of needless disruption. To advance these goals, the University has adopted policies on computer usage that are summarized here and stated in detail elsewhere. Most of these policies follow from pre-existing regulations, agreements, and/or laws. They fulfill a Board of Regents directive requiring adoption of explicit computer security and ethics policies.

* Like all University facilities, University computers and computer networks are to be used only by persons authorized by the University, and only for University purposes. University purposes include the educational programs of the University, as well as its research, administrative, and outreach activities. Use of University facilities for other purposes requires prior authorization.

* No one shall give a computer password to an unauthorized person, nor obtain another person's computer password by any unauthorized means whatsoever. Disclosing a password to an unauthorized person can be a crime under Georgia law.

* No one shall engage in, encourage, or conceal from authorities any "cracking," unauthorized tampering, or other unauthorized use or deliberate disruption of computers.

* No one without specific authorization shall read, alter, or delete any other person's computer files or electronic mail, even if the operating system of the computer permits them to do so.

* Users shall not place confidential data into computers without protecting it appropriately. The University cannot guarantee the privacy or authenticity of computer files or electronic communications unless special arrangements are made.

* No one shall copy or use software or data in violation of copyright laws, license agreements, or the basic requirements of academic honesty.

* Users shall take full responsibility for messages that they transmit through the University's computers and network facilities and shall obey the policies of discussion forums in which they participate. Laws and rules against fraud, harassment, obscenity, and the like apply to electronic communications no less than other media.

* Those who administer computers and network facilities shall perform their duties fairly, in accordance with University policies, and shall refer all disciplinary matters to appropriate authorities.

Violations of these policies incur the same types of disciplinary measures as violations of other University policies or state or federal laws, including criminal prosecution in serious cases.

University of Georgia Policies on Use of Computers

December 1994

Purpose:

This document has two purposes: to prohibit certain unacceptable uses of the University of Georgia's computers and network facilities, and to educate users about their responsibilities.

Most of these regulations simply restate obligations that follow from other existing policies or laws (see "Relevant Laws," below). They fulfill a Board of Regents directive requiring the University to adopt explicit computer security and ethics policies along the lines of those recommended in Internet RFC 1244.

This document is divided into rules and commentary, with the expectation that the commentary can be revised frequently to reflect technical changes and to answer questions that have come up, without materially changing the rules.

Penalties:

Violations of these policies incur the same types of disciplinary measures as violations of other University policies or state or federal laws, including criminal prosecution in serious cases.

Definitions:

* "University computers and network facilities" comprise all computers owned or administered by any part of The University of Georgia or connected to the University's communication facilities, including departmental computers, and also the University's computer network facilities accessed by anyone from anywhere.

* "Authorization" is permission granted by the appropriate part of the University's governance and/or management structure, depending on the particular computers and/or network facilities involved and the way they are administered.

Rules:

(1) No one shall use any University computer or network facility without proper authorization. No one shall assist in, encourage, or conceal from authorities any unauthorized use, or attempt at unauthorized use, of any of the University's computers or network facilities.

Comment: Computers and networks are just like any other University facilities -- they are to be used only by people who have permission.

Using a computer without permission is theft of services and is illegal under state and federal laws. In addition, the following specific computer crimes are defined by state law (Ga. Code 16-9-90 et seq.):

* Computer theft (including theft of computer services, intellectual property such as copyrighted material, and any other property);

* Computer trespass (unauthorized use of computers to delete or alter data or interfere with others' usage);

* Computer invasion of privacy (unauthorized access to financial or personal data or the like);

* Computer forgery (forgery as defined by other laws, but committed on computer rather than on paper);

a computer rather than on paper);

* Computer password disclosure (unauthorized disclosure of a password resulting in damages exceeding $500 -- in practice, this includes any disclosure that requires a system security audit afterward).

Maximum penalties are a $5,000 fine and 1 year of imprisonment for password disclosure, and a $50,000 fine and 15 years of imprisonment for the other computer crimes, plus civil liability.

(2) No one shall knowingly endanger the security of any University computer or network facility, nor willfully interfere with others' authorized computer usage.

Comment: Many of the other regulations given here deal with specific acts of this kind. You should not assume that other malicious acts or deliberate security violations are permissible merely because there is no specific rule against them.

(3) No one shall use the University's communication facilities to attempt unauthorized use, nor to interfere with others' legitimate use, of any computer or network facility anywhere.

Comments: State and federal laws forbid malicious disruption of computers. The University of Georgia does not tolerate individuals who invade others' privacy, steal computer services, or commit misrepresentation or fraud; nor pranksters who attempt to disrupt computers or network facilities for any other purpose.

Also, you should be aware that _ability_ to use a remote computer does not constitute permission.

Some computer services are open to the public, and clearly identify themselves as such; examples are anonymous FTP sites and Gopher servers. But the mere lack of security measures does not mean that a computer is open to anyone who wishes to use it. The same goes for unauthorized use of communication paths, such as remote dialout modems and the like.

(4) No one shall connect any computer to any of the University's networks unless it meets technical and security standards set by the University administration.

Comments: The applicable requirements depend on what kind of connection is being made. For example, dialing up with an ordinary asynchronous modem does not require any special authorization, but connecting to the campus-wide Ethernet cable does, because one improperly configured machine on a network can cause widespread disruption.

(5) All users shall share computing resources in accordance with policies set for the computers involved, giving priority to more important work and cooperating fully with the other users of the same equipment.

Comments: If you need an unusual amount of disk space, CPU time, or other resources, check with the administrators in charge of the computer rather than risk disrupting others' work. When resources are tight, work that is necessary to the University's mission (instruction, research, and service) must take priority over computing that is done to pursue personal interests or self-training on side topics. Also, no matter how important your work may be, you are only entitled to one person's fair share of the machine unless additional resources are available and appropriate permission has been granted.

Priorities for any particular machine are set by the administrators in

Priorities for any particular machine are set by the administrators in charge of it in consultation with the user community.

Obtaining extra computer resources through any form of deception (e.g., secretly opening multiple accounts, misrepresenting the nature of your work, or the like) is strictly prohibited.

(6) No one without specific authorization shall use any University computer or network facility for non-University business.

Comments: By law, the University can only provide computer services for its own work, not for private use. In this respect the University's computers are different from those owned by private colleges or corporations. If you need unlimited access to computer networks for private purposes, you can subscribe to a private service such as America Online or CompuServe.

The University's mission can be understood broadly as including education, self-training, and discussion on a wide range of subjects, not just those immediately necessary for a person's job or courses.

The University grants the use of its facilities to numerous organizations whose activities contribute to its mission, such as student organizations, professional societies, and the Campaign for Charities. But it is improper to use the University's computers for political campaigns, fund-raising, commercial enterprises, mass mailings, or other outside activities that have not been granted the use of the University's facilities.

Various policies permit members of the University community to earn outside income by writing books and articles related to their academic work, and to use University resources for this purpose, including computers. Most faculty are also permitted to use University facilities for outside consulting jobs provided the University is reimbursed for costs incurred. Check with your supervisor to find out how these policies apply to you.

(7) No one shall give any password for any University computer or network facility to any unauthorized person, nor obtain any other person's password by any unauthorized means whatsoever.

Comments: Giving your password to an unauthorized person can be a crime under Georgia law. The criterion is not whether _you_ trust them, but whether the University has authorized them.

A password is like the key to a building -- you are responsible for what happens to it while it's in your care. If you give it away, you are endangering the entire machine, not just your own files. In fact, there are computer criminals who would like to have your password so they can make it look as though you, not they, are committing their crimes.

You are responsible for choosing a secure password. Don't use names, nicknames, phone numbers, or recognizable words in any language, because some people guess passwords by automatically trying every word in a large dictionary.

A good way to make up a secure password is to use the initials of a phrase, and include some numbers as well as letters. For example, "57ityMwb" is a good password, and it's easy to remember because it stands for "57 is the year Michael was born."

Your password is secret. System administrators will not normally ask you for it. The computer will never ask you to type it unless you are logging in or changing your password. Beware of computer programs that ask you to "log in again" or type your password at any other time; they are likely to be tricks. (There are rare exceptions on some computers; check with your system manager. If anything that you don't understand ever happens after you type your password, then don't understand ever happens after you type your password, then change your password immediately.)

If you need to work with someone else on a project, don't share a password; instead, arrange to share file space. Learn how to use file permissions, groups, and other security features of the system you are using.

(8) No one shall misrepresent his or her identity or relationship to the University for the purpose of obtaining or using computer or network privileges.

Comments: Naturally, you must not claim to be someone else, nor claim to have a different relationship to the University than you actually do, when obtaining a computer account or access to a lab.

All access to the Internet through the University's facilities is restricted to people who are identified to the University, even if the purpose is to use a computer elsewhere.

(9) No one without specific authorization shall read, alter, or delete any other person's computer files or electronic mail. This rule applies regardless of whether the operating system of the computer permits these acts.

Comments: Don't even _try_ to guess or steal other people's passwords, or read their files, even if the computer permits this. Doing so would be like rummaging through someone else's desk. Even if you can pick the lock, and even if there is no lock at all, you have no right to intrude.

(10) No one shall copy, install, or use any software or data files in violation of applicable copyrights or license agreements.

Comments: This rule forbids making unauthorized copies, for use elsewhere, of software residing on the University's computers. It also forbids installing or using pirated software on University computers.

The price of a piece of software isn't just the cost of the disk -- it's also one user's share of the cost of developing and supporting it. It's wrong to use software without paying your fair share.

Not only that, but the University benefits from the generosity and good will of many software vendors; any sign of software piracy would bring this generosity to a halt and result in higher prices for everybody.

As if that weren't enough, unauthorized copying is usually a violation of federal copyright law.

Some educational software licenses forbid the use of the software for commercial purposes. Some software is "site licensed" and can be used on any University computer. (The terms of various site licenses differ.) Some software is genuinely free; the author allows everyone to use it free of charge. Before copying software, be sure what you are doing is legal, and consult people who have full information; don't just give yourself the benefit of the doubt.

License checks: If strangers show up at your computer site saying they are there to check software licenses, you should immediately contact Legal Affairs and your administrative superiors. After hours, contact Campus Police. Software licenses do not normally authorize these surprise inspections, and there is a substantial risk that the "inspectors" are not legitimate.

(11) No one shall create, install, or knowingly distribute a computer virus, "Trojan horse," or other surreptitiously destructive program on any University computer or network facility, regardless of whether any demonstrable harm results.

Comments: A virus is a hidden computer program that secretly copies itself onto users' disks, often damaging data. A Trojan horse is a program with a hidden, destructive function, or a program designed to trick users into revealing confidential information such as passwords. Even when the harm done by programs of these types is not readily evident, they confuse beginning computer users, degrade CPU performance, and waste the time of system managers who must remove them.

(12) No one without proper authorization shall modify or reconfigure the software or hardware of any University computer or network facility.

Comments: Do not modify the hardware, operating system, or application software of a University computer unless you have been given permission to do so by the department or other administrative unit that is in charge of the machine. The other users with whom you share the machine, and the technicians on whom you rely for support, are expecting to find it set up exactly the way they left it.

(13) Users shall not place confidential information in computers without protecting it appropriately. The University cannot guarantee the privacy of computer files, electronic mail, or other information stored or transmitted by computer unless special arrangements are made.

Comments: Ordinary electronic mail is not private. Do not use it to transmit computer passwords, credit card numbers, or information that would be damaging if made public. Bear in mind that students' educational records are required by law, and by U.Ga. policy, to be kept confidential. It is also necessary to protect confidential information about employees, such as performance evaluations. This applies not only to networked computers, but also to computers, tapes, or disks that could be stolen; an increasing number of computer thieves are after data rather than equipment.

The University will normally respect your privacy but cannot guarantee it absolutely. There are many ways a normally private file can end up being read by others. If a disk is damaged, a system administrator may have to read all the damaged files and try to reconstruct them. If email is mis-addressed, it may go to one or more "postmasters" who will read it and try to correct the address. For your own protection, system administrators will often look at unusual activity to make sure your account hasn't fallen victim to a "cracker."

The Georgia Open Records Act applies to information stored in computers. This act gives citizens the right to obtain copies of public records, including any record prepared, received, or maintained by the University in the course of its operations. Some kinds of records are exempt; among these are student records (including tests and homework), medical records, confidential hiring evaluations, trade secrets (which probably includes unpublished research), and material whose disclosure would violate copyright. Moreover, the Open Records Act is not a license to snoop; requests for information must be made through proper administrative channels.

(14) Users shall take full responsibility for messages that they transmit through the University's computers and network facilities. No one shall use the University's computers to transmit fraudulent, defamatory, harassing, obscene, or threatening messages, or any communications prohibited by law.

Comments: You have exactly the same responsibilities on the computer network as when using other forms of communication. You must obey laws against fraud, defamation, harassment, obscenity, solicitation of illegal acts, threatening or inciting violence, and the like. Bear in mind that uninvited amorous or sexual messages are likely to be construed as harassment. If you are bothered by uninvited email, ask the sender to stop, and then, if necessary, consult a system administrator.

Use of the computers to circulate chain letters and pyramid schemes is not permitted. If someone says, "Forward a copy of this to everyone you know on the Internet," _don't_. Such messages often contain misunderstood or outdated information, or even outright hoaxes. Even when the information is legitimate, chain forwarding is a needlessly expensive way to distribute it.

Send electronic mail only to people you actually wish to contact -- not to randomly chosen individuals who just happen to be on the same campus. (Well-known people do not like to serve as secretaries for their entire institutions.) If you do not have the email address of the person you want to reach, use ordinary mail or the telephone.

Never participate in schemes to deliberately flood a computer with excessive amounts of email. "Mail bombing" can incapacitate a whole computer or even a whole subnetwork, not just the intended victim.

Never falsify your name or status when using privileges such as electronic mail and newsgroups. On some computers, anonymous communication (concealing your name) is sometimes permitted. Deceptive communication, in which your messages appear to come from another specific person, is never allowed.

It is considered good practice to use your real name, rather than a nickname or pseudonym, in the headers of all outgoing communications. Use of nicknames is often interpreted as a sign of immaturity or an indication that you are not taking full responsibility for what you are sending out.

Fake electronic mail: All users should be aware that there is no guarantee that electronic mail actually came from the person or site indicated in it. Deceptive electronic mail is easy to fake, including the technical information in the header. Doing so is of course prohibited.

(15) Users shall comply with the regulations and policies of newsgroups, mailing lists, and other public forums through which they disseminate messages.

Comments: When participating in Usenet newsgroups and similar forums, you must respect their policies and practices, for two reasons:

* To join these networks, the University has to agree to abide by their policies. Misuse would endanger the University's eligibility to participate.

* Most of the cost of transmitting any message in a discussion is borne by the sites that receive it, not the site that sends it out. Thus, you are the guest of the whole network community, and it is important to abide by the policies and practices of the entire network.

The most ironclad rule is to respect the announced subject of each forum and not to post anything off-topic. Other things that are generally unwelcome include:

* Advertisements (except that many forums permit announcements that are directly relevant to their subject areas);

* Multiple postings of the same material (a general--interest message should go in one general--interest forum, not several specialized ones);

* Survey questionnaires and other mass solicitations;

* Questions that are easily answered by looking in dictionaries, encyclopedias, or readily available software manuals;

* Requests for help with homework;

* Uninformative criticisms of other people's postings (unwelcome material posted by others should be ignored, not discussed);

* Postings that are misspelled, obscurely worded, or TYPED IN ALL CAPITALS LIKE THIS;

* Postings that say "Test message, please ignore" (try out your software when you actually have something to say, or use a test newsgroup).

Before posting anything, make sure that you know how to cancel it in case you subsequently discover that it is redundant or misinformed. Also, before posting in any Usenet newsgroup, read the appropriate guidelines for new Usenet users, and read some of the messages that are already there so you can be sure you have not misjudged the newsgroup's subject or purpose.

Always assume that everyone in the entire world can read what you are posting, that permanent copies will be kept at several sites, and that you will be expected to take full responsibility for everything you say. Do not post anything that you would not want to see quoted in a major newspaper.

Remember that newsgroups are not confined to the United States and are certainly not confined to students. You will sometimes see postings from other countries in their native languages, and you will often see postings from senior professionals in their fields.

(16) System administrators shall perform their duties fairly, in cooperation with the user community, the appropriate higher-level adminstrators, University policies, and funding sources. System administrators shall respect the privacy of users as far as possible and shall refer all disciplinary matters to appropriate authorities.

Comments: The first responsibility of any computer or network administrator is to serve the user community. But regardless of what the users want, system administrators are not free to violate copyrights, software licenses, other legal restrictions, or obligations undertaken by the University in order to obtain funding.

Although computer users' privacy is never perfect, system administrators are expected to respect this privacy as far as possible and refrain from unnecessary snooping. Administrators who must read users' files for administrative reasons must be prepared to justify their actions to higher administrators and to the user community.

System administrators should not normally interfere with users' electronic communication, especially in any way that could be interpreted as favoring one side of a controversy or suppressing an unpopular opinion or topic. As far as possible, decisions affecting access to online information services should be made in full consultation with the user community, taking into account the cost of the computer resources involved.

The system administrator is not the judge, jury, and executioner in cases of computer misuse. Rather than penalizing users directly for their misdeeds, the system administrator is expected to refer all cases to appropriate authorities who can protect the rights of the accused. If you are accused of any violation that justifies disciplinary action, you have a right to a fair hearing just as if your alleged misdeeds had not involved computers.

It is important to distinguish actions taken to punish a person from actions taken to protect a system. If your account appears to have been misused or broken into, your system administrator will inactivate it and contact you or wait to hear from you. This is done to stop the misuse and does not presume that you are the guilty person; you can expect to have your privileges reinstated right away, with new passwords, as soon as you identify yourself and indicate willingness to follow the rules. Thus, you can resume using the computer while investigation of the incident continues.

Relevant laws:

Computer crimes defined by Georgia law were mentioned in the comments on rule 1. In addition, there is a specific law against electronic distribution of obscene material to minors (Ga. Code 16-12-100.1).

Federal law (18 USC 1030) provides for fines and imprisonment up to 20 years for unauthorized or fraudulent use of computers that are used by or for the federal government (which includes many of the computers on the net), and for unauthorized disclosure of passwords and similar information when this affects interstate commerce. (Recall that net messages, as well as long-distance phone calls, are interstate commerce and thus fall under this law.)

The Electronic Communications Privacy Act (18 USC 2701-2709) and other wiretap laws prohibit unauthorized interception of electronic communications, including electronic mail.

Computer users must also obey laws against private use of state property, divulging confidential educational records, copyright infringement, fraud, slander, libel, harassment, and obscenity. Laws against obscene or harassing telephone calls apply to computers that are accessed by telephone. The Georgia Open Records Act applies to records stored in computers as well as on paper.

The University must obey the policies of the University System (Board of Regents) and the regulations of the nationwide and worldwide networks to which its computers are connected.

Georgia Institute of Technology COMPUTER AND NETWORK USAGE POLICY

> Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, the right to privacy, and the right to determine the form, manner, and terms of publication and distribution. Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the academic community. The EDUCOM Code.

1. BACKGROUND AND PURPOSE

This document constitutes an Institute-wide policy intended to allow for the proper use of all Georgia Tech computing and network resources, effective protection of individual users, equitable access, and proper management of those resources. This should be taken in the broadest possible sense. This policy applies to Georgia Tech network usage even in situations where it would not apply to the computer(s) in use. These guidelines are intended to supplement, not replace, all existing laws, regulations, agreements, and contracts which currently apply to these services.

Campus units that operate their own computers or networks may add, with the approval of the unit head, individual guidelines which supplement, but do not relax, this policy. In such cases, the unit should inform their users and the Information Resources Security Coordinator in OIT prior to implementation.

Access to networks and computer systems owned or operated by Georgia Tech imposes certain responsibilities and obligations and is granted subject to Institute policies and local, state, and federal laws. Appropriate use should always be legal, ethical, reflect academic honesty, reflect community standards, and show restraint in the consumption of shared resources. It should demonstrate respect for intellectual property; ownership of data; system security mechanisms; and individuals rights to privacy and to freedom from intimidation, harassment, and unwarranted annoyance. Appropriate use of computing and networking resources includes instruction; independent study; authorized research; independent research; communications; and official work of the offices, units, recognized student and campus organizations, and agencies of the Institute.

2. DEFINITIONS

2.1. Authorized use

Authorized use of Georgia Tech-owned or operated computing and network resources is use consistent with the education, research, and service mission of the Institute, and consistent with this policy.

2.2. Authorized users

Authorized users are: (1) current faculty, staff, and students of the Institute; (2) anyone connecting to a public information service (see section 6.5); (3) others whose access furthers the mission of the Institute and whose usage does not interfere with other users' access to resources. The policy *Access by External Entities to Institute Information Technology Resources* (OIT, 11/3/93, and any subsequent revisions) may apply. In addition, a user must be specifically authorized to use a particular computing or network resource by the campus unit responsible for operating the resource.

3. INDIVIDUAL PRIVILEGES

It is the following individual privileges, all of which are currently existent at Georgia Tech, that empower each of us to be productive members of the campus community. It must be understood that privileges are conditioned upon acceptance of the accompanying responsibilities.

3.1. Privacy

To the greatest extent possible in a public setting we want to preserve the individual's privacy. Electronic and other technological methods must not be used to infringe upon privacy. However, users must recognize that Georgia Tech computer systems and networks are public and subject to the Georgia Open Records Act. Users, thus, utilize such systems at their own risk.

3.2. Freedom of expression

The constitutional right to freedom of speech applies to all members of the campus no matter the medium used.

3.3. Ownership of intellectual works

People creating intellectual works using Georgia Tech computers or networks, including but not limited to software, should consult *Determination of Rights and Equities in Intellectual Property* (Board of Regents Policy Manual, section 603.03, 2/2/94 and any subsequent revisions), and related Georgia Tech policies.

3.4. Freedom from harassment and undesired information

All members of the campus have the right not to be harassed by computer or network usage by others. (See 4.1.3.)

4. INDIVIDUAL RESPONSIBILITIES

Just as certain privileges are given to each member of the campus community, each of us is held accountable for our actions as a condition of continued membership in the community. The interplay of privileges and responsibilities within each individual situation and across campus engenders the trust and intellectual freedom that form the heart of our community. This trust and freedom are grounded on each person's developing the skills necessary to be an active and contributing member of the community. These skills include an awareness and knowledge about information and the technology used to process, store, and transmit it.

4.1. Common courtesy and respect for rights of others

You are responsible to all other members of the campus community in many ways, including to respect and value the rights of privacy for all, to recognize and respect the diversity of the population and opinion in the community, to behave ethically, and to comply with all legal restrictions regarding the use of information that is the property of others.

4.1.1. Privacy of information

Files of personal information, including programs, no matter on what medium they are stored or transmitted, may be subject to the Georgia Open Records Act if stored on Georgia Tech's computers. That fact notwithstanding, no one should look at, copy, alter, or destroy anyone elses personal files without explicit permission (unless authorized or required to do so by law or regulation). Simply being able to access a file or other information does not imply permission to do so.

Similarly, no one should connect to a host on the network without advance permission in some form. People and organizations link computers to the network for numerous different reasons, and many consider unwelcome connects to be attempts to invade their privacy or compromise their security.

4.1.2. Intellectual property

You are responsible for recognizing (attributing) and honoring the intellectual property rights of others.

4.1.3. Harassment

No member of the community may, under any circumstances, use Georgia Tech's computers or networks to libel, slander, or harass any other person.

The following shall constitute Computer Harassment: (1) Intentionally using the computer to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures, or other materials or threats of bodily harm to the recipient or the recipient's immediate family; (2) Intentionally using the computer to contact another person repeatedly with the intent to annoy, harass, or bother, whether or not any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease; (3) Intentionally using the computer to contact another person repeatedly regarding a matter for which one does not have a legal right to communicate, once the recipient has provided reasonable notice that he or she desires such communication to cease (such as debt collection); (4) Intentionally using the computer to disrupt or damage the academic, research, administrative, or related pursuits of another; (5) Intentionally using the computer to invade the privacy, academic or otherwise, of another or the threatened invasion of the privacy of another.

4.2. Responsible use of resources

You are responsible for knowing what information resources (including networks) are available, remembering that the members of the community share them, and refraining from all acts that waste or prevent others from using these resources or from using them in whatever ways have been proscribed by the Institute and the laws of the State and Federal governments. Details regarding available resources are available in many ways, including consulting your Computing Support Representative (CSR) (see section 6.4), conferring with other users, examining on-line and printed references maintained by OIT and others, visiting the OIT Information Center, and contacting the OIT Helpdesk.

4.3. Game playing

Limited recreational game playing, that is not part of an authorized and assigned research or instructional activity, is tolerated (within the parameters of each department's rules). Institute computing and network services are not to be used for extensive or competitive recreational game playing. Recreational game players occupying a seat in a public computing facility must give up that seat when others who need to use the facility for academic or research purposes are waiting.

4.4. Information integrity

It is your responsibility to be aware of the potential for and possible effects of manipulating information, especially in electronic form, to understand the changeable nature of electronically stored information, and to verify the integrity and completeness of information that you compile or use. Do not depend on information or communications to be correct when they appear contrary to your expectations; verify it with the person who you believe originated the message or data.

4.5. Use of desktop systems

You are responsible in coordination with your CSR for the security and integrity of Institute information stored on your personal desktop system. This responsibility includes making regular disk backups, controlling physical and network access to the machine, and installing and using virus protection software. Avoid storing passwords or other information that can be used to gain access to other campus computing resources.

4.6. Access to facilities and information

4.6.1. Sharing of access

Computer accounts, passwords, and other types of authorization are assigned to individual users and must not be shared with others. You are responsible for any use of your account.

4.6.2. Permitting unauthorized access

You may not run or otherwise configure software or hardware to intentionally allow access by unauthorized users. (See section 2.2.)

4.6.3. Use of privileged access

Special access to information or other special computing privileges are to be used in performance of official duties only. Information that you obtain through special privileges is to be treated as private.

4.6.4. Termination of access

When you cease being a member of the campus community (graduate or terminate employment), or if you are assigned a new position and/or responsibilities within the Institute, your access authorization must be reviewed. You must not use facilities, accounts, access codes, privileges, or information for which you are not authorized in your new circumstances.

4.7. Attempts to circumvent security

Users are prohibited from attempting to circumvent or subvert any system's security measures. This section does not prohibit use of security tools by system administration personnel.

4.7.1. Decoding access control information

You are prohibited from using any computer program or device to intercept or decode passwords or similar access control information.

4.7.2. Denial of service

Deliberate attempts to degrade the performance of a computer system or network or to deprive authorized personnel of resources or access to any Institute computer system or network are prohibited.

4.7.3. Harmful activities

The following harmful activities are prohibited: creating or propagating viruses; disrupting services; damaging files; intentional destruction of or damage to equipment, software, or data belonging to Georgia Tech or other users; and the like.

4.7.4. Unauthorized access

You may not:

- □ damage computer systems
- □ obtain extra resources not authorized to you
- □ deprive another user of authorized resources
- □ gain unauthorized access to systems

by using knowledge of:

- □ a special password
- □ loopholes in computer security systems
- □ another user's password
- □ access abilities you used during a previous position at the Institute

4.7.5. Unauthorized monitoring

You may not use computing resources for unauthorized monitoring of electronic communications.

4.8. Academic dishonesty

You should always use computing resources in accordance with the high ethical standards of the Institute community. Academic dishonesty (plagiarism, cheating) is a violation of those standards.

4.9. Use of copyrighted information and materials

You are prohibited from using, inspecting, copying, and storing copyrighted computer programs and other material, in violation of copyright.

4.10. Use of licensed software

No software may be installed, copied, or used on Institute resources except as permitted by the owner of the software. Software subject to licensing must be properly licensed and all license provisions (installation, use, copying, number of simultaneous users, term of license, etc.) must be strictly adhered to.

4.11. Political campaigning; commercial advertising

Board of Regents policy (section 914.01) states "The use of System materials, supplies, equipment, machinery, or vehicles in political campaigns is forbidden." The Georgia Tech Faculty Handbook (section 6.15.3.8(b)) states "Political campaign and commercial advertisement shall not be displayed on the campus." The use of Institute computers and networks shall conform to these policies.

4.12. Personal business

Computing facilities, services, and networks may not be used in connection with compensated outside work nor for the benefit of organizations not related to Georgia Tech, except: in connection with scholarly pursuits (such as faculty publishing activities); in accordance with the Institute Consulting Policy or the policy *Access by External Entities to Institute Information Technology Resources* (OIT, 11/3/93, and any subsequent revisions); or in a purely incidental way. This and any other incidental use (such as electronic communications or storing data on single-user machines) must not interfere with other users' access to resources (computer cycles, network bandwidth, disk space, printers, etc.) and must not be excessive. State law restricts the use of State facilities for personal gain or benefit.

5. GEORGIA TECH PRIVILEGES

Our society depends on institutions like Georgia Tech to educate our citizens and advance the development of knowledge. However, in order to survive, Georgia Tech must attract and responsibly manage financial and human resources. Therefore, Tech has been granted by the State, and the various other institutions with which it deals, certain privileges regarding the information necessary to accomplish its goals and to the equipment and physical assets used in its mission.

5.1. Allocation of resources

Georgia Tech may allocate resources in differential ways in order to achieve its overall mission.

5.2. Control of access to information

Georgia Tech may control access to its information and the devices on which it is stored, manipulated, and transmitted, in accordance with the laws of Georgia and the United States and the policies of the Institute and the Board of Regents.

5.3. Imposition of sanctions

Georgia Tech may impose sanctions and punishments on anyone who violates the policies of the Institute regarding computer and network usage.

5.4. System administration access

A System Administrator (i.e., the person responsible for the technical operations of a particular machine) may access others files for the maintenance of networks and computer and storage systems, such as to create backup copies of media. However, in all cases, all individuals' privileges and rights of privacy are to be preserved to the greatest extent possible.

5.5. Monitoring of usage, inspection of files

Units of Georgia Tech operating computers and networks may routinely monitor and log usage data, such as network session connection times and end-points, CPU and disk utilization for each user, security audit trails, network loading, etc. These units may review this data for evidence of violation of law or policy, and other purposes.

When necessary, these units may monitor all the activities of and inspect the files of specific users on their computers and networks. Any person who believes such monitoring or inspecting is necessary must obtain the concurrence of the unit head and the campus Legal Division. In all cases all individuals' privileges and right of privacy are to be preserved to the greatest extent possible.

5.6. Suspension of individual privileges

Units of Georgia Tech operating computers and networks may suspend computer and network privileges of an individual for reasons relating to his/her physical or emotional safety and well being, or for reasons relating to the safety and well-being of other members of the campus community, or Institute property. Access will be promptly restored when safety and well-being can be reasonably assured, unless access is to remain suspended as a result of formal disciplinary action imposed by the Office of the Vice President for Student Services (for students) or the employee's department in consultation with the Office of Human Resources (for employees).

6. GEORGIA TECH RESPONSIBILITIES

6.1. Security procedures

Georgia Tech has the responsibility to develop, implement, maintain, and enforce appropriate security procedures to ensure the integrity of individual and institutional information, however stored, and to impose appropriate penalties when privacy is purposefully abridged.

6.2. Anti-harassment procedures

Georgia Tech has the responsibility to develop, implement, maintain, and enforce appropriate procedures to discourage harassment by use of its computers or networks and to impose appropriate penalties when such harassment takes place.

6.3. Upholding of copyrights and license provisions

Georgia Tech has the responsibility to uphold all copyrights, laws governing access and use of information, and rules of organizations supplying information resources to members of the community (e.g., acceptable use policies for use of Internet).

6.4. Individual unit responsibilities

Each unit has the responsibility of:

- □ enforcing this policy
- □ providing for security in their areas
- □ providing individuals equipped with Institute-owned desktop systems with resources for regular disk backups (software, hardware, media, and training) and for virus protection

If warranted by the importance and sensitivity of information stored and processed in their facility, a unit must also:

- □ provide system administration personnel
- □ perform and verify integrity of regular media backups
- □ employ appropriate security-related software and procedures
- □ guard confidentiality of private information, including user files and system access codes
- □ control physical access to equipment
- □ provide proper physical environment for equipment
- □ provide safeguards against fire, flood, theft, etc.
- □ provide proper access administration; e.g., prompt and appropriate adjustment of access permissions upon a user's termination or transfer
- □ control and record system software and configuration changes
- □ monitor system logs for access control violation attempts

Units are to designate a person employed by the unit as their Computing Support Representative (CSR); the Director of Client Services, Office of Information Technology is to be notified of CSR appointments. CSRs should be knowledgeable about their unit's computing environment and about central resources and services. The CSR serves:

- □ as the first point of contact for unit personnel seeking problem resolution, information, and other assistance regarding computing and networking
- □ to facilitate interaction between the unit and the Office of Information Technology

6.5. Public information services

Units and individuals may, with the permission of the appropriate unit head, configure computing systems to provide information retrieval services to the public at large. (Current examples include "anonymous ftp" and "gopher.") However, in so doing, particular attention must be paid to the following sections of this policy: 2.1 (authorized use [must be consistent with Institute mission]), 3.3 (ownership of intellectual works), 4.2 (responsible use of resources), 4.9 (use of copyrighted information and materials), 4.10 (use of licensed software), and 6.4 (individual unit responsibilities). Usage of public services must not cause computer or network loading that impairs other services.

7. PROCEDURES AND SANCTIONS

7.1. Investigative contact

If you are contacted by a representative from an external organization (District Attorney's Office, FBI, GBI, Southern Bell Security Services, etc.) who is conducting an investigation of an alleged violation involving Georgia Tech computing and networking resources, inform the office of the Executive Director for Information Technology (EDIT) and the Chief Legal Advisor immediately. Refer the requesting agency to the EDIT office; that office will provide guidance regarding the appropriate actions to be taken.

7.2. Responding to security and abuse incidents

All users and units have the responsibility to report any discovered unauthorized access attempts or other improper usage of Georgia Tech computers, networks, or other information processing equipment. If you observe, or have reported to you (other than as in 7.1 above), a security or abuse problem with any Institute computer or network facilities, including violations of this policy:

- Take immediate steps as necessary to ensure the safety and well-being of information resources. For example, if warranted, a system administrator should be contacted to temporarily disable any offending or apparently compromised computer accounts, or to temporarily disconnect or block offending computers from the network (see section 5.6).
- Ensure that the following people are notified: (1) your Computing Support Representative, (2) your unit head, (3) the Information Resources Security Coordinator (IRSC), who is located within the Office of Information Technology.

The IRSC will coordinate the technical and administrative response to such incidents. Reports of all incidents will be forwarded to Student Services (for apparent policy violations by students) or the unit head (for employees), and to the Executive Director for Information Technology and the Chief Information Officer.

7.3. First and minor incident

If a person appears to have violated this policy, and (1) the violation is deemed minor by OIT, and (2) the person has not been implicated in prior incidents, then the incident may be dealt with at the OIT or unit level. The alleged offender will be furnished a copy of the Institute Computer and Network Usage Policy (this document), and will sign a form agreeing to conform to the policy.

7.4. Subsequent and/or major violations

Reports of subsequent or major violations will be forwarded to Student Services (for students) or the unit head (for employees) for the determination of sanctions to be imposed. Units should consult the Office of Human Resources regarding appropriate action.

7.5. Range of disciplinary sanctions

Persons in violation of this policy are subject to the full range of sanctions, including the loss of computer or network access privileges, disciplinary action, dismissal from the Institute, and legal action. Some violations may constitute criminal offenses, as outlined in the Georgia Computer Systems Protection Act and other local, state, and federal laws; the Institute will carry out its responsibility to report such violations to the appropriate authorities.

7.6. Appeals

Appeals should be directed through the already-existing procedures established for employees and students.

Policy rev. 1994-08-08
HTML editing rev. 1996-06-05
Back to Table of Contents.

UNIVERSITY OF ILLINOIS
AT URBANA-CHAMPAIGN

CAMPUS ADMINISTRATIVE MANUAL
Emergency Plans, Environmental
Health and Safety, Security, and
Risk Management
Section V/C - 4

Date Issued: April 17, 1995
Issued by: Division of Public Safety
and Risk Management
Approved by: Vice Chancellor for Administration
and Human Resources

COMPUTER SECURITY

Campus units acquiring computer hardware should plan in advance for proper security. When properly secured hardware is damaged or stolen, the criteria and procedure for seeking financial assistance for reimbursement are described in this policy.

Campus departments have the primary responsibility for properly securing their computer hardware.

Computers and office/lab equipment of the size that could be easily removed should be acquired with the understanding that the cost of a proper security device is a part of acquisition. The campus does not have insurance to cover losses sustained through vandalism, theft or burglary, yet such losses can have a severe negative financial and operational impact. Therefore, it is essential that campus departments assume primary responsibility for securing computers and other office/lab equipment or areas where such items are located.

The Office of Vice Chancellor for Academic Affairs may assist campus departments to restore/replace computers and other office/lab equipment if:

- Campus funds are available, AND
- The department sustaining the loss had security measures in place which had been approved by the University Police Crime Prevention Specialist when the loss occurred.

Approved security measures include:

1. The use of an Anchor Pad or similar device when
   a. The value of the equipment item exceeds $4,000, AND
   b. The location lacks an approved level of security when not in use.
2. The use of a Cable Locking Device when
   a. The value of the item is less than $4,000 AND
   b. The location lacks an approved level of security when not in use.
3. The use of approved alternative security devices/measures for perimeter protection of office/lab with multiple items. These devices/measures may include door/window locks, alarm systems, key controls, etc.

4. Approved supervision of unsecured items when an otherwise secure office/lab is open for operational purposes.

University Police Crime Prevention Specialist/Campus Risk Manager need not be consulted when an Anchor Pad or Cable Locking Device is properly utilized per #1 and #2 above. For the determination of "an approved level of security" as described in #1 and #2 and conditions of #3 and #4, the Crime Prevention Specialist within the University Police Department <u>must</u> be consulted. Departments are strongly encouraged to be proactive and have a Crime Prevention Specialist from the University Police analyze the areas where computers and other office/lab equipment are kept.

Requests for financial assistance to cover loss(es) should be directed to the Office of the Vice Chancellor for Academic Affairs, Swanlund Administration Building, MC-304. The Vice Chancellor for Academic Affairs (or his/her designee) will then request a loss site analysis by a University Police Crime Prevention Specialist to determine if security measures as outlined in this policy were in place at the time of the incident.

The University Police Crime Prevention Specialist will document the existence or lack of approved security devices/measures on site and recommend assistance accordingly. (It is highly unlikely assistance will be provided any department that had not properly utilized an Anchor Pad or Cable Locking Device, or consulted a University Police Crime Prevention Specialist in advance for approval of alternative security measures.)

Campus policy does not prohibit the acquisition, with nonstate funds, of insurance for loss(es) of computers and other office equipment. However, such coverage may not be cost-effective given the type of loss(es) likely to be suffered from theft/burglary. Advice on this specific matter is best obtained from the University Risk Management Office at 333-3113.

Questions concerning this policy should be directed to the Associate Vice Chancellor for Academic Affairs, 3-4493, or Campus Risk Manager, 3-4660.

UNIVERSITY OF ILLINOIS
AT URBANA-CHAMPAIGN

CAMPUS ADMINISTRATIVE MANUAL
Use of Services and Stores Policies
Section VII/B - 12

Date Issued: May 27, 1992
Approved by: Vice Chancellor for Administration
and Human Resources

ACQUISITION POLICY FOR OPERATING SYSTEMS WITH PERSONAL COMPUTER PURCHASES

The UIUC prohibits copying of copyrighted computer software and may require that an operating system be purchased with each personal computer system.

General Policy

In recognition of the fact that computer software is copyrighted material and that software licensing requirements normally prohibit the copying of software for use with more than one personal computer system, it is the policy of the University of Illinois at Urbana-Champaign to require that an operating system (or disk operating system, i.e., DOS) be purchased with each personal computer system acquired.

This policy shall apply to personal computers acquired through the Purchasing Division, the Computer Center at Central Stores, or via the Departmental Purchase Order procedure.

Exceptions

An operating system will not be required to be purchased with a personal computer system in the following circumstances:

A. The operating system software to be used with the new personal computer system is currently owned by the department purchasing the system and is not utilized with an existing personal computer system.

B. The operating system software to be used with the new personal computer system is currently owned by the department purchasing the system and can be legally copied for use with the new system(s) in accordance with the software's licensing agreement.

C. The operating system software to be used with the new personal computer system is "bundled" with the personal computer system being acquired and is included in the purchase price of the new system. In this instance, the operating system may be either installed or uninstalled.

D. The operating system software to be used with the new personal computer system is a network version that is licensed for use with more than one personal computer system.

It is the responsibility of department heads of units acquiring personal computer systems to inform their faculty and staff members of this policy.

Questions concerning this policy statement should be directed to the Associate Vice Chancellor for Administration and Human Resources, 4-4457.

DRAFT

UIUC Computing and Networking Policies

1.0 Purpose

The University of Illinois at Urbana-Champaign provides extensive computing and network communications services at the campus level. Most services are available to the campus community without charge. In recent years these services, especially those involved in electronic communications, have become necessities for nearly everyone on campus. They are now considered part of the campus infrastructure, available to everyone on campus.

Near-universal utility and availability of most services without chargeback has raised questions for both the users of those services and those who manage them: who can use the services, in what quantity, for what purposes and in what ways? These questions are not new, but the circumstances of their posing often are. Although existing laws and policies frequently offer guidance, judgments must be made in their application to new areas. In other instances decisions must be made based only on analogy to existing services or knowledge of the requirements of the common good.

The campus network represents a new communications resource whose very design requires shared and cooperative use. The rules for sharing have evolved from experience and, while they continue to develop with the technology, it is useful to document their present state. Just as commonly accepted rules of the road contribute immeasurably to the safety and value of the highway system, a common understanding of the conventions of use of the campus network enhances its utility to the campus.

For the first time in the short history of networking the rate of growth in demand is threatening to exceed advances in capacity offered by new technology. This is evidenced both on campus and in the world at large. It is prudent to consider now, before problems develop, the levels of service members of the campus should assume and how needs beyond those levels might be accommodated.

The primary purpose of this document is to state the policies that govern the use and management of campus computing and networking resources. Because of the importance of the network and its relative newness to the campus, network-related policies are predominant in this document. These policies establish the conventions which make management and shared use of the network possible and which maximize the network's utility to the campus.

A second purpose for this document is to define the levels of service that the campus community should assume to be part of the campus infrastructure. Service beyond these levels can often be provided by special arrangement, and possibly for a fee.

Unless explicitly applicable only at the campus level, policies stated here extend to computing and network communications equipment in all departments.

2.0 Assumptions

The following general statements are considered as given. They provide the basis for making the specific recommendations that appear here and for deriving answers to future policy questions. The assumptions:

a) The laws of our state and nation apply to the use of computing and network services provided by the campus.

b) Similarly, general University policies apply.

c) The accepted rules of etiquette and courtesy extend to electronic communications.

d) CCSO is responsible for the design, operation and management of the computing and network communications services provided at the campus level. Responsibilities include:
   - The choice of protocols supported by the network.
   - The definition of campus standards necessary for efficient operation of the network or for the security of transmitted data and networked computers.
   - Application of network management policies adopted by the campus to ensure inter-operability of departmental LANs.

e) CCSO is the campus' representative to the Internet community and is responsible for ensuring that the campus is a responsible member of that community.

3.0 Definition

The term UIUCnet when used in this document is broadly defined to include the campus computer and data communications infrastructure, independent of ownership. It includes the campus backbone and local area networks, all equipment connected to those networks that are managed by UIUC personnel, and all computers in the uiuc.edu address domain.

4.0 Policy

The policies stated below deal with known concerns and in aggregate do not necessarily form a comprehensive policy statement. Network communications is changing rapidly both in terms of technology and application and additional policy questions will surely arise in this area.

Use of UIUCnet is governed by the policy statements given here, other relevant University policies, and all applicable laws. Violation of these policies and laws may result in the withdrawal of services.

CCSO's management of campus computing and network services will normally be in accordance with policies stated here. However, in emergency situations CCSO may take any action needed to protect the integrity of the UIUCnet environment.

4.1 The following statements define the proper and authorized use of UIUCnet:

a. Use of UIUCnet is limited to legitimate users as defined in Appendix A.

b. UIUCnet is provided in support of the educational, research and public service missions of the University and its use must be limited to those purposes. Specifically, UIUCnet may not be used by non-University entities except as specified by contract and may not be used for commercial purposes.

c. Legitimate University users associated with a non-University enterprise may use their UIUCnet connectivity when working for that enterprise only if such use is permitted by the University Guidelines and Procedures for Conflict of Interest.

d. Legitimate non-University users may use their University provided accounts and Internet access only in conjunctions with their university-related activities.

e. UIUCnet resources may be used in support of organizations identified in Appendix A. While it is appropriate for the WWW home pages of these organizations to provide some information about external organizations, clubs, commercial entities, etc., the UIUCnet connected equipment may not be the primary source of that information.

4.2 The following statements clarify the responsibilities of UIUCnet users:

a. University supplied network IDs and computer signons are the property of the University. They are the keys that give access to campus services. Passwords associated with network IDs and computer signons should never be shared.

b. Electronic mail and other forms of electronic communications should be used in a responsible, courteous manner. All such communications must carry the proper identity of the sender (except where allowed by the server ANONYMUS@uiuc.edu.)

c. Users should understand the weak privacy afforded by electronic data storage and electronic mail. Users should not normally commit confidential information to either.

Under the Freedom of Information Act (FOIA), electronic files are treated in the same way as paper files. Documents in the files of employees of the State of Illinois are considered to be public documents, and may be subject to inspection through FOIA or subject to subpoena in the case of a lawsuit.

The contents of electronic messages might be seen by a system administrator in the course of routine maintenance. In addition, electronic mail systems store messages in files (e.g. the file containing a user's inbound mail.) These files are copied to tape in the course of system backups. The contents of these files and the copies on system backup tapes are subject to the liabilities stated above.

For more information, see section III-18 (Electronic Mail Advisory) of the Campus Policy and Procedures Manual. An on-line version of this manual can be found through the UIUC web page which lists it under the heading "Resources and Services."

d. Individual units that provide access to UIUCnet are responsible for ensuring that use is limited to legitimate users and is consistent with University policies and with contractual obligations governing the software or services offered on UIUCnet.

e. Information servers (e.g. WWW and gopher servers) must display the Unit, name and e-mail address of the University person responsible for maintaining the information displayed.

f. The use in electronic publications of the University's name or of trademarks and logos must follow the guidelines provided by the University's Office of Publications.

g. Any University program which, in the interest of collaboration with an external entity, wishes to provide it with Internet access or to host non-university materials on a UIUCnet connected server must consult with CCSO beforehand to discuss appropriateness and alternatives.

4.3 The following statements clarify CCSO's responsibilities in managing UIUCnet:

a. Any use of UIUCnet that consumes so many resources as to noticeably degrade services to others will be reviewed by the host LAN's network administrator or system administrator and CCSO. Exceptional measures such as suspension of accounts or lowering the service priority of the offending application may be taken if needed to protect the quality of service to others.

b. CCSO will work with any unit to develop a network to meet its needs. However, needs directly related to the University's education, research or public service missions have first claim on resources. If needs must go unmet for lack of resources, it will be those not directly connected with one of the University's missions.

c. Networks serving the Residence Halls, Certified Student Housing and other housing are unusual because of their high density and unique environment. CCSO may impose special restrictions on their use if needed to protect the quality of service to the students who share those networks.

d. CCSO offers a news service which includes off-campus, commercially provided news groups as well as news groups that are local to this campus and restricted to it. The newsgroups provided and the length of time news postings are retained will be a function of experience, input from the campus community and available resources.

CCSO will not censor news in any way except in situations that are clearly illegal or which adversely impact the service as a whole. E.g. CCSO may elect not to distribute news groups that ignore copyrights or may refuse to handle newsgroups with no tie to an academic program if they would generate burdensome amounts of traffic on the network or campus computers.

All posts to the UIUC.* newgroups except those explicitly allowed through the "ANONYMUS" posting service must clearly identify the poster, most commonly by including the poster's network ID in the form "net-id@uiuc.edu" in the "From:' or signature fields of the post. CCSO will delete posts that do not identify the poster.

Posts which falsify the identity of the original poster constitute impersonation and are illegal. CCSO will deal with them as such.

e. In situations where there is reasonable evidence that University resources are being used illegally or contrary to University policy CCSO may limit or revoke access to the campus network, network services or campus computers. Systems that allow unauthorized use of copyrighted materials or licensed software will be disconnected from the network.

While CCSO does not monitor all use of UIUCnet, when it does discover illegal activities it will pursue them with the appropriate disciplinary or legal authorities and cooperate with law enforcement agencies.

f. Unless legally required to do otherwise, CCSO will afford the following confidentiality to users' data and electronic mail:
- CCSO will not examine the contents of a user's data files or electronic mail messages.
- CCSO will not grant access to a user's data files or electronic mail messages or give copies of them to a third party without the user's consent or, under exceptional circumstances, authorization by a Dean or Vice Chancellor.
- When, in the course of handling undeliverable electronic mail, CCSO will examine header fields that identify sender and receiver but will not read the contents of the messages themselves.

4.4 CCSO is responsible for the design or approval of departmental LANs that are connected to the campus network and their connections to the campus backbone. The following statements clarify policies and procedures pertaining to LANs and their connection to the campus backbone. The term 'LAN' as user here refers to the routers, repeaters, cabling and patch panels but excludes the server and other computers.

a. The current standard for attachment to UIUCnet is Ethernet. Whenever feasible and upon request from a department, CCSO will bring to a building a UIUCnet connection that is of Ethernet quality or better. The standard Ethernet access is 10Mbit per second, with the effective rate for any one computer somewhat less, depending on the number of communicating computers and the design of the networks between them.

b. Campus buildings that are served by the campus fiber distribution system will be connected to the campus backbone via fiber optic cable. When a building is not served by the campus fiber distribution system and where it would be cost-prohibitive to install, CCSO will use the most cost effective media available to provide connectivity, commensurate with the volume of network traffic expected.

c. Some campus units are housed in facilities not reached by the campus telecommunications wiring plant. CCSO will work with those units to design network connections to UIUCnet. Costs in excess of those normally required to provide Ethernet connectivity on campus must be paid by the unit. Due to the high cost of running fiber off campus, most off-campus connections will be provided over telecommunications circuits, possibly at much slower speeds than Ethernet.

d. Each LAN must have at least one designated network administrator, responsible for the administration and management of the LAN. It is strongly recommended that there be at least one backup system administrator.

   CCSO's Network Administrator Support group provides training, consulting and support at no cost to registered network administrators and their backups.

   CCSO's Network Operations Center will contact the network administrator if it detects a problem on the LAN or with a portion of UIUCnet connect to the LAN.

e. CCSO normally supports the installation of separate LANs for administratively separate units. There are cases, however, where units are sufficiently small that providing individual LAN attachments would not be cost effective. In these cases CCSO will ask the groups to share a single LAN. In such cases each cooperating unit may have its own support staff but there must be only one designated network administrator and backup per LAN connection. If there are specific requirements for isolation or security issues between the groups sharing a LAN, the CCSO Network Design Office will offer network designs to meet those requirements.

f. Only CCSO approved domains may be operated within UIUCnet address space. Publicly accessible Domain Name Servers must be approved by CCSO before they are placed in service.

g. Some servers connected to UIUCnet provide services or software that are restricted by licensing agreements to use by University students, faculty and staff. Some licenses may further limit use to Campus, College or Unit. Servers must be set up in such way as to give access to restricted services or software only to those eligible to use them.

h. Departments are responsible for the uses to which their local area networks and servers are put. In particular, departments are responsible for oversight of the materials published electronically on their servers for relevance to the department's mission.

i. Network administrators and the owners of local networks may develop their own network policies. These policies should not restrict access to campus services except where specific security concerns require it and may not mitigate policies stated here.

j. CCSO is responsible for the telecommunications wiring system on the UIUC campus. If portions of this system are used in the construction of a LAN, all such use must conform to campus standards.

k. If a LAN was designed and installed or approved by the CCSO Network Design Office, CCSO will work with the network administrator to identify and repair network hardware problems. There is no charge for this service which includes the provision of repair parts and spare units. Owning units are responsible for maintenance of all other LANs.

l. At the present time the campus backbone universally supports only the IP, AppleTalk and IPX protocols, with IP the only protocol supported for access to the Internet. A network administrator may support other protocols within a LAN but may not assume their availability on the campus backbone.

Because of the possible adverse effect on the performance of the campus network, AppleTalk and IPX must not be tunneled to other networks without first obtaining CCSO's approval.

m. When traffic levels on departmental LAN become a problem, CCSO will, upon request, evaluate the LAN and take performance measurements. The Network Design Office will then evaluate the LAN's performance and suggest design changes that will isolate traffic and improve performance. If this evaluation indicates a need for increased capacity on the link between the LAN and the campus backbone, CCSO will attempt to provide additional bandwidth between the LAN and the backbone. The actual implementation and cost sharing will be worked out on a case-by-case basis.

4.5 The security afforded by commonly used operating systems and by current networking technology is often weak. Because of the interconnections provided by the network, a security violation on one machine can threaten security of other systems on the network. Policies in this section describe the steps that will be taken in response to security threats. They also describe circumstances when data normally considered private can be collected and examined by an individual managing a LAN, server, or system.

a. Any security violation that represents a significant misuse of University resources will be brought to the attention of the appropriate authorities.

b. In the event that CCSO judges that a LAN presents an immediate security risk to UIUCnet equipment, software, or data CCSO may, without notice, terminate or restrict the LAN's network connection.

If there is no immediate risk, CCSO will bring the matter to the attention of the LAN's network administrator. If CCSO is unable to resolve the problem at this level it will contact the unit head.

c. In the event that CCSO judges that an account on one of it's multi-user systems presents an immediate security risk, CCSO may inactivate the computer account without notice.

d. The administrator of a server or UIUCnet connected computer is responsible for the security of that system.

With the exception of servers of public information, a UIUCnet connected server or computer must require user authentication before allowing connections to it from the network. At minimum, this will require the connecting user to supply a unique userid/password.

The system administrator must monitor and log accesses and keep other system logs that could be useful in establishing the identities of individuals who use the system to breach network or system security.

The administrator of a server which distributes public information and which does not require user authentication must not provide unrestricted access to UIUCnet or Internet services.

e. Units that operate publicly accessible computers connected to UIUCnet must implement safeguards against network abuse appropriate to the network access available to users of those systems.

f. Any terminal server that grants network access through the phone system must authenticate each user, requiring at minimum a unique userid/password.

g. The owner of a private system (e.g. a desktop system in a faculty member's office) that is connected to UIUCnet is responsible for ensuring that the system is not used by unauthorized individuals.

h. Network data transmissions are not secure. Sensitive data should either be encrypted separately before transmission or a network transmission protocol which automatically encrypts every data should be used.

i. Software and hardware which permit the capture and examination of sensitive information must be used only by authorized personnel. Constraints on the use of these tools include:
   - These tools must be used with the knowledge of the network administrator of the affected network.
   - The minimum information needed to solve the problem must be collected from each packet. E.g. the part of the packet containing user data should not be captured unless needed to solve a problem.
   - These tools must be used only by individuals who know how to restrict their field of view to the minimum range prescribed here.
   - All data collected must be discarded as soon as it has served its purpose.
   - All information collected by these tools must be considered confidential. No disclosure of any kind can be made without approval of the Associate Vice Chancellor for Computing and Communications in consultation with legal counsel.

j. Managers of systems and network services have the right to log connections to their machines and services made via dialup or UIUCnet. The information recorded may include the source and destination for a connection and session start and end times. Logs maintained by CCSO's network servers may include additional information such as the user's network ID.

   Operators of multi-user systems have the right to keep logs of activities on their systems. The logs may include timestamps and commands issued.

   Network administrators will monitor users' data transmitted across the network only after obtaining appropriate administrative authorization or when asked to do so by a law enforcement agency. Any such monitoring will be done in such a way as to collect only the specific information authorized.

k. Units may establish policies governing monitoring of their own LANs that differ from those stated here, so long as those policies are made known to users of their LANs and do not mitigate the policies stated here.

l. Unless permission has been granted in an Allied Agency agreement or otherwise obtained from CCSO, a system connected to UIUCnet must not be used to provide network services or access to any person or organization not identified in Appendix A as a legitimate user. For example:
   - A desktop computer and modem on campus must not be used to provide network access to anyone who is not a legitimate user.
   - A UIUCnet connected machine must not be used to provide e-mail or e-mail routing services for persons or organizations that are not legitimate users.
   - No UIUCnet connected system may route traffic between UIUCnet and networks outside of the UIUC.EDU domain without the written approval of CCSO.

   When there is benefit to the University and when other conditions are met, units can arrange for CCSO to provide such services.

5.0 Management Guidelines

This section defines the limits for subsidized computing and network services and advises CCSO how it should manage those cases where needs exceed limits.

The principles which serve as the basis for recommendations that follow are listed below. By employing the same principles, others should be able to formulate recommendations for the management of new services consistent with those given here. The principles:

a. Entitled legitimate UIUCnet users can assume no-cost access to basic computing and network communications services. These are services planned and funded at the campus level and include both services of general use (e.g. network transport of files, e-mail, access to services available on the Internet, reasonable amounts of CPU time and disk space) and specialized services installed for use by a subset of the campus community (e.g. access to very fast computers, large amounts of memory.)

b. CCSO must protect the quality of basic computing and network communications services from degradation caused by uses not considered at the time the services were implemented.

c. If use of a service by a project or individual seriously degrades its value to others, CCSO should first try to help the project or individual obtain the needed service without seriously impacting others. For example, CCSO might:
   - adjust schedules or relocate equipment to minimize adverse impact
   - upgrade the campus infrastructure, assuming money is available and implementation timelines permit
   - help the individual or project seek funds to purchase alternate equipment, software, or services.

d. If attempts to find a mutually satisfactory solution fail, CCSO may ask the project or individual to:
   - modify use of the service to eliminate the adverse affect on others sharing the same service, and/or
   - pay some or all of the incremental charges associated with delivering the service without adverse impact on others

5.1 Management Guidelines - Network Bandwidth

The guidelines stated below pertain only to the campus network. Guidelines for the use of departmental subnets and targets for available bandwidth per port on subnets will vary by installation and are the responsibility of the respective network managers. Similarly, traffic related problems local to a subnet must be solved by the unit that owns the subnet.

No statements made here about reasonable bandwidth expectations apply to transmissions crossing the Internet. The speed of such transmissions is subject to factors beyond campus control.

5.1.1 Residence Hall Networks

The newer equipment used to build the Residence Hall networks measures the volume of traffic through the b-jack in each room. For this network:

a. Residence hall students should assume availability of a maximum of 500MB/day of network capacity for each room. CCSO may ask residents of a room generating traffic in excess of this threshold to reduce the level of traffic or move the service to a more appropriate network location.

b. The 500MB/day threshold should be periodically reviewed by CCSO and raised as technology permits.

5.1.2 Campus Backbone

The older equipment used to build the campus network measures traffic only at the building level. Measurements at the machine level can be made only with the use of a special monitor that can be targeted at a specific machine. The lack of readily available machine-specific data makes it impossible to implement volume-based guidelines of the kind used for the Residence Hall networks. Therefore only the following general guidelines can be given at this time:

a. As a guideline, a network user should expect to be able to transmit no more than an average of 35KB/sec across the campus network and should expect to transmit a volume of data each day that is normal and customary. The definition of ‘normal and customary’ will vary by department but should not be so great as to reduce service to others below 35KB/sec.

b. If CCSO identifies an individual as consistently transmitting a volume of data so great as to adversely impact other users of the campus network, CCSO should discuss the problem with the individual to ask that use of network bandwidth be reduced or that the machines involved be moved to a more appropriate network location.

c. Extensive uses of new applications that consume very large amounts of bandwidth on the campus backbone (e.g. video across the network, teleconferencing with video and voice) which have the potential of reducing campus network speed for others below the 35KB/sec level must be discussed with CCSO beforehand. It may be impossible to accommodate some applications immediately.

d. The data rate and volume limits used in these guidelines should be reviewed periodically by CCSO and adjusted upward as technology permits.

5.1.3 WWW Servers

Web servers are capable of generating more network traffic than most networked machines and thus separate volume-based guidelines are appropriate. A unit/project/individual operating a web server should assume the ability to transmit at most 500MB/day across the campus backbone. Any greater volume has the potential of adversely affecting other users of the campus backbone. CCSO may ask operators of web servers generating traffic in excess of 500MB/day to relocate their server to a more appropriate network location.

Note that use of shared resources other than the campus network may dictate a limit lower than 500MB/day. E.g. a web server operating on a multi-user systems operated by CCSO should normally transmit no more than 200MB/day to avoid impacting other users of those systems.

5.1.4 Recommendations

As the campus backbone is upgraded and metering at the machine level becomes available, network guidelines for the entire network should be modeled on those proposed above for the Residence Hall network. A machine transmitting more data per day than specified in the then current guidelines should be moved closer to the machines with which it normally communicates to minimize cross-campus traffic, or alternatively, the owner or department may be assessed a fee to upgrade the campus network to accommodate the greater load. Generators of very large amounts of campus network traffic should pay any extra cost the campus incurs to meet their needs.

We recommend that published guidelines for traffic volume be enforced, even if there is no immediate problem. To do otherwise would encourage people to ignore the guidelines and invite charges of capricious enforcement.

We recommend that the campus speed the use of ATM for the campus backbone and switched Ethernet technology for departmental LANs. In addition to providing the extra bandwidth that will soon be needed anyway, ATM will provide tools to allocate network bandwidth as needed and greatly simplify the handling of network applications that require high guaranteed bandwidth.

University of Indiana

OFFICE OF INFORMATION TECHNOLOGIES

POLICIES

- □ **Account Structure and Access to Services**
- □ **Political Use of University Computing Resources**
- □ **Computer Users' Privileges and Responsibilities**
- □ **Data Collection Policy**
- □ **Policy: Providing Content on the National Information Infrastructure**
- □ **Policy: Community Access K-12 to the Internet**
- □ **Policy: Termination of Computer Accounts**
- □ **Policy: Academic Computing Policy Committee Statement of Electronic Mail Access for Mass Distributions**
- □ **Policy: Policy on Servers Installed on UCS Resources**
- □ **Policy: The NSFNET Backbone Services Acceptable Use Policy**
- □ **Policy: Password Sharing**
- □ **Policy: Software Copying**
- □ **Policy: Email Surveys**
- □ **Policy: Community Access to the Internet**
- □ **Policy: Draft Policies Under Review**
    - □ **Information Security Standards for Access to Institutional Data**

UCS pubs

Fall 1996

Computer Users' Privileges and Responsibilities

Table of contents

Introduction

This document constitutes a University-wide policy for the management of computer data networks and the resources they make available, as well as stand-alone computers that are owned and administered by Indiana University. The policy reflects the general ethical principles of the university community and indicates, in general, what privileges and responsibilities are characteristic of the university computing environment. Because some networks operate in environments in which some of the specific items in this policy do not apply, system administrators are free to create policies that are at variance to this one. In such cases the system administrators should make relevant variances known to their users.

CONTENTS

Terminology

A number of terms used below have very specific meanings in the context of this document. We define them here:

- □ Networked computer - A computer system that is connected to any IU data network.
- □ Shared computing resource - A networked computer and its peripherals that can be used by more than one person.
- □ Central - Refers to networked computers and peripherals purchased, maintained, and operated by University Computing Services and made available to the entire university community.
- □ Campus - Refers to networked computers and peripherals purchased, maintained, and operated by

the computing center of a given IU campus and made available primarily to that campus community.

□ Departmental - Refers to networked computers and peripherals purchased by university departments or other administrative units, primarily for the use of the unit's personnel.

□ Individual - Refers to networked computers purchased for use by an individual member of the university community, and which can be made available to other individuals or groups.

□ System manager - The person or group responsible for the operation and security of one or more networked computers (the person or group with system privileges).

□ System administrator - The person having executive authority over one or more networked computers.

CONTENTS

General Policies

Computer use has become an essential part of many university activities. While much computing is now done on privately controlled computers (personal computers, workstations, and so forth) most information sources and telecommunications systems reside on shared, central computers, or use shared networks. Distributed resources such as microcomputer clusters provide additional computing tools. University Computing Services (UCS), together with computing centers at each campus, as well as many academic departments and administrative units, have responsibility for providing and maintaining shared computing tools. General policies regarding the resources it provides are outlined below.

□ Access - Indiana University will provide access to appropriate central and campus computing resources, and to their attached networks, to all members of the university community whose work requires it. Fees are charged for some services.

□ Availability - Indiana University will make its central and campus computing resources and networks available to users with the fewest interruptions possible.

CONTENTS

Security

Central and campus resources

Indiana University will help users of its central and campus shared computing resources protect the information they store on those resources from accidental loss, tampering, or unauthorized search, or other access. Appropriate information on the security procedures implemented on each central or campus resource will be made available by the system administrator. In the event of inadvertent or non-malicious actions resulting in the loss of or damage to that information, or the invasion of the user's privacy, the IU computing centers will make a reasonable effort to mitigate the loss or damage. In most cases, however, ultimate responsibility for prevention and resolution of such problems rests with the user. Indiana University will assume no responsibility for the security of publicly accessible computer files. Users may request that arrangements be made to protect information stored on such resources. These requests will be honored at the discretion of the unit that manages the resource.

Other resources

The system administrators of departmental and individual computing resources are responsible for the security of information stored on those resources, for making appropriate information on security procedures available to users of those systems, and for keeping those systems free from unauthorized access.

Confidentiality

In general, information stored on computers is considered confidential, whether protected by the computer operating system or not, unless the owner intentionally makes that information available to other groups or individuals. Indiana University will assume that computer users wish the information they store on central and campus shared computing resources to remain confidential. IU computing centers will maintain the confidentiality of all information stored on their computing resources. Similarly, privileged information on account usage (i.e., that available only to users with system privileges) will be held in confidence. Requests for disclosure of confidential information will be reviewed by the administrator of the computer system involved. Such requests will be honored only when approved by university officials authorized by the campus involved, or when required by state or federal law. Except when inappropriate, computer users will receive prior notice of such disclosures. [Note: Indiana State law requires that public records be made available to any citizen who requests them. Exceptions are made for records concerning research conducted under the auspices of an institution of higher education; examinations and students' scores; intrauniversity or interagency advisory or deliberative material communicated for the purpose of decision making; diaries, journals, or other personal notes serving as the functional equivalent of a diary or journal; administrative or technical information that would jeopardize a recordkeeping or security system; and computer software owned by the university or entrusted to it.]

CONTENTS

Censorship

Free expression of ideas is central to the academic process. IU computer system administrators will not remove any information from individual accounts unless the appropriate system administrator finds that:

- □ The presence of the information involves illegality (e.g., copyrighted material, software used in violation of a license agreement).
- □ The information in some way endangers computing resources or the information of other users (e.g., a computer worm, virus, or other destructive program).
- □ The information is inappropriate, because it is unrelated to or is inconsistent with the mission of the university, involves the use of obscene, bigoted, or abusive material on IU resources, or is otherwise not in compliance with the legal and ethical usage responsibilities listed in the section, "Responsibilities of the User."

IU computing centers may remove from central or campus computers any information that is inappropriate, as defined above. Guidelines for appropriate use of each Indiana University bulletin board system shall be available on that system. Users whose information is removed will be notified of the removal as soon as is feasible. Users who wish to appeal such removal of information may do so through an appeals board made up of the governing body appropriate to the status of the user.

CONTENTS

Responsibilities of the User

Access to computing resources is a privilege to which all university faculty, staff, and students are entitled. Access may also be granted to individuals outside the university for purposes consistent with the mission of the university. Certain responsibilities accompany that privilege; understanding them is important for all computer users. These responsibilities are listed below.

Institutional purposes

Use of IU computing resources is for purposes related to the university's mission of education, research, and public service. All classes of computer service user may use computing resources only for purposes related to their studies, their instruction, the discharge of their duties as employees, their official business with the university, and their other university-sanctioned activities. The use of IU computing resources for commercial purposes is permitted only by special arrangement with the appropriate computing center or computer system administrator.

Security

The user is responsible for correct and sufficient use of the tools each computer system provides for maintaining the security and confidentiality of information stored on it. For example:

- □ Computer accounts, passwords, and other types of authorization are assigned to individual users and should not be shared with others.
- □ The user should select an obscure account password and change it frequently.
- □ The user should understand the level of protection each computer system automatically applies to files and supplement it, if necessary, for sensitive information.
- □ The microcomputer user should be aware of computer viruses and other destructive computer programs, and take steps to avoid being their victim or unwitting vector.

Legal usage

Computing resources may not be used for illegal purposes. Examples of illegal purposes include:

- □ Intentional harassment of other users.
- □ Intentional destruction of or damage to equipment, software, or data belonging to IU or other users.
- □ Intentional disruption or unauthorized monitoring of electronic communications.
- □ Unauthorized copying of copyrighted material.

Ethical usage

Computing resources should be used in accordance with the high ethical standards of the university community as desacribed in the "Code of Student Ethics" and the "Academic Handbook." Examples of unethical use follow; some of them may also be illegal.

□ Violations of computer system security.

□ Unauthorized use of computer accounts, access codes, or network identification numbers assigned to others.

□ Intentional use of computer telecommunication facilities in ways that unnecessarily impede the computing activities of others (randomly initiating interactive electronic communications or e-mail exchanges, overuse of interactive network utilities, and so forth).

□ Use of computing facilities for private business purposes unrelated to the mission of the university or university life.

□ Academic dishonesty (plagiarism, cheating).

□ Violation of software license agreements.

□ Violation of network usage policies and regulations.

□ Violation of another user's privacy.

Facilitative usage

IU computing resource users can facilitate computing in the IU environment in many ways. Collegiality demands the practice of facilitative computing. It includes:

□ Regular deletion of unneeded files from one's accounts on central machines.

□ Refraining from overuse of connect time, information storage space, printing facilities, or processing capacity.

□ Refraining from overuse of interactive network utilities.

Sanctions

Violation of the policies described above for legal and ethical use of computing resources will be dealt with seriously. Violators will be subject to the normal disciplinary procedures of the university and, in addition, the loss of computing privileges may result. Illegal acts involving IU computing resources may also be subject to prosecution by state and federal authorities. This policy is endorsed by the Academic Computing Policy Committee (ACPC), the Administrative Computing Advisory Committee (ACAC), the Academic Computing Coordinating Committee (ACCC), University Computing Services Deans and Directors, the Academic Deans, the Faculty and Staff Councils, the Academic Program and Priorities Committee, and the Indiana University Student Association (IUSA), fall 1996. B9108.IU0001

CONTENTS

Last updated: fall 1996
URL: http://www.indiana.edu/~ucspubs/iu001/
Comments: pubster@indiana.edu

Staff Internet Handbook
Providing Electronic Information and Using the Internet at the Library of Congress

September, 1995

CONTENT

This staff guide is divided into four parts:

1) **Internet Policies of the Library of Congress: Part I,** ***Providing Electronic Information on the Internet at the Library of Congress.*** Establishes the Library policy and guidelines for providing electronic information to Congress and the public. It includes a copy of the *Internet Dissemination Approval Form.*

2) **Internet Policies of the Library of Congress: Part II,** ***Use of the Internet by Library of Congress Staff.*** Encourages staff use of the Internet to provide high-quality service to LC constituents, enhance service, and promote staff development.

3) **Information for Staff on Internet Dissemination Tools, Management Responsibilities, and Library-wide Teams.** Provides more detailed information to staff on types of information and Internet tools available, Library-wide teams dealing with Internet, and institutional responsibilities for Internet maintenance.

4) **Information for Staff and Managers on Internet Training Rooms, Internet Training Materials, and Internet Training Courses and Services.** Provides information on training rooms available in the Library, training materials available for teaching staff to use the Internet, and Internet courses available via FLICC/FEDLINK and other "for-fee" training vendors in the D.C. metropolitan area.

NOTE: An electronic copy of this document is available in WordPerfect 5.1 format via the Library's staff FTP site (URL: **ftp://staff.loc.gov/pub/docs/policy/int_hand.wp**)

TABLE OF CONTENTS

Staff Handbook:
Providing Electronic Information and Using the Internet at the Library of Congress

PART 4: INFORMATION FOR STAFF AND MANAGERS ON INTERNET TRAINING ROOMS, INTERNET TRAINING MATERIALS, AND INTERNET TRAINING COURSES AND SERVICES

INTRODUCTION

Staff Internet Handbook:
Providing and Using Electronic Information
at the Library of Congress

The Library of Congress intends to use modern communication and networking technology to provide an environment that fosters internal communication, facilitates employee access to the growing array of electronic research tools, and supports improved methods of electronic information dissemination internally, to the U.S. Congress, and to the public. Technically, these objectives are achieved, in part, by connecting workstations throughout the Library campus to its internal network, and linking this network, in turn, to the Internet--the current implementation of the global "information superhighway."

The development of these technical capabilities requires the concurrent establishment of policies and guidelines that will enable the Library to achieve its strategic goals as a digital library and that will enable its employees to use these new technologies to their maximum benefit. The purpose of this document is to establish and present these policies and guidelines.

The policies incorporated in the first two parts of this document were approved by the Library Management Team in April of 1995 and were made available to staff via electronic means and through *Special Announcement No. 95-10* from the Office of the Librarian. Following the policies is additional information for Library staff on use of the Internet, management responsibilities for various Internet tools, lists of teams overseeing Internet development, and approaches to obtaining Internet training for Library staff.

Louisiana State University

Computer Usage Policy - March 1996

An individual who uses the computer resources provided by Louisiana State University should be aware of the following:

□ LSU computer resources are defined as all networks, processors, peripherals and supplies under the administration of the Office of Computing Services and various academic departments and colleges.

□ Use of the LSU computing and network resources is a privilege and not a right. As with all privileges, abuses will not be tolerated.

□ An individual faculty, staff, or student member of the LSU community may be issued a logonid to access one or more LSU computing resources. Accounts are issued on an individual basis. The proper use of a logonid is the ultimate responsibility of the individual under whose name it has been assigned. Logonid's are not to be shared.

□ Allowing use of your account, with or without revealing your password, to another individual will be viewed as computer fraud.

□ The use of another individual's logonid will be viewed as the stealing of LSU resources and as computer fraud.

□ Inappropriate use of LSU computer resources, the Internet, and other networks to which LSU is directly or indirectly connected will be deemed as abuse of computer privileges. Examples of inappropriate include but are not limited to the following: participation in network activities that place a strain on computer resources, the sending of obscene and or harassing messages, and the unauthorized access or attempted access of another networked computer system from any LSU computer resources.

□ Louisiana State University will take the following action against an individual who abuses or has gained unauthorized access to computer resources:

   □ Logonid(s) will be immediately deactivated.
   □ The appropriate administrative authorities will be notified. This includes LSU, state and federal agencies.
   □ The LSU Code of Student Conduct, LSU Policy Statements, state and federal statutes and laws will be used in determining appropriate action.

Back to the LSU Homepage

webmaster@www.lsu.edu

UNIVERSITY OF NEW MEXICO

Passed: July 1, 1991

UNM ETHICS CODE AND POLICY FOR COMPUTER USE

The Computer and Information Resources and Technology (CIRT) and other University of New Mexico (UNM) units provide computer services to a large number of faculty, staff, and students, as well as outside clients of the university. All computer users have two basic rights -- privacy and a fair share of resources. All computer users have the responsibility to use the UNM computer systems in an effective, efficient, ethical, and lawful manner. The ethical and legal standards that are to be maintained are derived directly from standards of common sense and common decency that apply to the use of any public resource within the university.

The following policy, rules, and conditions apply to all users of UNM computer services. Violations of any of the conditions are considered unethical and possibly unlawful. UNM views the use of computer facilities as a privilege, not a right, and seeks to protect legitimate computer users by imposing sanctions on those who abuse the privilege. Eliminating computer abuse provides more computing resources for users with legitimate computing needs. UNM's policy for use of its computing facilities is based on the United States Copyright Law and the laws of the State of New Mexico; Chapter 30, Article 45, Computer Crimes. This policy incorporates the definitions in the law and provides guidelines for appropriate use of computers, and outlines the administrative procedures that will be imposed on computer users who fail to comply with the policy. In accordance with established university practices, violations may result in disciplinary action which could result in expulsion from the university or dismissal from a position, and/or legal action.

Computer users are governed by the following provisions, which apply to all use of computers and network interconnections owned or administrated by UNM including university-wide microcomputer facilities.

I. COMPUTER USERS SHALL RESPECT THE INTENDED USE OF ACCOUNTS ESTABLISHED FOR THEIR USE

There are two types of accounts. One is a "University Account" which is the property of the University of New Mexico and is to be used only for university work. The contents of "University Accounts" shall be the property of the authorized user, subject to applicable university copyright and intellectual property policies and applicable federal and state laws. Access to information within these accounts by CIRT personnel may be authorized by the Associate Vice President for CIRT or and his/her designee if CIRT feels the integrity of the system is threatened. In other cases, authorization for non-user access shall be sought from the Vice President to whom the account user reports. All such access must be recorded and the user notified on an appropriate schedule. If the user is a student who was assigned the account by a faculty member, the faculty member also should be notified.

The other type of account is a "Private Account" which may be obtained from CIRT via contract at the personal expense of the private user. Such accounts are the property of the owner who is subject to the same conditions of use and laws as any other user, except the account may be used for personal, i.e., private use as contracted. Authorization for the use of the accounts is given by the Schools, Colleges, and other authorized units of the university for specific academic, administrative, or other authorized university purposes. Private accounts shall be used as specified in the contract. Attempts to: (a) defeat the security systems of any UNM computer, (b) circumvent the accounting system, (c) use an account without authorization, or (d) use accounts for other than their intended purposes, are prohibited. Use of an account which invades others' rights of privacy or which misappropriates others' data or files may subject the wrongdoer to both criminal and civil liability. UNM reserves the right to bar a computer user from a university or private account (after due process, including right of appeal) if impropriety is determined by the designated UNM officials.
Users should ensure that their account resource limits, both storage and memory, are sufficient for authorized work needs. If individual resources are low, the user should notify the course instructor or other authorized officials to arrange for additional resources. UNM reserves the right to limit a computer user's session if there are insufficient resources or if the user is determined by the responsible authorities

to be acting in an irresponsible or unlawful manner. UNM also reserves the right to cancel, restart, or place a hold on a job, process, or program to protect or to improve system performance if necessary. Game playing is not allowed on UNM's systems during any academic semester unless it is sanctioned by an instructor or the unit to which the system belongs. At other times the availability of games is at the discretion of the facility management and may be played when other use is low.

II. COMPUTER USERS SHALL RESPECT THE INTEGRITY OF THE SYSTEM

Computer users shall not intentionally develop or use programs which harass other computer users of the facility or which infiltrate the system and/or damage the software or hardware components of the system. Computer users shall use great care to ensure that they do not use programs or utilities which interfere with other computer users of the facility or which infiltrate or modify the system or an account. This includes all network links and/or damages caused to the software or hardware components of the system. Computer users shall not use network links for any use other than permitted in network guidelines (e.g., BITNET, Internet). The use of any unauthorized or destructive program may result in legal civil action for damages by any injured party, including the university, as well as criminal action.

UNM recognizes the value of academic game development, research on computer security, and the investigation of self-replicating code. Individuals who wish to use UNM central facilities under CIRT control to play games for recreational purposes may be limited by the UNM system administrator to minimize the effects. Restrictions on computer security and self-replicating code are defined in a manner that protects university and individual computing environments, but does not restrict or limit legitimate academic pursuits.

The well-being of all computer users depends on the availability and integrity of the system. Any defects discovered in system accounting or system security are to be reported to the appropriate system administrator so that steps can be taken to investigate and solve the problem. The cooperation of all users is needed to ensure prompt action.

The integrity of the system is maintained by password protection of accounts. A computer user who has been authorized to use an account may be subject to both civil and criminal liability if the user discloses the password or makes the account available to unauthorized persons without permission. Users are advised to obtain permission in writing where possible to protect themselves when using someone else's account.

Use of the electronic communication facilities (such as MAIL or PHONE, or systems with similar functions) to send fraudulent, harassing, obscene, indecent, profane, intimidating, or other unlawful messages is prohibited by state law. Also, the electronic communication facilities are not to be used for the transmission of commercial or personal advertisements, solicitations, promotions, destructive programs, or any other unauthorized use.

III. COMPUTER USERS SHALL RESPECT THE PRIVACY OF OTHER COMPUTER USERS

Computer users shall not intentionally seek, provide, modify information in, or obtain copies of files, programs, or passwords belonging to other computer users without the permission of those other computer users. This includes all system files and accounts.

The UNM system provides mechanisms for the protection of private information from examination by others. Attempts to circumvent these mechanisms in order to gain unauthorized access to the system and to private information are unlawful and certainly will be treated as a violation of UNM policy. Searching through non-public directories, libraries, or any other storage media to find unauthorized information likewise is a violation. Computer users, when requested in writing, shall cooperate with system administrators in investigations of system abuse. Users are encouraged to report suspected abuse, especially any damage to or problems with their files. UNM recognizes that files and mail messages are confidential. Authorized UNM employees may access computer users' files at any time during system maintenance and will report suspected unlawful or improper activities to the proper authorities.

IV. COMPUTER USERS SHALL RESPECT THE RULES AND REGULATIONS GOVERNING THE USE OF FACILITIES AND EQUIPMENT

Each UNM site has specific rules and regulations which govern the use of equipment and facilities at that site. Violation of these rules and regulations is grounds for disciplinary action. Each site has operators, consultants, and/or supervisors who have been given the responsibility to supervise the use of that site. Computer user cooperation with these individuals, and adherence to UNM policies is expected at all times. Students are encouraged to utilize CIRT and other UNM consulting services; however, obtaining program code from CIRT or other staff when forbidden by an instructor is prohibited.

V. COMPUTER USERS SHALL RESPECT THE PROPRIETARY RIGHTS OF SOFTWARE

All software protected by copyright shall not be copied except as specifically stipulated by the owner of the copyright. Protected software is not to be copied into, from, or by any UNM facility or system, except by license. This means that such computer and microcomputer software may only be copied in order to create backup copies, if so licensed. The number of copies and distribution of the copies may not be done in such a way that the number of simultaneous users in a department exceeds the number of original copies purchased by that department, unless otherwise stipulated in the purchase contract.

Pennsylvania State University

PENNSTATE

Center for Academic Computing

Computer Use Policies and Guidelines

Note that the University does not make all policies available electronically.

University Policy Manual

- □ AD11 University Policy on Confidentiality of Student Records
- □ AD20 Computer and Network Security
- □ AD23 Use of Institutional Data
- □ AD35 University Archives and Records Management
- □ ADG01 Glossary of Computerized Data and System Terminology
- □ AD02 Computer Facility Security Guideline

Student Guide to University Policies and Rules

- □ Policy Statement on Computer And Software Misuse

Center for Academic Computing Policies

- □ Access Accounts for Distance Education Students
- □ Access Accounts for Non-credit Courses or Seminars
- □ Password Policy
- □ Software Selection Policy
- □ Ethical Use of Software (EDUCOM Statement)

This information is provided by the Center for Academic Computing (CAC) at Penn State. Please address comments and suggestions to the editor. For assistance contact our Help Desk.

4. POLICY STATEMENT ON COMPUTER AND SOFTWARE MISUSE* (POL12, 5/5/96)

a. Access to and use of computer facilities, electronically stored data, and software shall comply with federal laws, the laws of the Commonwealth of Pennsylvania, and the rules and regulations of the University including those rules and regulations set forth in Administrative Policies AD-20 and AD-23 and Administrative Guidelines ADG-1 and ADG-2.* Misuse of computers, computer facilities, and software may violate federal or state criminal laws and may result in criminal charges against the user. Members of the University community may be subject to University sanctions, including disciplinary charges.

b. It is a violation of University regulations to:

(1) intentionally and without authorization, access, alter, interfere with the operation of, damage or destroy all or part of any computer, computer system, computer network, computer software, computer program, or computer data base.

(2) intentionally or knowingly and without authorization, give or publish a password, identifying code, personal identification number or other confidential information about a computer, computer system, computer network or data base.

c. University regulations apply to all University computers and computer equipment, computerized data and all data owned or held through agreement by the University. These regulations may also apply to computer equipment and data belonging to or held by agreement by members of the University community or others when violations are deemed to have a substantial adverse effect upon the University community or upon individual members of the University community.

d. It is important that members of the University community be aware of the intellectual rights involved in the unauthorized use and copying of computer software.

Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to the work of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, right to privacy, and the right to determine the form, manner, and terms of publication and distribution.

Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violation, may be grounds for sanctions against members of the academic community. (EDUCOM, 1987)

*University Policy Manual, AD-20, AD-23, ADG-1, and ADG-2

Syracuse University Computing & Media Services
*This document last updated: **11/30/95.***
Information expires: ***No expiration.***

Syracuse University's Computing Policy

Syracuse University, through Computing & Media Services, provides central computing facilities and services for the instructional, research, and administrative computing needs of the University. Access to the University's computing facilities and resources is a privilege granted to Syracuse University students, faculty, and staff. In addition, other individuals may be eligible for accounts (dependents and alumni, for example).

All users of the computing resources must act responsibly and maintain the integrity of these resources. The University reserves the right to limit, restrict, or extend computing privileges and access to its resources. Those who do not abide by the policies listed below are subject to revocation of computer privileges and possible referral to the University Judicial Board or other appropriate authority.

It is the responsibility of all users of computing resources to notify Computing & Media Services about violations of computer laws and policies, as well as about potential loopholes in the security of its computer systems and networks. The user community is expected to cooperate with CMS in its operation of computer systems and networks as well as in the investigation of misuse or abuse. Should the security of a computer system be threatened, user files may be examined under the direction of the appropriate authority. Any concerns, complaints, or reports of misconduct with regard to computing resources on campus should be reported to Charlene Kirchoff, Director of Client Services at 443-3631.

By using Syracuse University's computing resources, you agree to abide by the computing use policies listed here as well as those that might fall under the auspices of the Code of Student Conduct.

Syracuse University's Policies on Computing include, but are not limited to:

- □ **Do not "share" a computer account.** Do not try to obtain a password for someone else's computer account. Do not attempt to disguise the identity of the account or machine you are using.
- □ **Do not use Syracuse University's network resources to gain or attempt to gain unauthorized access to remote computers.**
- □ **Do not deliberately perform an act which will seriously impact the operation of computers, terminals, peripherals, or networks.** This includes, but is not limited to, tampering with components of a local area network (LAN) or the high-speed backbone network, otherwise blocking communication lines, or interfering with the operational readiness of a computer.
- □ **Do not run or install on any of Syracuse University's computer systems, or give to another, a program which could result in the eventual damage to a file or computer system and/or the reproduction of itself.** This is directed towards, but not limited to, the classes of programs known as computer viruses, Trojan horses, and worms.
- □ **Do not attempt to circumvent data protection schemes or uncover security loopholes.**
- □ **Abide by the terms of all software licensing agreements and copyright laws. In particular, you must not make copies of copyrighted software, unless Syracuse University has a site license specifically allowing the copying of that software.** Furthermore, you must not copy site-licensed software for distribution to persons other than SU faculty, staff, and students, nor may you copy site-licensed software for use at locations not covered under the terms of the license agreement.

□ **Do not deliberately perform acts which are wasteful of computing resources or which unfairly monopolize resources to the exclusion of others.** These acts include, but are not limited to, sending mass mailings or chain letters, creating unnecessary multiple jobs or processes, generating unnecessary or excessive output, or printing or creating unnecessary network traffic. Using the printers in the clusters as copy machines (i.e. printing multiple copies of papers, flyers, etc.) is also prohibited.

□ **Do not place any of the following type of information or software on any University-owned computer system or print on any University-owned printer: anything that infringes upon the rights of another person, that is abusive, profane, or sexually offensive to the average person, that consists of any advertisements for commercial enterprises, or that consists of information which may injure someone else and/or lead to a lawsuit or criminal charges.** (Examples of these are: pirated software, destructive software, pornographic materials, or libelous statements.)

□ **Do not harass others by sending annoying, threatening, libelous, or sexually, racially, or religiously offensive messages.**

□ **Do not attempt to monitor another user's data communications, nor may you read, copy, change, or delete another user's files or software, without permission of the owner.**

□ **Do not use any of Syracuse University-owned computers, workstations, or networks for other than a University course, research project, departmental activity, or personal communications. In particular, Syracuse University computing resources are not to be used for commercial purposes.**

□ **Limit recreational use** of any Syracuse University's computers or networks, if such use prohibits others from getting their classwork done. In particular, if you are using a machine in a public cluster for recreational purposes, and others are waiting for a machine to use for academic purposes, you are expected to give up your seat.

Any network traffic exiting the University is subject to the acceptable use policies of the network through which it flows, as well as to the policies listed here.

Help us improve to help you better. Give us some feedback on this page and whether or not the information and the way it is presented is useful to you.

Return to:

COMPUTING & MEDIA SERVICES

SYRACUSE UNIVERSITY
EMPLOYEE ACKNOWLEDGEMENT OF POLICIES REGARDING ACCESS, USE, AND SECURITY OF UNIVERSITY INFORMATION

NAME: ______________________________ SOC SEC NUMBER: _____ - ___ - ______

A. GENERAL POLICIES

Information contained in the University's administrative systems ('Information') is the property of the University and represents official University records. Employees who have access to this information, in all formats (printed materials, on-line systems, data files) accept responsibility for adhering to certain principles in the use and protection of that information.

1. Employees who have access to information are responsible for maintaining its confidentiality. Information remains under the control of the University, and its data custodians. Any use of this information for purposes other than originally authorized is prohibited.*

2. Employees are responsible for understanding the meaning and purpose of the information to which they have access, and may only use this information to support the normal functions of their administrative and academic duties. All information to which they have access, in printed or electronic format, must be maintained and disposed of in a secure manner. *

3. Employees may not use information in any manner which duplicates a function reserved by a University data custodian without the permission of that custodian. Examples of reserved functions are reports for government agencies, transcripts, employment verification, financial and budget reports, and enrollment reports.*

4. All University information is governed by data security policies published in the Administrative Policy Manual. In addition, disclosure of Student Records information is governed by the *Family Educational Rights and Privacy Act of 1974* which generally requires the written consent of the student. *

5. Printed information, (e.g., reports, labels, data files) may not be distributed outside the University without approval of the data custodian.*

B. COMPUTERIZED INFORMATION GUIDELINES

Access to any of Syracuse University's computerized information systems requires the approval of the data custodian responsible for that data. Specific guidelines govern computerized access, and all employees who become authorized users of these online information systems must comply with the following security procedures:

1. Never disclose your password.

2. Never use another person's sign-on ID.

3. Always sign off the system when finished; do not leave a terminal unattended while you are logged onto a system.

4. Never allow a student who does not have an authorized sign-on ID to access any of the University's Online systems.

5. Report all security violations to the Information Coordinator in your department, a data custodian or Information Systems.

C. ENFORCEMENT

Acts which achieve or attempt to achieve the unauthorized use of computer resources or the unauthorized use or copying of data or software owned by or in the care of the University are prohibited. Examples of unauthorized use of copying include attempts to alter systems, attempts to circumvent systems protection features, attempts to alter or destroy data, attempts of unauthorized access or copying of data or software, attempts to release data or software for which the attempter is not the University authorized processor or custodian, and the condoning, approving or directing of unauthorized use or copying. *

The University regards an unauthorized attempt to use or unauthorized use of computer resources or the unauthorized copying of data or software owned by or in the care of the University as an extremely serious violation of University policy. Violation of policy will result in appropriate sanction, and may also result in suspension or termination from University status as a student or employee, and/or in civil proceedings, and/or in criminal prosecution under Article 156 of the New York State Penal Code.*

I have read, understood, and retained a copy of the Acknowledgement, and agree to comply with the University policies and procedures described above.

____
Signature of Employee

Dated: ____/____/____

**Reprinted or paraphrased from the Syracuse University Administrative Policy Manual.*

recovery plan in which administrative systems operation would be resumed at an off-site location within several days of the time of the disaster. If there is a disaster, the data custodians for the various administrative systems supported by CMS are responsible for:

- Reprocessing all data between the time of the disaster and the time that the most recent disaster backup tapes were created (up to five work days).
- Having in place a contingency plan for continuing essential departmental operations for a period of up to several days, during which time all administrative computer system processing would be suspended.

POLICY ON UNIVERSITY DATA, SOFTWARE ACCESS, AND DATA SECURITY

All computers, software, and University data which consists of data, business records, and student records in any form - - electronic, paper, or other media - - belong to the institution. Any person committing an offense with respect to them may be subject personally to criminal sanctions and other liability.

Computer data and software that are created and maintained by the University, as well as vendor-licensed or copyrighted software used by the University, are vital assets. It is mandatory, therefore, that proper controls and procedures be employed to preserve and protect them. Computer data for the purposes of this policy are defined as institutionally owned and created data, processed either on the centralized computer facilities operated by Computing and Media Services or in any other Syracuse University organizational units with stand-alone, distributed, or remote computer processing facilities including, but not limited to, personal computers, local area networks, and distributed servers.

Acts which achieve or attempt to achieve unauthorized use of computer resources, or the unauthorized use or copying of computer data or software owned by or in the care of the University, are prohibited. Examples of unauthorized use or copying include: attempts to alter systems, attempts to circumvent system protection features, attempts to alter or destroy data, attempts of unauthorized access or copying of data or software, attempts to release data or software for which the user is not the University authorized processor or custodian, and the condoning, approving, or directing of unauthorized use or copying.

Under Article 156 of the New York State Penal Code, criminal sanctions are imposed for offenses involving computers, software, and computer data. The offenses include unauthorized use of a computer, computer trespass, computer tampering, unlawful duplication, and unlawful possession of computer related material. Improper or unauthorized access, or release or manipulation of, any University data in such form is included within those offenses.

The University regards an unauthorized attempt to use or unauthorized use of computer resources, or the unauthorized use or copying of data or software owned by or in the care of the University, as an extremely serious violation of University policy. Where appropriate, the University will cooperate with law enforcement authorities in prosecuting all persons who commit any such offense. Violation of policy will result in appropriate sanction, and may also result in suspension or termination from University status as a student or employee, and/or in civil proceedings, and/or criminal prosecution.

The Student Affairs section of this manual contains additional information regarding computer resources for students and the responsible use of those resources. It should be noted that the policies regarding improper use of resources, as outlined in the Student Affairs section, apply not only to students but to faculty and staff as well.

POLICY ON UNIVERSITY DATA

The purpose of the following guidelines is to insure that access to the University's computer data is authorized either electronically or in writing by the data custodian (see definition below). These policies apply to University data which is not classified as available for access to the general public.

- All requests for access to computer data, regardless of the data format or storage media, must be made to the appropriate data custodian.

- Requests for data access may be for a specific project, in which case the user must specify the data desired along with its intended use, or the requests may be for long-term access to specific categories of data. In either case, access will be granted only to support a function directly related to the information needs of the data user or the operations of that user's organizational unit (i.e. college, department, or program).

- Transfer of centralized computer data to other computer facilities will be done only with the express approval of the data custodian, and will be approved if the intended use of the data does not adversely affect the responsibilities of the data custodian to maintain and safeguard the data.

- The only official University reports are those auditable reports authorized by data custodians.

- In the situation when a request for data is denied and the requester wishes to appeal the decision of the data custodian, the appeal should be made to the Vice President for Research and Computing (VPRC). The VPRC has the authority to make a judgment and determine whether the data requester should receive access to the requested data. If either the data requester or the data custodian wishes to appeal the decision of the VPRC, that appeal should be directed to the Chancellor and the implementation of the decision of the VPRC shall be delayed until the Chancellor has had the time to make a judgment.

POLICY ON USE AND MANAGEMENT OF COMPUTER DATA

The defined responsibilities for the proper use and control of University computer data are based on the following organizational classifications: Data Custodian, Data Administration Committee, Information Coordinator, Data Processor, Data User.

Data Custodian. The custodian for computer data is responsible for creating, maintaining and using data to support the operation and information needs of the University. This data may reside either in centralized facilities maintained by Computing and Media Services or on distributed facilities in campus departments. In both cases the data is owned by the University and in the custody of the unit responsible for maintaining the data.

Each custodian of computer data is responsible for specific procedures governing access to and the use of University data, whether it is stored locally or in centralized computing facilities. Additional guidelines governing access to widely-used data may be found in the various custodians' sections of this manual. In all cases, the data custodian is responsible for:

- Establishing collection, maintenance, access, distribution, and utilization criteria for the data.

- Defining the criteria for archiving or destroying the data to satisfy retention requirements.

- Determining the value of the computer data to the functioning of the organization and defining reasonable requirements for protecting the data asset.

- Developing a workable plan for resuming operations in the event a disaster destroys all computer data except those which have been stored off-site.

- Specifying data control and protection requirements to be adhered to by data processors and data users. This includes determining the data classification for data within their area of responsibility.

DATA ADMINISTRATION COMMITTEE

The Data Administration committee is composed of representatives from the major data custodial areas, Archives and Record Management, Internal Audit, and Computing and Media Services. Additional representatives from other areas of the University attend meetings as the need dictates. This group provides a forum for discussion of data-related issues and reports its recommendations and findings to the Administrative Computing Advisory Group.

The Data Administration Committee is responsible for:

- Providing general standards and guidelines on creation, maintenance, use, retention, and disposition of data.

- Making recommendations to the Administrative Computing Advisory Group for policies and guidelines on the creation and maintenance of University data.

Information Coordinators. Information coordinators are individuals within University organizations who handle a variety of computer security and data access-related functions.

Information Coordinators are responsible for:

- Handling access requests for administrative information applications from people in their organization.

- Insuring that staff in their organization who use University data are aware of their responsibilities as data users.

- Monitoring the status of staff in their area who have access to administrative information and maintaining the status of the person's access when their employment status or position changes.

- Participating in training and informational sessions sponsored by Computing and Media Services.

Data Processor. The data processor is any organizational unit possessing computer hardware, software, or any other media used to process University data.

Computing and Media Services is the institutionally designated data processor for all centrally stored computer data. This definition, however, also includes any organizational unit on campus which is storing University data locally and has therefore accepted responsibility for its storage and use.

The data processor is responsible for:

- Taking appropriate measures with respect to the processing of data to guard against unauthorized modification, destruction, or disclosure of data, whether accidental or intentional.

- Adhering to all custodian-specified protection and control criteria for data processed by its computer facilities.

- Establishing such standards, procedures, and guidelines as may be necessary to insure data security and to provide controlled access to confidential, privileged, or otherwise sensitive data.

- Implementing backup and secure off-site storage procedures in cooperation with the data custodian to preserve vital data along with the software and programs which process that data in the event of destruction or a disaster.

- Following reasonable standards with respect to the selection, design, testing, and documentation of hardware, software, and computer programs to ensure proper use and accuracy of processing results.

Data User. Data users are those individuals or organizational units with a need to have access to the University's computer data and who have been properly authorized by the data custodian to have the requisite access. Users who accept access to University data, regardless of the storage media or data format, also accept responsibility for adhering to certain principles in the use and protection of that data:

Data users are responsible for:

- Using the University's computer data only for the purposes for which they have been authorized.

- Understanding the meaning and purpose of the data to which they have access, and using this data only to support the normal functions of the user's administrative and academic duties.

- Obtaining the custodian's approval to disseminate the results of all studies using custodian-supplied computer data. Such derived data may be subject to review by the Internal Audit Department. The data custodian may deny or place limits on requests to disseminate the results of such studies.

- Complying with all reasonable protection and control procedures for computer data to which they have been given access.

- Producing a secondary copy of data only for the purpose of backup; otherwise, data users are not to transfer, duplicate, or recreate any computer data to which they have been given access without the written approval of the data custodian.

- Not using data for any application that duplicates a function reserved for the official data custodian without permission of the data custodian. Examples of reserved functions are:
    - Transcripts, grade reports, and University enrollment reports
    - Reports for government or funding agencies
    - Private or public release of data to outside parties such as students, parents, and the news media.

3.16 of the *Faculty Manual*, Edition 18, January, 1995 and subsequently amended. A sanction need not in every case be imposed. Where appropriate, sanctions for a person found to have violated those prohibitions may range from a verbal or written reprimand, to suspension of the faculty privileges and responsibilities, either with or without salary or benefits for a period not to exceed the remainder of the semester and the semester following hearing board action, to termination of contract or tenured position. In extraordinary circumstances, the Chancellor or designated representatives may suspend the accused person pending hearing of the charges.

Computing Resources

Computers, network access, and computer accounts are provided for Syracuse University community use consistent with the goals and standards of the University. Computing & Media Services (CMS) publishes usage policies in whole or in part in both electronic and print form. Electronic form includes SyraCWIS, the on-line information repository for the University. Print form includes the CMS publications Computing at a Glance and Newsline, information sheets distributed with new computer accounts, the Syracuse University handbook, and other publications as needed. Please contact Computing & Media Services for information on current policies.

A) Timesharing accounts are issued to University faculty, staff, and students for University purposes. These accounts must not be used for commercial purposes.

Every computer account issued by Syracuse University is the property and responsibility of the person in whose name it is issued. That individual must keep the account secure by keeping the password secret, by changing the password often, and by reporting to Computing & Media Services when anyone else is using the account without permission. Accounts are normally issued to a single user, and are not to be shared (anyone who needs an account should obtain their own account, not share someone else's). Using another persons' account (even with their permission) or allowing someone else to use an account makes both parties potentially liable to disciplinary action.

B) Improper use of interactive computer systems and networks is prohibited. The following are examples of improper and irresponsible uses of shared computer systems and the network:

- Harassment: Some examples include: obscene, threatening, or repeated unnecessary messages; continuing to send messages after a request to stop; and procedures which hinder a computer session.
- Destruction: Maliciously destroying any computer-stored material including that in primary memory.
- Unauthorized Use/Access: Actions that give simulated sign off messages, public announcements, or other fraudulent system responses. Having or changing system control information (for example, program status, protection codes, and accounting information) is prohibited, especially when used to

defraud others, steal passwords, programs, or data files, or otherwise interfere with or destroy their work.

- Mail Forgery: Forging mail, usually to conceal the sender's identity.
- Chain Letters: Sending people material and requesting them to send additional messages to other people, such that the original material is repeatedly copied and forwarded.
- Theft/Unauthorized Use of Data: Data created and maintained by the University, or acquired from outside sources, are vital assets. Administrative, research, and other data at the University may be subject to a variety of use restrictions; consult the data's University "owner" for proper use.
- Program Theft: Unless specifically authorized, copying computer program(s) from University computers is a violation of copyright law.

C) Public computer clusters operated by CMS are a shared University resource, and are available on a first-come, first-served basis. A valid University or SUNY ESF ID card is required to use the clusters. Individuals playing games or engaging in other non-academic activities may be asked to give up their station when others are waiting to do academic work. Food and beverages are prohibited in the clusters. Clusters may be reserved for exclusive use by a class or group; schedules are posted on each cluster's door and published electronically to various newsgroups every week. Some clusters are owned by departments other than Computing & Media Services; contact those departments for their usage guidelines.

D) Mail Distribution Lists (often called LISTSERVs) facilitate e-mail discussions on specified topics. List owners have responsibility for list maintenance and membership, and have final say over content (list owners function as "benevolent dictators"). CMS may rename lists whose topics have changed, terminate lists due to resource constraints or relevance to the SU community, or take action regarding violation of University or computing policies. Posting of material unrelated to a list's normal content is strictly prohibited. Posting unrelated material to multiple lists ("spamming") will be grounds for account revocation.

E) Under Article 156 of the New York State Penal Code, criminal sanctions are imposed for offenses involving computers, software, and computer data. The offenses include unauthorized use of the computer, computer trespass, computer tampering, unlawful duplication, and unlawful possession of computer related material. Improper or unauthorized access to, or release or manipulation of, any student record in such form is included in such offenses.

All computers, software, data, business records, and students records of the University in any form, electronic or paper, belong to the institution. Any person committing an offense with respect to them may be subject personally to criminal sanctions and other liability. Federal laws may also apply to some circumstances.

F) Software Copyright: "The Copyright Laws of the United States prohibit unauthorized copying. Violators can be prosecuted or held liable for monetary damages."

In general, you may not install or use software without acquiring a license from the publisher (you may not copy it from a friend or other source). For further information, you can obtain a brochure about the ethical and legal use of software from the Information Center, 116 Hinds Hall.

G) Computer accounts are controlled by the person in whose name they are issued, and data files and programs stored under that account are considered private. However, if there is probable cause to believe such data files or programs contain information relevant to a University academic or administrative inquiry or legal proceeding, a person other than the authorized user may examine such data files or programs. Access to accounts and/or data may be granted to do computer systems or maintenance work; access to personal files will be limited to completing the systems and/or maintenance procedures.

Backup copies of all data on shared computers are made routinely to protect against loss of data. No exceptions can be granted. If you use shared computers, you must accept that these copies will be made. CMS takes great care that these copies are protected at least as well as the originals.

H) Waivers to some policies may be requested for specific projects, and will be reviewed on an individual basis. Under no circumstances will a waiver be granted that violates NY or other laws.

APPROPRIATE USE OF INFORMATION TECHNOLOGY

The University of Toronto is committed to ensuring a working and learning environment in which all persons treat others with humanity and respect. University information technology facilities include computing devices and associated peripherals, communications infrastructure and related equipment, facsimile machines, scanners, copiers, telephones, video and other multimedia devices and all forms of software.

Such resources and tools are made available to employees in support of their teaching, research, and administrative activities and to students in support of their respective academic objectives and requirements.

Their use is circumscribed by codes such as the Code of Student Conduct, the Code of Behaviour for Academic Matters, the Ontario Human Rights Code, and the Criminal Code of Canada in concert with various rules and guidelines adopted in local units.

Every users bears primary responsibility for the material he or she chooses to access, store, print, send, display or make available to others. The facilities may not be used in any manner to create, store, send, display or make available to others material which contravenes the relevant policies or statutes. When devices, such as portable computers, are the property of the user, the appropriate use expectations still apply when such devices are used to access University information technology facilities.

Failure to adhere to these guidelines may result in the suspension of access privileges as well as other action as deemed appropriate by the user's division, University of Toronto Computing and Networking Services and/or the University of Toronto.

Appropriate use of information technology includes, for example:

- □ respect for the rights of others
- □ respect for the property of others
- □ consideration of other persons using shared systems, equipment and facilities
- □ confidentiality in use of passwords and personal identification numbers
- □ a presumption of the right to privacy
- □ use of tools for the purpose for which they are intended
- □ adherence to the rules governing use of accounts, equipment, networks, or other facilities, whether the rules are established by the University of Toronto or by the organization providing these tools to the University, and
- □ adherence to etiquette and culture as defined in systems that you use

Inappropriate use of information technology includes, for example:

- □ unauthorized access, alteration, destruction, removal and/or disclosure of data, information, equipment, software, or systems
- □ deliberate over-extension of the resources of a system or interference with the processing of a system
- □ disclosure of confidential passwords, personal identification numbers and/or access devices or information for accounts, equipment, and telephone voice mail

- □ use of University facilities and resources for commercial purposes
- □ propagation of hate literature
- □ propagation of pornographic materials
- □ harassment, including sexual harassment
- □ theft of resources
- □ malicious or unethical use, and
- □ use that violates provincial or federal laws

Computing and Networking Services (UTCNS) Position Statement on Censorship

UTCNS does not and will not act as a censor of information available on our campus network but will investigate properly identified allegations arising from the University community and will comply with applicable federal and provincial laws. To the extent that the latter requires specifically identified information to be banned pursuant to a court order, UTCNS will make every practical attempt to comply with both the spirit and the substance of the law.

By way of clarification, it must be noted that there can be many practical reasons including network and storage resource constraints that would cause UTCNS to limit the numbers, types and storage retention periods of various information classes, either temporarily or permanently. Similar decisions which might further restrict the classes of information available locally can and should be made by local units, such as colleges and departments, consistent with the intended usage of available information and the capacity of local facilities.

Guidelines Regarding the Issue of Potentially Offensive Materials

The following statement was developed by a special committee created by the Vice-President and Provost and the Vice-President, Computing and Communications, 23/09/93.

These guidelines address the issue of potentially offensive information on the University's computer systems, whether generated locally or imported from other systems via the Internet. Other than the particular modality of the computer and network, the issues to be addressed are not generally technical. Any guidelines or procedures for handling this particular situation address only a single facet of a much broader policy issue regarding the production, storage, dissemination of and access to information available using information technology facilities. Rather than dealing with the global issue, these guidelines (in this section) focus only on handling, dissemination and display of objectionable material.

First, a guiding principle is the University will ensure that its efforts to create an environment in which all its members treat each other with respect extend to facilities and activities associated with information technology.

There are wide variations in the range of things to which people take offense. What may be offensive to one person may seem innocuous or even informative to another. Generally, a person's access to a particular piece of information will not be proscribed simply because someone else finds it offensive. On the other hand, no one should be involuntarily presented with information which the person transmitting it should reasonably know would be viewed by the recipient as offensive or insulting.

Thus, when a member of the University community, with properly authorized access to the University network, actively seeks information which is legitimately and publicly available on a computer or network, the University will ordinarily take no action to restrict that individual's access based on the nature of the information being sought.

In situations where a member of our community is presented, through the network, with offensive information without consent having been either sought or granted, Computing and Networking Services will investigate the incident and take appropriate action. Such action may include, for example, referring any information about the incident to the faculty, office or college, or assisting the complainant in bringing action under the appropriate University code of behaviour. Relevant policies include Code of Student Conduct and the Sexual Harassment policy, among others.

Complaints about potentially illegal information being produced locally will be investigated, and the University may initiate criminal charges directly and/or actions under the relevant University codes of behaviour."

Personal Privacy

The property of the University includes the facilities related to computing accounts and files and other aspects of the information technology network in a similar manner to the telephones, filing cabinets, desks, etc., which an employee uses in carrying out the duties of her or his job. In principle, they are subject to inspection at any time. In practice, however, such inspections other than for verification of physical assets are unusual and take place only where there is reason to suspect an infraction of the rules.

Generally, with respect to computing accounts established for students, faculty and staff there is a presumption of privacy. Under certain circumstances, access to files is authorized by University policy, or, for example, certain student files may be accessed by instructors as part of course requirements. However, if an infraction is suspected, the appropriate officials at the University of Toronto will investigate the matter and, if circumstances warrant, proceed to investigate the traffic and files associated with the suspected infraction in accordance with the applicable University policy or procedure.

Such action requires the authorization of the respective chair or department head and/or dean or principal or vice-president. The Director, Computing and Networking Services should be advised promptly of any such action and that office is available to provide technical advice and guidance regarding suspected occurrences of inappropriate use. Local units are encouraged to establish, through a standing order from the appropriate academic or administrative head, the range of actions available to the designated individuals with responsibility for oversight of local information technology facilities.

It is essential that all users of information technology facilities and services recognize that it is possible for unauthorized individuals to monitor transmissions on networks in certain circumstances. It is also possible, for example, to create and send counterfeit mail under the name of another person and in a manner which makes it appear the message has emanated from the named user's desktop. It is suggested, therefore, that confidential information not be sent electronically unless the user is operating on a know secure network or is using encryption mechanisms.

Procedure in the Event of a Suspected Violation of University Policy, Provincial or Federal Law

The nature, severity and possible consequences arising foam infractions of the use of University information technology resources cover a wide spectrum. These can range from mere inconvenience or loss of privileges to damage of the University's reputation or even to charges being laid if federal or provincial laws have been violated. The speed, nature and escalation of notification procedures should be commensurate with the severity of the infraction.

For infractions that contravene established University policy or facility rules, the relevant local administrator should proceed in accordance with the applicable codes or rules and should inform the department head or chair of the event and the action taken.

Violations that have broader consequences such as unauthorized access to and/or modification of institutional data here or elsewhere, or the commission of illegal acts require additional consideration. The process should include notification of the dean or division head as well as the department head or chair. A the same time, Security Administration in the Networking and Computing Services department should be informed by telephone, electronic mail, or facsimile (see numbers below). In the absence of a response conforming receipt of the notification within an hour, the Vice-Provost should be informed directly.

Should the circumstances warrant it, the dean or division head, in collaboration with the Vice Provost, should inform the provost or president and/or a joint decision may be taken to inform the appropriate legal body or law enforcement agency.

Contact numbers for Computer Security Administration, Computing and Networking Services (UTCNS)

E-Mail: **security.admin@utoronto.ca**

If you wish to report a security breach, call the ***Computer Security Hotline*** at the following number:

Computer Security Hotline ☎ 416-978-1354

Facsimile: 📠 416-971-2085

↩ Back to Computer Security Administration Page.

Computer Security Administration - University of Toronto
Last updated: September 26, 1995

University Policies, Procedures & Regulations Database

Senate Policy

Policy on Computing and Information Technology Facilities

# : Sen 001

Description:

Notes: Approved by Senate and Delegated to SCAC: 1994/12/08; Approved by SCAC: 1995/02/16; Policy Statement and Guidelines Approved by UEC: 1995/02/06; Policy Statement and Guidelines Approved by BPC: 1995/02/07; SCAC's Report to Senate on Policy, Guidelines & Procedures: 1995/04/27; Procedures for Students Implemented Under the Authority of AVP (Technological Services & Registrar) Date Effective: 1995/04/27

Approval Authority: President and Senate

Signature: "Malcolm Ransom"

Policy Statement

1. York University's computing and information technology facilities are made available to students in support of their academic objectives and requirements; to faculty in support of their teaching, research and administrative activities; to staff in support of their assigned responsibilities; and to other authorized users. Such facilities may include computers and associated peripherals, the communication infrastructure and related equipment, facsimile machines, scanners, copiers, telephone, video and other multimedia devices and forms of software.

2. Computing and information technology facilities may be used only in a manner which does not contravene York University's relevant policies, codes, agreements, and network protocols, and provincial and federal laws.

3. Access to computing and information technology facilities is a privilege. Users who contravene the relevant policies and laws may be subject to immediate withdrawal of the privilege and/or disciplinary procedures. Illegal acts involving computing and information technology facilities may also be subject to criminal prosecution or other legal action.

Guidelines for Users of Computing and Information Technology Facilities

Users shall

1. Be responsible for using these facilities in an effective, ethical and lawful manner.
2. Respect the rights and interests of others.
3. Respect the property of others, including intellectual property.
4. Respect the copyrights of the owners of all software and data they use.
5. Respect the licensing agreements entered into by the University.
6. Respect privacy and confidentiality.
7. Use only those facilities for which they have authorization, whether these facilities are at York University or at any other location.
8. Use facilities and services only for their intended purposes.
9. Take all reasonable steps to protect the integrity and security of the facilities including software and data.

10. Properly identify themselves in any electronic correspondence and provide valid, traceable identification if required by applications or servers within the University's facilities or in establishing connections with the facilities.

Users shall not

1. Access systems or data without authorization.
2. Alter systems, software and/or data without authorization.
3. Copy software and/or data without authorization.
4. Destroy or remove software and/or data without authorization.
5. Disclose data without authorization.
6. Interfere with the processing of a system, such as deliberately overextending the resources of a system.
7. Misrepresent themselves as another user.
8. Disclose confidential passwords, access codes, account numbers or other authorization assigned to them.
9. Change another person's password without authorization.
10. Use the University facilities and resources for unauthorized purposes, including unauthorized commercial purposes.

Procedures for Allegations of Student Misconduct in the Use of York's Computing and Information Technology Facilities

1. Each computer lab/network/service available for student use shall identify to the Senate Committee on Academic Computing an appropriate individual associated with the lab/network/service who agrees to serve as a local Computer-Complaints Officer in regard to offences related to the use of computer systems.
2. Each computer lab/network/service available for student use shall identify to the Senate Committee on Academic Computing an appropriate faculty member associated with the lab/network/service who agrees to serve as a local Computer-Hearing Officer in regard to offences related to the use of computer systems.
3. Each computer lab/system/service available for student use shall adopt the Senate Committee on Academic Computing's (SCAC's) Guidelines.
4. The Guidelines shall be posted on each door into the labs and/or broadcast at the point of access to the system. By entering the lab and/or signing onto the system, the user agrees to abide by these Guidelines.
5. Students violating the Guidelines may lose the privilege of computer access in a hearing before the local Computer-Hearing Officer. This procedure shall normally be initiated by or through the Computer-Complaints Officer.
6. The Computer-Complaints Officer shall preserve any evidence, including electronic evidence of abuse, for the consideration of the local Computer-Hearing Officer.
7. The local Computer-Hearing Officer shall hear the case as expeditiously as possible and may impose a term of suspension and/or set conditions of access to the local lab/network/service. The local Computer-Hearing Officer may also recommend to the Associate VP (Technological Services & Registrar) that access to all of York's computer labs/networks/services be suspended. The Associate VP (Technological Services & Registrar) may impose a university-wide restriction on the privilege of computer-access.
8. The Computer-Complaints Officer may, on the basis of prima facie evidence of serious abuse and/or the potential for serious harm, immediately impose a temporary suspension of a student's local computer access pending a hearing. This temporary suspension shall be reviewed by the Associate VP (Technological Services & Registrar) or Chair of SCAC or designates, normally within 1 working day. The Associate VP (Technological Services & Registrar) or Chair of SCAC or designates may reverse the suspension, uphold the suspension, or make the suspension university-wide pending a hearing.
9. The penalty of suspension of computer-access is in addition to penalties which may apply under other codes and laws such as The Senate Policy on Misconduct in Academic Research, The Senate Policy on Academic Honesty, the civil law of Ontario, *The Copyright Act* and *The Criminal Code*

of Canada.

10. In cases where computer access is essential to the course work of a student who has had computer access suspended, the student may appeal the penalty only, and not the finding of abuse, to SCAC. The Committee will assess the consequences of the penalty and may choose to grant reinstatement of the student's privileges or conditional/limited reinstatement for the completion of the course work in question. SCAC may recommend to the relevant Faculty's Petition Committee late withdrawal without academic penalty from the course/s in question. SCAC may also deny the appeal.

SPEC

SYSTEMS AND PROCEDURES EXCHANGE CENTER

SELECTED READINGS

ASSOCIATION OF RESEARCH LIBRARIES OFFICE OF MANAGEMENT SERVICES

CAUSE Information Resource Library. CAUSE/EFFECT homepage, <http://cause-www.colorado.edu/>.

"Communications of the ACM," December 1995, vol. 38, no. 12.

Denning, Dorothy E., Ed., et al. *Rights and Responsibilities of Participants in Networked Communities.* National Academy of Sciences - National Research Council, Washington, DC. Computer Sciences and Telecommunications Board. 1994, 172 p.

Graves, William H., Carol G. Jenkins, and Anne S. Parker. "Development of an Electronic Information Policy Framework." CAUSE/EFFECT, vol. 18: 2, Summer 1995, pp. 15-23.

Shade, Leslie Regan. "Wired in the Ivory Tower: Access and Copyright Issues Surrounding the Internet and Higher Education in North America." *Education* vol. 13, no. 3, Sep 1995, pp. 211-28.

Skolick, Barbara, Angela Y.Dumas, and Marjorie W. Hodges. "Crafting and Implementing Responsible Use Policy: Retrospect and Futures." Presentation at annual Educom conference, 1995, Portland, Oregon.

Stager, Susan. "Individual Rights vs. Institutional Responsibilities." *Educom Review,* May/June 1993.

Stager, Susan, Virginia Rezmierski, and Tad Pinkerton. "The 1990's Challenge of Insulating the Institution with 1980's Information Technology Policies." 1995 CAUSE annual conference, pp. 2-5-1 to 2-5-13.