

Table of Contents

Chapter 1	Internet Acceptable Use Standards	
	Internet Acceptable Use Guidelines	.1-2
	Behavior Resulting in Disciplinary Action	1-3
	Internet Gateways	1-4
	Internet Accounts	1-4
	Passwords	1-5
	Internet Services	1-5
	Personal Workstation	1-6
	Network Reliability	1-6
	Closing the "Back Doors"	1-6
	Electronic Mail (E-mail)	1-7
	File Transmission	1-8
	Usenet News and Mailing Lists	1-8
	File Transfer Protocol (FTP)	1-10
	Telnet	1-10
	World Wide Web	1-11
	Acceptable Use Policy	1-12
Chapter 2	Acceptable E-Mail Use	
	E-mail Forwarding	.2-2
	Generic Accounts	.2-2
	New User Accounts	.2-3
	Passwords	.2-3
Chapter 3	Forms	
	E-mail Policy Reminder	.3-2
	Dismissal Memo	.3-4

Acceptable Internet Use

1

The recognition of the business related need to access the public Internet within News Corporation business units is well established. With this interconnection comes the potential for significant loss of confidentiality over the Internet. Messages and files can be intercepted, read, or even altered by others connected to the Internet if they had the desire to do so. Furthermore, connection to the Internet means that everything in the business unit local network may become directly or indirectly connected to the Internet, and individuals seeking unauthorized entry to the local or global ATM network can possibly attain access via the Internet unless minimal security measures are in place.

Access to the Internet is a privilege. As such, it is the responsibility of the users to protect both the company and the company's networks through security-aware usage of their Internet access.

All security systems are only as good as their weakest link. The user of Internet services inside the company plays a crucial part in maintaining the security of the company's networks and data. Following a few simple procedures and guidelines when using the Internet through the company's established gateways and firewalls can significantly enhance security.

This standard is designed to address those areas in which Internet users have traditionally created potential security holes, allow for a productive computing environment, and protect against the compromising of our networks and data. These guidelines apply to all company employees connecting to the Internet. The company specifically reserves the right to modify, change or discontinue any portion of the Internet Acceptable Use Policy from time to time at its sole discretion.

This chapter describes the Internet acceptable use policies and covers the following topics:

- Internet Acceptable Use Guidelines
- Acceptable Use Policy

Acceptable Internet Use

Internet Acceptable Use Guidelines

This chapter describes the Internet acceptable use policies and covers the following topics:

- Behavior Resulting in Disciplinary Action
- Internet Gateways
- Internet Accounts
- Passwords
- Internet Services
- Personal Workstation
- Network Reliability
- Closing the "Back Doors"
- Electronic Mail
- File Transmission
- Usenet News and Mailing Lists
- File Transfer Protocol (FTP)
- Telnet
- World Wide Web

Acceptable Internet Use

Behavior Resulting in Disciplinary Action

The following behaviors are examples of actions or activities which will result in disciplinary action. Because all possible actions cannot be enumerated, this list is 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 misbehavior governs the severity of the disciplinary action.

- Unauthorized attempts to break into any computer whether belonging to the company or to any other organization. (Cracking).
- Using company time and resources for personal gain.
- Using company time for downloading or playing games, downloading non-business related graphics, "surfing" the Internet, or reading non-business related news groups.
- Sending threatening messages via e-mail or Usenet.
- Sending racially and/or sexually harassing messages.
- Theft or copying of electronic files without permission.
- Sending or posting company confidential information to an outside organization.
- Sending confidential company information to an authorized third party if the information is not adequately protected by encryption.
- Refusing to cooperate with a security investigation.
- Sending chain letters through e-mail, or posting a chain letter to any Usenet news group (e.g. MAKE.MONEY.FAST)

Acceptable Internet Use

Internet Gateways

- All computer resources containing sensitive or confidential firm information or connected to an internal network must connect via the security gateway when accessing services on the Internet.
- All new gateways and firewalls must be approved by the security group.
- All managers of Internet gateways must comply with the applicable security standards.

Internet Accounts

- All Internet accessing accounts must be approved and acquired through the appropriate Gateway Administrator.
- To acquire an account, proper business use justification must be presented, as well as all the Internet services required to fully meet those business needs. The Gateway Administrator reserves the right to deny the provision of a requested service should they not be capable of reasonably securing it through their current firewall.
- Accounts are for the express use of the registered user, they should not be shared or made accessible to others. This includes leaving a terminal while an Internet session is still active.

Acceptable Internet Use

Passwords

- All passwords are to be kept strictly confidential. They should not be written down and left in easily accessible places.
- Login ID's and Passwords should not be sent via e-mail for any reason other than for administrative purposes, and then only in encrypted form.
- Login ID's and Passwords should NEVER be given out over the phone for any reason. System crackers have been known to obtain passwords by calling users and impersonating technical support staff or other employees.
- Passwords should be changed at least as often as specified by the Gateway Administrator.
- One time authentication tokens and password lists should not be left where they are easily accessible or stolen.

Note: *Passwords should consist of eight or more characters, including numeric and non alpha-numeric characters. They should not be dictionary words or names easily associated with you. They should use a combination of upper and lower case letters. (Example: &nOWay4U! would be a good password)*

Internet Services

- Use of Internet Services should be approved and configured by the Gateway Administrator.
- Under no circumstance should a user try to obtain or configure a service which has not been approved by the Administrator.

Acceptable Internet Use

Personal Workstation

- Consider your workstation to be "at risk" when connecting to Internet Services.
- Client software (Explorer, Netscape, etc.) has been exploited to provide unauthorized access to the local workstation (i.e. World Wide Web clients can provide holes for system crackers to exploit to gain access to your workstation or even to the local internal network).
- To protect your personal workstation, implement the following:
 - A regular backup schedule of the workstation (i.e. once a week, once a month, etc.)
 - Encrypt any sensitive files that are stored on your personal workstation.

Network Reliability

- Users should immediately report any suspicious activities or occurrences in their accounts or on the network to the Gateway Administrator.
- Users should refrain from activities which interfere with other network users. Large file transfers and system impacting processes should be reserved for times when the system's usage is low.

Closing the "Back Doors"

- When away from a terminal or workstation for any amount of time, users should logoff or implement a password protected screen saving device to disallow access to any passers by.
- Users should insure that workstations and terminals are turned off at the end of the day, especially those containing modems or other outside communications capabilities.

Acceptable Internet Use

Electronic Mail (E-mail)

E-mail use should follow the guidelines set forth in the External E-Mail Acceptable Use Policy (see attached) with the following additions:

- E-mail accounts are for the express use of the individual to which they are granted; these accounts should not be shared with other individuals.
- Passwords should not be transmitted in e-mail messages, except for administrative purposes, and then only if those messages are encrypted.
- Internal network configurations, addresses, or system names should not be disclosed in e-mail messages.

Note: *All e-mail is vulnerable to eavesdropping on the public Internet. The capturing or reading of e-mail packets is a trivial process which is widely used by individuals seeking unauthorized access to computer systems or proprietary information. Proper awareness and responsible e-mail usage are CRITICAL to the success of any information security plan.*

- All mail, news postings, or other electronic messages originating from a News Corporation account or system represents the company -- regardless of whether that posting is recreational or professional. For this reason, all electronic messages must comply with company policies and standards governing public representation of the company. Despite the use of a disclaimer in your messages, the company's name is still in the address header of your message, and any messages which offend other users will be associated with the company.

Acceptable Internet Use

File Transmission

- NEVER download executables from public sites. For downloads from other sources always try to obtain the source code when possible. Executables have the potential for carrying hidden viruses and Trojan horses which would not be detectable. Source code can be examined to determine its integrity before compiling the executables.
- Software that is downloaded from the Internet should meet all specified software purchasing and licensing requirements.
- All software downloaded should be checked for viruses and Trojan horses before it is allowed to reside on the internal network.
- Software should not be downloaded from sites deemed questionable by the Administrator. The Administrator should advise all users of any sites which might be considered insecure.
- Consider encrypting any files downloaded to/from a private site to protect confidentiality.

Usenet News and Mailing Lists

- Beware that many of the news groups violate copyright laws. Be careful in what you download and also in what you post that you are abiding by copyright laws.
- Keep messages to the point. Some people have to pay for each byte of data they receive.
- Beware of using an auto reply responder. People on a mailing list you are subscribed to don't care if you are on vacation.
- Be sure to change your mailing address if your account changes. Do not simply forward your mail from one account to another. This creates a burden on the network.
- Look before you Leap. Monitor a news group and read its FAQ if it has one before you jump into the conversation.
- Do not advertise company services or products. This violates the Acceptable Use Policies of many of the intermediate networks and is also considered to be just plain rude. It is acceptable to reply to requests for information.
- Do not re-post messages without permission.

Acceptable Internet Use

- Avoid cross-posting messages. If you do cross-post, make sure the subject of your message is relevant to all recipients. If you are going to cross-post, apologize, especially if a large number of the group participants overlap. Also apologize for any mistakes in posting.
- Do not post personal messages to a group. Example: Don't post something like "I am looking for Joe Smith who went to Smallville High School in 1967."
- Do not post messages anonymously. This is viewed as bad form by the Usenet community and system managers are asked to track down offenders. This wastes the company's time and resources.
- If you survey a group, post a summary of your results.
- Indicate quoted materials, and make sure your citations are right.
- Place a clear description of your subject in the "Subject:" line.
- Post test messages only to *.test groups. Posting test messages to other groups is rude.
- Remember that monitoring news groups or participating in mailing lists takes time. Don't overextend yourself. For Usenet, check news.announce.newusers for FAQ lists and other interesting stuff on getting started.
- Flame carefully, or not at all. Remember there's a person on the other end of your connection. Never flame 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.

Acceptable Internet Use

File Transfer Protocol (FTP)

- Do not ftp to any machines on which you do not have an account, or which doesn't advertise anonymous ftp services. Do not randomly search the net for ftp sites and files
- Observe working hours or posted hours for ftp sites. Most sites request you NOT to ftp between their local hours of 8 am to 5 pm.
- Don't ftp during your sites prime hours.
- Look "locally" before ftp'ing something from a site geographically remote.
- Don't ftp on the off chance that you might need it someday. Conversely, don't hunt around for "neat stuff" to ftp. If you discover you don't need what you have ftp'ed, delete it. You can always get it again if you need it.
- Observe any posted restrictions on the server.
- Use your real username and node as your password on anonymous ftp servers.
- Follow all posted guidelines for uploading files to an ftp server.
- Make sure your uploaded files are working or error free before posting them on an ftp server.

Telnet

- Do not telnet to machines on which you do not have an 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've telneted.
- Do not try to telnet into miscellaneous ports; use only authorized ports for access.
- Do not leave yourself logged in when you are not using the machine. Log out if you are leaving, you can always telnet in again later.

Acceptable Internet Use

World Wide Web

- Observe any posted restrictions on the server to which you've connected.
- When downloading large files, choose off-peak, non-business hours to do so.
- Observe requests to limit usage during posted hours, World Wide Web servers are very popular on the Internet and overtaxing your favorite server can lead to its demise. System Administrator's will shut down servers if the network flow is causing capacity or performance problems on their networks.
- Use Bookmarks to mark you're favorite sites so that you can return to them quickly and efficiently.

Acceptable Internet Use

Acceptable Use Policy

The News Corporation Global ATM Network provides network transport services for News Corporation and its business units. The News Corporation provides for inter-networking between News Corporation locations, between News Corporation locations and other locations. The existing infrastructure also carries information between News Corporation locations and public networks, including the public Internet. The internal networks carry sensitive, proprietary, and confidential information needed to conduct Company business. This Acceptable Use Policy details the user responsibilities in protecting any and all information that travels this network or is accessible via this network.

Users, defined as employees of the Company and other individuals authorized to use all or part of this network, are expected to act responsibly when using the resources of this network, just as they are expected to act responsibly when using any resources of the Company. Users are expected to access only those resources for which they are authorized, to consume only those resources needed to perform their business function, and to maintain professionalism in all communications among peers and in public forums.

- Misuse and abuse of network services, including unauthorized access or lack of attention in implementing security measures on systems connected to the network, puts the integrity and confidentiality of the Company's and our clients' information at risk.
- All use of the network consumes resources, and misuse or abuse of capacity can impact availability in the short run and cause unnecessary expense in the long run.
- Careless or unprofessional communications with clients or on public forums places the Company's reputation at risk.

The following list of DO's outline behavior expected of the professional and dedicated employees and business partners authorized to use any network to conduct Company business, including the News Corporation world-wide network, News Corporation Network resources (including its ISPs), client networks and the public Internet.

- DO access only those systems and networks for which you have been authorized. Attempts to use the network or resources on the network to access unauthorized information, to identify or exploit security holes, or to bypass security measures, is improper behavior. Those with a justified business need, i.e., network and security management, must be authorized in writing by their technology director to perform these activities.

Acceptable Internet Use

- DO perform all security precautions that are necessary to protect systems and information under your control. Follow all security standards and take additional precautions as necessary to protect the confidentiality and integrity of information. For managers this means you must direct and expect your administrators and users to include security in their job responsibilities. For administrators this means staying informed about security risks, implementing and maintaining security processes per Company standards, and following good practice concepts per your system type. For users this means maintaining awareness of security risks and taking actions to reduce those risks, i.e., good password management, maintaining secure workstation configurations, protecting physical access, maintaining backups, etc.
- DO respect the confidential nature of all information. Review and understand the Company standard regarding proprietary and confidential information. Remember that all information, unless specifically encrypted, travels the network in clear text. Users should be especially careful when conducting business across the public Internet to evaluate the confidential nature of these communications. If in doubt about the confidential nature, ask and obtain written permission or use other means to deliver the information.
- DO respect all copyright and ownership rights. When obtaining information from public repositories or providing information, verify your right to reproduce and distribute this information.
- DO make efficient use of your network resources. Transfer large quantities of information during time frames with the least impact on network capacity. Recognize that certain activities, chain letters, large file transfers, multi-media services, games like DOOM, etc., can severely impact network resources. Any such activities must be authorized by local management. If the activity crosses network boundaries, it must be authorized by all effected network management groups. Chain letters that propagate and multiply information on the network are never authorized.
- DO keep personal use to a minimum. All network usage creates expenses in sizing the network. Excessive use for personal reasons is improper behavior. Personal use of network services to access resources on the public Internet must be authorized by your local management. All other personal use is unauthorized.
- DO maintain professional demeanor in all communications, especially those on public forums. When your identify is coupled with the News Corporation name while communicating in public forums and with client companies, carefully consider the impact of your words on this audience. Review all communications to verify that your message conveys the professionalism and expertise symbolized by the News Corporation name. If in doubt, ask a colleague, your manager, or even public relations, to review your message for potential impact on the public audience.

1

Acceptable Internet Use

- DO review and understand your responsibilities when accessing resources on the public network. Many news groups provide FAQs (Frequently Asked Questions) that explain the rules and expected behavior for that forum. Learn about the expected behavior for every service you use or provide and perform this service as specified by the service provider.
- DO verify that all network services provided to the public meet Company standards. All network services, including Web servers, anonymous FTP sites, mailing groups, etc., must be reviewed and approved by XXX. These services have a strong impact on our public image and must meet the high standards that our reputation demands. These standards may refer to both content and security issues.
- DO access and provide network resources as a trusted and responsible person performing Company business. This Company believes that its employees and business partners are trustworthy and responsible people. The Company also recognizes that there will be occasions when people abuse that trust and perform inappropriate, irresponsible, improper and even illegal activities. These people must understand that they will be held accountable for this type of behavior.

Acceptable Email Use

2

This chapter describes News Corporation's electronic e-mail policies and covers the following topics:

- E-mail Forwarding
- Generic Accounts
- New User Accounts
- Passwords

Acceptable Email Use

E-mail Forwarding

It is a violation of our corporate email and email security policy to forward corporate email from our internal post office to an unsecured outside mail account such as, but limited to AOL, Hotmail, Yahoo mail and like services. These accounts are not secure, nor do they scan for viruses. Once received they can by the very nature of forwarding (or relay) infect our systems with a virus or libel us if we cause harm to another companies email system.

- Anyone asking about this should be informed of the consequences if they choose to go ahead anyway as this can lead to disciplinary action or termination.
- That individuals who have been informed of this policy, but show a disregard for this policy will have a email sent to them again explaining this policy again and the issues involved.
- That the forwarding rule will be suspended and their account password changed within 24 hours.
- That in the email, they are to be told that the password has been changed and to contact the help desk for assistance in obtaining a new password.
- That an email is to be sent to Information Protection - Director, Desktop Support - Director, and the Account Administration Team Members that this is going to be done.
- That an administrative note be placed in the "admin" box noting the date and by whom was the account- forwarding rule canceled.

GroupWise Remote access, dial-up, VPN services were established for this purpose. If explained in the right manner, generally most will abide by this request.

Generic Accounts

There is to be no creating of generic accounts moving forward, if some one is logging into our systems, creating and sending email, accessing the Internet then he or she needs an account. Example would be "temp1, temp2" and so on. This may be a pain but not near as much if, legal or HR needs to identify an individual to email or incident and we can not.

Acceptable Email Use

New User Accounts

The same goes for the renaming of an existing email account to a new user. That user account will be disabled and set for our standard 30-day deletion (unless otherwise noted) and new account will be created. If access is needed and this was not a hostile termination then rights to that account can be granted to read the email contained in the old account.

If it was a hostile termination, to prevent any litigation possibilities, HR must give their permission to have the password changed and access granted to that account.

If requested by management other than HR that the account password be changed and access be granted, then again HR must give permission.

It should not be assumed that because they were terminated that we (management) have the right to open the mailbox.

Passwords

It is a violation of both Fox and News Corporations electronic usage policy to share, give, record or pass-on passwords to individual network logon or email accounts. For those employees that require the ability to share email each person has the right to set up a "proxy account." Passwords are for the owner of the account and are not to be shared. Employees that are aware of this policy or violate this policy and after being warned, can face dispensary action up to including termination of employment.

2

Acceptable Email Use

News Corporation IT Forms

3

This chapter provides the following example forms and memos:

- E-mail Policy Reminder
- Dismissal Memo

News Corporation IT Forms

E-mail Policy Reminder

Date:

To:

From: Information Protection & Security, Fox Entertainment Group

Subject: E-Mail Policies

The purpose of this email is a reminder that Fox has an Electronic Usage Policy that covers both email usage and Internet access as well as other forms of "electronic communications." This policy which is enforced by Information Protection & Security and endorsed by both News Corp, Fox Human Resources and Fox Group Legal Affairs can lead up to and include termination of an employee who shows a disregard for this policy or may cause harm to News Corp and or its affiliates computer environment. This policy covers the sending of material that may be considered offensive by the receiving party or is a clear misuse of corporate resources; this covers both an employee of News Corp and any other entity.

Some email by their very nature when sent in mass or thought of as funny; can be mis-directed to companies or parties other than the intended. They can cause system and network slowness as well as system crash's. This puts an undue burden on the groups that are charged with maintaining the integrity and serviceability of our corporate network and email environment. These can also contain viruses or malicious code that can destroy data both on your local computer, as well networked systems. The best course of action is to delete these messages before you open them and to inform the sender of our policy regarding these types of email. Never send or forward them yourself either internally or to any other outside mail service.

Please be aware that Information Protection & Security is in receipt of such an email sent by you and you are in violation of this policy.

The JOKE_SMALLPEN virus has been detected in e-mail traffic.

Sender: xxxxx@fox.com

Recipient: aphunk@earthlink.net, andreachia@yahoo.com,
[Amy Buesing@condenast.com](mailto:Amy.Buesing@condenast.com), agent_elle@hotmail.com,
Jamie.Becker@rhino.com, fipper@excite.com, JacqVuong@aol.com,
MJohnigan@Affinity.com, ciida@mveg.com, alexis@tomlynchco.com,
jupiter@freshjive.net, aball@agron.com

File: Rumor.exe

Action: deleted

Tuesday, November 11, 2000 @ 8:55 A.M.

News Corporation IT Forms

By receipt of email, we consider you have been notified and that any further email of this type will generate a report and be forwarded to Fox Human Resources and Fox Group Legal Affairs for appropriate action. If you have any questions please feel free to contact me, if you want a copy of the above stated policy please contact your HR Representative. Thank you for your attention to this matter.

Sincerely,

News Corporation IT Forms

Dismissal Memo

Date: 01/17/01

To: Fox Plaza Security, Fox Lot Security

From: Jack Johnson, Manager, Information Protection, Fox

Subject: Access to Fox Facilities

As of today, the following person is not to be granted access to any 20th Century Fox entity.

- Jane Doe
- John Doe

There are to be no exceptions to the above list without written authorization. Any requests for changes to this list must bear the signature of either John Smith, Exec Director, CCS, Mary White, Associate Director, Information Protection, Alice Anderson, Director HR -IT or Jack Johnson, Manager, Information Protection. Any questions you may contact me at 310-555-0000 or by Cellular 310-555-1111