Horses and Barn Doors: Evolution of Corporate Guidelines for Internet Usage

Sally Hambridge & Jeffrey C. Sedayao – Intel Corp.

ABSTRACT

Intel's Internet usage policy evolved from practically non-existant to explicitly defined – all in reaction to changing conditions and security threats. This paper covers the evolution of Intel Internet access policy, a continual struggle to close the barn doors before the horses get out. Throughout the paper, we outline key lessons we have learned during the policy-making process. It discusses Intel's first taste of the Internet, Intel's policy-making process, the open access policy of that period, and the resulting security challenges. It then covers the imposition of a stricter policy and implementing a firewall to enforce that policy. The paper proceeds to describe today's problems, the majority of which center around Intel people accessing the Internet. In response to this problem and growing numbers of people wanting to use the Internet, Intel has drawn up explicit corporate guidelines on Internet use. These guidelines are then compared to various Acceptable Use Policies and Netiquette guides. The paper concludes with some additional tasks Intel is planning in order to keep the barn doors closed.

Intel's Introduction to the Internet

Intel Corporation has had access to the Internet since 1987. At that time, we had a dial-up connection to the now defunct CSNET. We dialed Boston from Santa Clara, California several times a day to pick up and drop off mail. We did not have any kind of Internet access policy. We felt secure in having complete copies of all messages sent in and out and having our modems block dial-ins.

While the dial-up connection provided much-needed mail access to and from customers, vendors, and research partners, functionality was too limited. Delivery was so slow at times (days!) that paper proved a quicker and more reliable communication medium. Users complained that carrier pigeons would deliver mail faster. The long distance calls grew to be expensive. Because of these concerns and the desire for direct FTP and telnet access to the Internet, in 1989 we traded our CSNET dial-up connection for one with direct IP access over a leased line. An increase in functionality always means an increase in risk, as we will see in the next section.

The Challenges of an Open Door

Our first policy was this: anyone in the company could go out on the Internet, and rlogin, telnet and FTP access into Intel would be blocked. WE were the access providers, and so we imposed this policy unilaterally. The only place this was written down was in the router access list configuration.

What were the results of our (wide) open door? We received many complaints about Internet access from various system administrators around the company. They did not like the gaping door. Later, with unsolicited help from federal agents, we found some crackers who did.

- Key Lesson #1 – Research Policy Issues
- Key Lesson #2 – Consult with users and stakeholders on policy decisions
- Key Lesson #3 – Make the policy available and readable.

Our policy was incredibly naive. We did not think it through in depth and did not realize how easy it would be for intruders to exploit gaping holes. Furthermore, we did not have buy-in to our policy. System administrators weren't comfortable with it. Even worse, they were uncomfortable with a policy they couldn't even read. Things had to change.

Shutting the Door Part Way

The problems we encountered forced us to realize our mistakes. We looked into Internet access schemes implemented at other companies. We wrote down and proposed a limited access policy. This document was circulated for comment by electronic mail and presented at various user forums within Intel. Finally, we had the policy approved by an internal change control group. This was an official stamp that gave us legitimacy.

Our new policy restricted outbound Internet access to specific systems. Inbound access was limited to certain protocols going to dedicated servers. The outbound systems, controlled by site administrators, would be tightly controlled. Applications for Internet access systems would have to be signed by site network managers, the system administrator's manager, and our internal Information Security group. Applicants promised to read and obey our policy, which was circulated with the application forms.

- Key Lesson #4 – Get key people to buy into a policy. Better yet, get some kind of official stamp of approval.
- Key Lesson #5 – Forms with signature loops are a way of making sure that people are serious about wanting something. It is also a way to inform key parties of change and get their buy-in.

We managed to get people involved in making our policy. They bought into it, and we got an official stamp of approval from a internal group. By using forms, we weeded out people who weren't serious about managing Internet access systems. Moreover, we gave our Information Security group a chance to review and buy into the decision of who would want access.

- Key Lesson #6 – Provide metrics on usage and quality of service.

We made the decision that we would track how much the gateway was used and who was using it. We look at sheer volume, such as how many bytes each access system exchanges with the Internet and how many messages are exchanged through the gateway mail servers. We also decided to track some service metrics like mail delay through the gateway. An Internet gateway status and usage report is produced and widely distributed every quarter.

Keeping metrics has proven to be a good decision. We can track utilization, which helps us with capacity planning and with justifying new equipment. Management, initially unsure about funding our gateway, is usually persuaded when they see how much their people are using the Internet. Finally, keeping metrics gives us some idea how well we are managing the gateway.

Ironically, by shutting the door part way, usage boomed. Throughout the six years we have had mail capability, we have witnessed an exponential growth in the amount of mail coming into and going out of the company. This growth is consistent with Internet growth trends industry wide. (See Figures 1 and 2.)[1] Since Intel is a multi-site, multinational operation, almost all Intel sites dedicated a number of machines to provide ftp and telnet capability for groups within the site.

With growth in the number of Internet knowledgeable employees, (as well as those who have heard of the Internet but know little) we've seen demands for accounts on these machines skyrocket. We've also seen a corresponding growth in different kind of security problems – from Intel instead of to Intel. Most of these problems stem from people attempting logins to defunct accounts, or naively trying to telnet to ftp machines and vice versa. Still, even these innocent mistakes mean time and trouble. This is time and trouble for the system manager of the machine where the ''break-in'' is attempted as well as Intel's Internet contact and the system administrator of the internal Intel machine from which the ''attempt'' occurred. Intel personnel must then check system logs to determine who was logged in at the time, then contact those people to find out whether intent was indeed malicious. All of this takes time from resources which function better as network and system managers than High School Vice Principals.

We discovered that almost all of our policy focused on system and network administrators and not on users. Although we put conditions on how the access systems should be administered, we did not provide any tools or help to do so. We should not have been surprised that some of the Internet access systems were far more open than we liked. The incidents with misguided users sparked another fear. We could conceive scenarios [2] where a user could create an incident severe enough to cause Intel to shut down or tremendously restrict our Internet connection.

Getting the Horses to Behave

To combat these problems, an Internet Security Task Force was formed. This ad hoc group consists of representatives from Corporate Information Security and system managers and users. We had learned from past experience that only by getting people involved could we create workable policies.

Corporate Information Security bears the responsibility of protecting Intel's intellectual property assets. This group sets policy and procedures for Information Security, publishes a yearly summary of those policies, and has recently developed a class on information security for Intel employees.

In its Internet Policies, the Task Force has tried to maintain a balance between getting people to information (and information to people) and maintaining reasonable security. First, although most of us eschew bureaucracy, we ask those users requesting accounts on machines which have Internet telnet and ftp access to justify having an account. We have found that many people think they need direct access to the Internet in order to send Internet mail. Since sending Internet mail is possible from any networked machine at Intel, we inform the user how to send mail and this eliminates the need for the account. We do ask that the user have a legitimate business reason for telnet and ftp access before we grant the account.

Second, accounts on Internet accessible machines are set to expire at 6 months. If a user doesn't use the account enough to notice it has expired, it will not be an open door. This is a minor inconvenience to users who need their accounts (especially compared to the benefits).

- Key Lesson #7 – User education is critical
- Key Lesson #8 – Create explicit and enforceable policies

Third, Intel has created a set of Internet Etiquette Guidelines for Internet users (contained in appendix A). The Task Force felt it needed a distinct set of guidelines for a number of reasons: First, policies need to be explicit. Tradition and word-of-mouth fail to carry any legal consequence. Second, existing Acceptable Use Policies[3,4] are too generic. Although most of these provide good general guidelines, they do not deal with circumstances specific to Intel or even specific to a business environment. Third, we've found that Netiquette Guides[5] are good for beginning users, but may not necessarily address behavior problems of the more knowledgeable.

Increasingly, we have found that Intel employees fall into 3 camps: those that know everything about the Internet; those that know about the Internet but feel it's ''just like the computer bulletin boards I've used from home''; and those that have heard of it, know that ''good stuff is out there,'' but have no idea how to proceed. Although these groups have very different levels of understanding all indulge in behaviors which need governance.

The experienced user may have had access to the Internet in previous jobs or in college. That previous experience may have been in an environment less demanding than Intel's, since the Corporation emphasizes a stringent work ethic and places heavy demands on employee time. Those employees familiar with bulletin boards may have no clue as to the global community in which they now find themselves, and those new to the 'Net just have no clue. Each needs help understanding the environment.

Experienced users should be informed that Internet use should indeed be work related. Wanting to get to Usenet Newgroups to keep up with discussions on rec.whatever is not an acceptable reason for 'Net access, although needing to stay current with comp.sys.intel certainly is. Experienced users should also understand that their role and responsibility has changed. As students at Wherever.edu no one cared what they said in postings, but people form opinions of a company based on its employee's communications. Disclaimers don't seem to matter, no matter how sincerely stated. Strongly offended readers focus on ''intel.com'' in mail and article headers.

Half-way knowledgable users need to be educated to the ways of the Internet. These users may be familiar with other forums of computer communication, most likely PC-type bulletin boards, or Prodigy/Compuserve models. These users need to know that their postings span countries and continents, rather than a local community or even the US. They need to learn the jargon and the context of discussion groups. They should ''lurk'' for a while before jumping into discussions.

Inexperienced users need all the help available. They need to know what kinds of services are available, what the community is, and how to interact with it. With these communities in mind, the guidelines Intel provides fall roughly into those covering technical/security issues, those covering etiquette, and those to help new users. They are broken into categories for electronic mail, mailing lists and newsgroups, ftp, and telnet.

The electronic mail section covers such new user concerns as `SENDING MESSAGES IN CAPITALS`, use of the smiley face :-), and watching punctuation and spelling while not criticizing others' mistakes. Etiquette, such as letting a sender know a message was received (especially when one cannot respond immediately) and having a signature file, is also defined. Issues such as taking care when sending replies, sending plain ascii text (as many Intel users often send PC file attachments in cc:Mail), and being aware of system etiquette on their native system comprise the technical issues addressed. Finally we remind users that electronic mail is unencrypted and easily readable.

The section of the guidelines on Internet mailing lists and Usenet News groups references the section on electronic mail. This is by far the longest section of the guidelines since all employees can send and receive Internet mail. They are also most likely to make mistakes in this area, although in general these mistakes will be less catastrophic than in telnet or ftp. Here, we inform users to disclaim speaking for Intel, and that even if they do, they will represent the company de facto through having ''Intel'' in the mail header. Along with that technical warning, we direct users to watch verbosity since many Internet sites pay by the byte, to obey copyright law, and to be careful using auto-reply features in mail. We also tell them to change their addresses with mailing lists when they change accounts. There are many guidelines covering straight etiquette: Monitor any group you join for a while, No advertising of Intel products, Don't re-post without permission, Summarize if you survey, Indicate quoted material, No anonymous postings, and No postings about that dying child in England (he got better)! New users are cautioned to make sure the subject of messages is clear in the Subject: line, to think about how much time mailing lists or news groups will absorb, to read the FAQs, to be careful of flaming, and not to go overboard if they're flamed.

The section on ftp leans heavily toward technical issues. The only point of etiquette is that users should type in real Internet addresses for passwords when accessing anonymous ftp sites. The other issues covered: do not deliberately ftp to machines without ftp access, random net-hunting is not approved; observe working or posted hours for ftp sites and observe any restrictions posted at those sites; look locally for ftp materials (where items are posted more than once); and finally don't ftp on the ''off chance you'll need the information someday.''

The telnet section is even more succinct, covering posted restrictions, using only authorized ports, not not deliberately telnetting into machines with no guest account.

There is a final section, listing a bibliography of Internet resources for beginners. It lists Kehoe[6], Krol[7] , LaQuey[8], and Tennant, et al.[9]. Hopefully, the beginning users armed with the Guidelines, and one of these publications, can survive on the 'Net.

There is another section of the Guidelines listing behavior which is subject to disciplinary action. Here is where our Guidelines differ most dramatically from generic Netiquette guides, since these are areas where we do more than recommend behavior. The guidelines promise action for sending chain letters, for using Intel equipment for personal gain, for sending sexually or racially harassing messages, for unauthorized attempts to break into any system (since Corporate Information Security occasionally gets authorization to attempt break-ins), theft, or copying electronic files without permission, sending Intel confidential materials outside of Intel, and refusing to cooperate with a reasonable security investigation. These guidelines were specifically derived from the Corporate Information Security guideline on mail and from the Human Resources general guidelines. Since this is policy and not procedure, it does not include specific disciplinary actions which might be taken but leaves that for Human Resources to sort out at the time of the incident.

The guidelines were drafted by one person and submitted to an internal mailing list which included the Internet Security Task Force and system managers of machines which have Internet access. This draft gathered comments from ''It's fine the way it is'' to ''Change everything about it''. Comments were incorporated into a second draft, which was again circulated to the group. Comments on this draft were minor, although Corporate Information Security made a few specific requests, most having to do with making implicit statements more explicit. (**Mail on the Internet is Not Secure** being the major one.) The final version was sent to the internal mailing list of system managers for distribution to their users. It was also made available for anonymous ftp within the company.

Finally, the policy was adopted as a formal Intel Policy. We did have to get it approved by Intel's legal staff. Now we'd had our policies ratified.

Keeping the Barn Doors Closed

- Key Lesson #9 – Policy transitions can be hard, especially when you have to take something away.

Although we have drawn up new ''official'' policies, we find that it can be hard to get people to transition to them. It is especially difficult when people lose privileges they once had. For example, we would like to reduce the number of Internet access machines at each site. Getting groups to give up their access is not easy, especially if they have had their own access system for several years. We have found the best time to get people to implement policy changes is after an incident has occurred. While this truly is closing the barn doors after the horses are out, it definitely prevents any more horses from leaving. After implementing the policy on some of the major access nodes, we have had a drop in reported incidents from them.

We need to improve our user education. Although we have created guidelines and even an Intel Internet user guide, it is obvious to us (as indicated by gross violations of Netiquette) that this information has not propagated widely. Getting users to read and understand the policies is a major challenge. One bright spot is a class that Intel has created on Information Security for its employees. Information Security is planning to include the policy in the next edition of its booklet distributed to all employees.

Unfortunately, closing the door to the Internet means keeping some of those resources unavailable to Intel employees. Intel still needs to maintain a competitive edge. In order to allow additional access to Internet resource, we are considering and implementing alternatives. We have implemented an internal ftp machine, which holds internal information for the company, provides mailing list capability, and caches and mirrors external archives. This capability allows us to fill many information needs without having to grant full internet access to the entire company (it also helps us to conserve the bandwidth of our Internet connection). Employees who have one-time needs can send mail to an ftp-admin account with their request and the ftp administrator will search the Internet and mail the results to the employee.

- Key Lesson #10 – Policies exist to serve. They should be changed when circumstances warrant.

Many employees still find our policies limiting. Having someone else search for you is never as satisfying as searching for something yourself. Users have been clamoring to run Gopher, WAIS, World Wide Web clients from their own PCs. We are looking at alternatives like proxy agents for these services. We are also evaluating easing some of our policies for WAIS and Gopher access. The Internet is a constantly changing environment, with new services springing up all the time. We will need to make changes to our policies, but when we do so, we will not ignore the many lessons we learned.

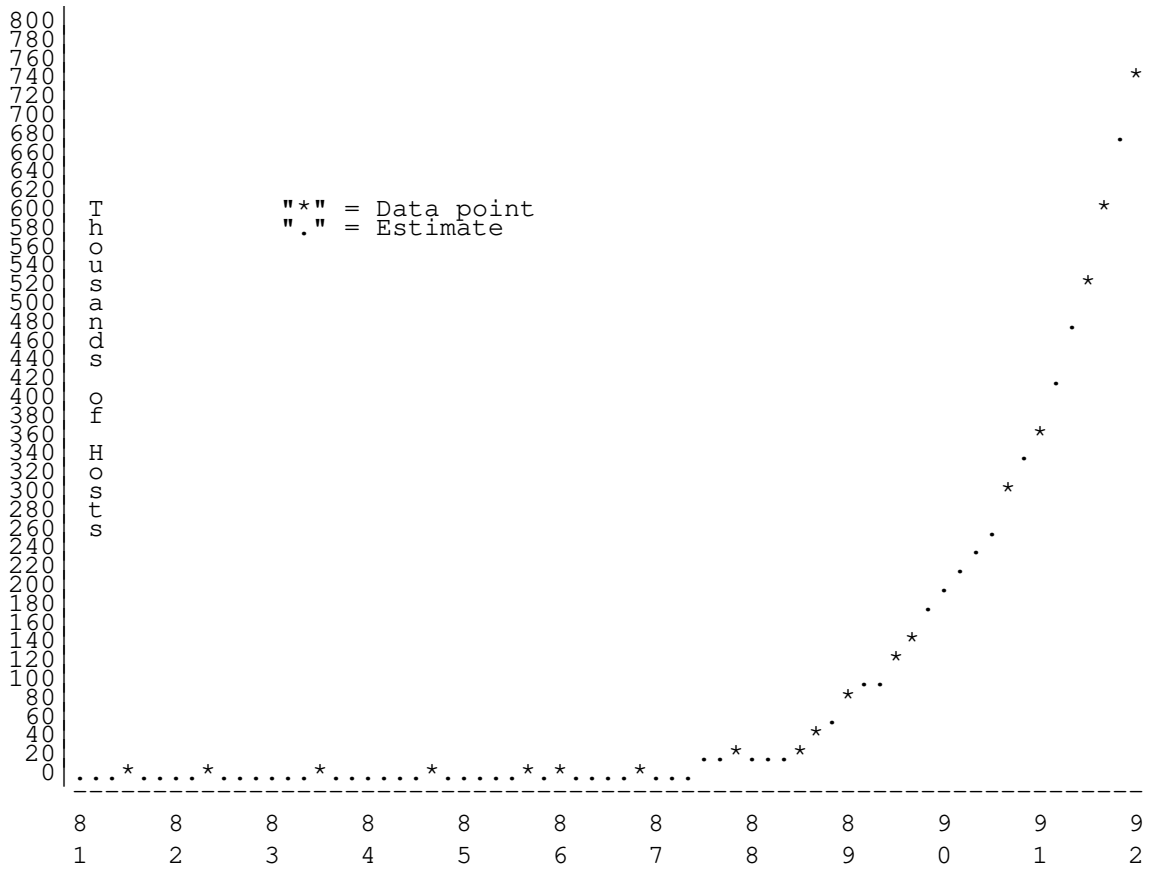

Figure 1: RFC 1296, Internet Growth (1981-1991)

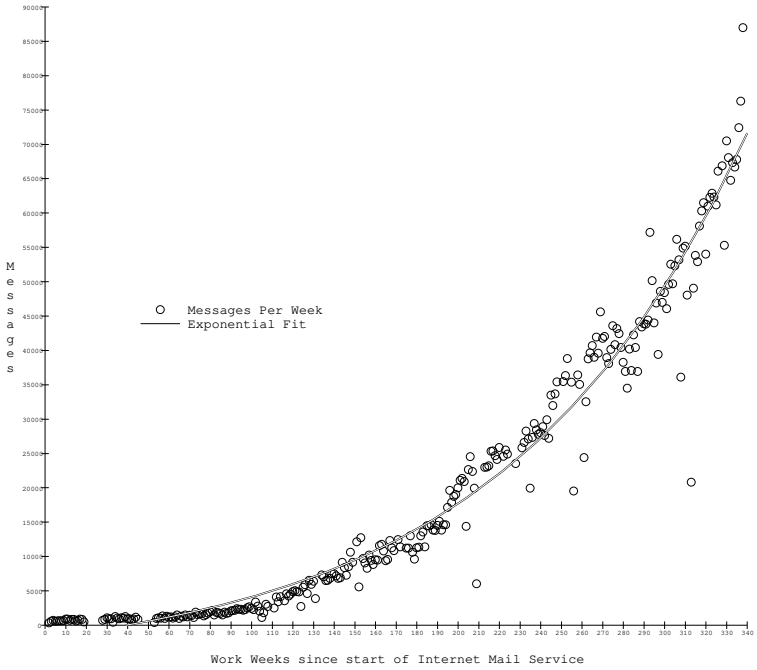

Figure 2: Internet mail by week since 1987

Author Information

Sally Hambridge received her BA in English from UCLA in 1970 and her MLS also from UCLA in 1979. She worked as a contract employee for Xerox. Joining USC/ISI in 1980, she got her first taste of the Internet. She moved to Atari in 1982, then joined Intel in 1984. There, she has been librarian, database analyst, currently runs an internal ftp server. Reach her via U.S. Mail at Intel Corp; SC3-15; 2880 Northwestern Parkway; Santa Clara, CA 95052-8119. Reach her electronically at sallyh@ludwig.intel.com.

Jeff Sedayao received a B.S.E in Computer Science from Princeton University in 1986 and a M.S. in Computer Science from the University of California at Berkeley in 1989. He has worked at Intel Corporation since 1986, spending most of his time running Intel's main Internet gateway. Reach him at Intel Corp; SC9-37; 2250 Mission College Boulevard; Santa Clara, CA 95052-8119. Reach him electronically at sedayao@argus.intel.com.

References

[1] Lotor, Mark. ''Internet Growth (1981-1991); RFC 1296,'' January 1992. Available via anonymous ftp at ftp.nisc.sri.com rfc/rfc1296.txt.

[2] Holbrook, J. P.; Reynolds, J. K. ''Site Security Handbook; RFC 1244,'' July 1991. Available via anonymous ftp at ftp.nisc.sri.com rfc/rfc1244.txt.

[3] ''Acceptable Use Policy for NSFNET Backbone''. February 1992. Available via anonymous ftp at is.internic.net as infosource/nsf-nren-nii-info/nsfnet/acceptable-use-policy.

[4] ''Corporation for Research and Educational Networking (CREN) Acceptable Use Policy''. January 1993. Available via anonymous ftp at cren.net pub/cren-doc/cren.net_use.

[5] Von Rospach, Chuq, Gene Spafford. ''A Primer on How to Work with the Usenet Community''. January, 1991. Available via anonymous ftp at ftp.eff.org pub/internet-info/usenet.etiquette.

[6] Kehoe, Brendan P. *Zen and the Art of the Internet: A Beginner's Guide*. Englewood Cliffs, NJ: Prentice Hall, 1993.

[7] Krol, Ed. *The Whole Internet: User's Guide and Catalog*. Sebastopol, CA: O'Reilly & Associates, 1992.

[8] LaQuey, Tracy. *The Internet Companion: A Beginner's Guide to Global Networking*. Reading, MA: Addison-Wesley, 1993.

[9] Tennant, Ron, John Ober & Anne G. Lipow. *Crossing the Internet Threshold: An Instructional Handbook.* Berkeley, CA: Library Solutions Press: 1993.

Appendix A: The Intel Guidelines

EFFECTIVE DATE OF CURRENT REVISION: 6/93
LATEST REVIEW APPROVE DATE:
NEXT DATE TO BE REVIEWED:
SOURCE FUNCTION: Internet Security Task Force
COORDINATOR: Internet Education
RESPONSIBLE REVIEW MANAGER: Intel Security

1.0 PURPOSE/SCOPE

These guidelines set the standards for appropriate behavior of an Intel employee when accessing the Internet. These guidelines apply to all Intel employees. Intel specifically reserves the right to modify, change or discontinue any portion of the Internet guidelines from time to time at its sole discretion.

2.0 DEFINITIONS

- Cracking – attempting to break into another system on which you have no account, and is treated as malicious intent.
- Netiquette – a word made from combining ''Network Etiquette.'' The practice of good manners in a network environment.
- MIME – Multipurpose Internet Mail Extension. The format for Internet mail which includes objects other than just text.

3.0 GENERAL

4.0 GUIDELINES

4.1 Behavior resulting in disciplinary action.

The following behaviors are examples of actions or activities which can result in disciplinary action. Because all possible actions cannot be contemplated, the list is necessarily incomplete. Thus, disciplinary action may occur after other actions when the circumstances warrant it. Disciplinary actions range from verbal warnings to termination; the severity of the mis-behavior governs the severity of the disciplinary action.

- Unauthorized attempts to break into any computer whether of Intel or another organization. (Cracking).
- Using Intel time and resources for personal gain.
- Sending threatening messages.
- Sending racially and/or sexually harrassing messages.
- Theft, or copying electronic files without permission.
- Sending or posting Intel confidential materials outside of Intel, or posting Intel confidential materials inside Intel to non-authorized personnel.
- Refusing to cooperate with a reasonable security investigation.
- Sending chain letters through electronic mail.

4.2 Behavior considered prudent, good manners, etiquette.

The following behaviors are recommended for sending Internet mail, participating in Internet mailing lists and Usenet groups, ftp, and telnet. Lack of conformance may result in loss of Internet access. These guidelines have been gleaned from a variety of Internet Guides. A bibliography follows these guidelines, and we recommend you acquire one (or more) of these guides.

4.2.1 Electronic Mail (Email)

The following guidelines cover the sending of electronic mail outside of Intel.

- MAIL ON THE INTERNET IS NOT SECURE. Never include in a Email message anything which you want to keep private and confidential. Email is sent unencrypted, and is easily readable.
- Be cognizant of any system etiquette. The computer on which you reside may have quotas on disk space usage. Mail takes up space. It's best not to save every message you receive.
- Do not attempt to send anything but plain ascii text as mail. Recipients may not have the ability to translate Word or WP documents. MIME format messages are encouraged. (MIME=Multipurpose Internet Mail Extension).
- Be careful when sending replies – make sure you're sending to a group when you want to send to a group, and to an individual when you want to send to an individual. It's best to address directly rather than use the reply command.
- Include a signature which contains methods by which others can contact you. (Usually your Email address.)
- Let senders know you've received their mail, even if you can't respond in depth immediately. They'll need to know their mail hasn't gotten lost.
- Watch punctuation and spelling.
- Remember that the recipient is a human being. Since they can't see you, they can't tell when you're joking. Be sure to include visual clues. Convention indicates the use of the smiley face. :-) (Look sideways).
- DO NOT SEND MESSAGES ALL IN CAPITALS. It looks as if you're shouting. Use capitals for emphasis or use some other symbol for emphasis. That IS what I meant. That *is* what I meant.

4.2.2 Internet mailing lists and Usenet News Groups.

All the guidelines covering Email should apply here as well.

- Actively disclaim speaking for Intel. Note that if you use an Intel system to post an article, Intel's name is carried along with what you post in (at least) the headers. The ''standard'' disclaimers attached to many articles are meaningless if the reader finds the article offensive.
- Remember that some people have to pay for each byte of data they receive. Keep messages to the point without being so terse as to be rude.
- Obey copyright laws.
- Be sure to change your mailing address if your account changes. Do not simply forward your mail from your old account to your new one. This creates a burden on Intel machines.
- Be careful using auto-reply features in mail when you belong to mailing lists. These replies are often sent to the entire list, and most don't care that you're on vacation.
- As a new member of a group, monitor the messages for a while to understand the history and personality of the group. Jumping right into the discussion may make you look foolish if you have no context.
- Do not advertise Intel products. This violates the Internet Acceptable Use Policy.
- Do not re-post any messages without permission.
- Avoid cross-posting whenever possible. When not, apologize, especially if the groups seem to have a lot of overlap. Of course, apologize for any mistakes in posting.
- Do not post personal messages to a group.
- If you survey the group, post a summary.
- Indicate quoted material.
- Do not post any messages anonymously. This is viewed as bad form by the Usenet community and system managers are asked to track down offenders. This wastes Intel's time and resources.
- Do not re-post any requests for a dying child in England to get postcards to get into the Guiness Book of World Records. The child got well, and the category has been removed from Guiness.
- Make sure the subject of your message is clear in the Subject: line.
- Join lists or monitor newsgroups giving thought to how much time these activities absorb. Also for Usenet, look at the news.announce.newusers group. It contains good information on getting started. There are also local Intel groups which are good for new people.
- Be sure to read the FAQs (Frequently Asked Questions) for your group(s).
- If provoked, do not send angry messages (flames) without waiting overnight. If you still think a flame is warranted, label your message with ''flame on''. If you receive a flame, don't go overboard in reaction.

Remember that not everyone is as polite as you are.

4.2.3 FTP

These guidelines cover file transfer protocol.

- Do not ftp to any machines on which you do not have an account, or which doesn't advertise anonymous ftp services. Random net-hunting is not approved.
- Observe working hours or posted hours for ftp sites. Most sites request you NOT ftp between their local hours of 8-5.
- Don't ftp during your site's prime hours as well.
- Look locally before ftping something from a site geographically remote. Your system manager can help you find the closest site.
- Don't ftp on the off chance you'll ''need it someday.'' Conversly, don't hunt around for ''neat stuff'' to ftp. If you discover that you don't need what you've ftp'ed, delete it. You can always get it again if you discover you do need it.
- Observe any posted restrictions on the ftp server.
- Use your real username and node as your password on anonymous ftp servers.

4.2.4 TELNET

These guidelines cover telnetting to remote systems.

- Do not telnet to machines on which you have no account, or there is no guest account. Do not attempt to telnet deliberately into anonymous ftp servers.
- Observe any posted restrictions on the machine to which you're telnetted.
- Do not try to telnet into miscellaneous ports; use only authorized ports for access.

5.0 Selected Bibliography

LaQuey, Tracy. *The Internet Companion.* Reading, MA: Addison-Wesley, 1993.

Kehoe, Brendan. *Zen and the Art of the Internet*. Englewood Cliffs, NJ: Prentice-Hall, 1992.

Krol, Ed. *The Whole Internet: User's Guide and Catalog*. Sebastopol, CA: O'Reilly & Associates, 1992.

Tennant, Ron, John Ober & Anne G. Lipow. *Crossing the Internet Threshold: An Instrustional Handbook.* Berkeley, CA: Library Solutions Press, 1993.