Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Development of an Effective Communications Use Policy

I have just finished editing a proposed Communications Use Policy that is currently awaiting adoption by my company's leadership. The policy was in draft form when I received it, but I inherited the responsibility for getting the policy approved by the governing board of the company. The proposed policy faced almost immediate re-editing due to an outbreak of a computer virus caused by a user accessing an Internet based email service through the company's Internet portal. While I was editing the policy, by drafting a re...

Copyright SANS Institute
Author Retains Full Rights

AD
CounterTack
Counter Tack Active Monitoring for In-Progress Attacks
GET THE WHITE PAPER NOW >>>

GIAC Security Essentials Practical
Development of an Effective Communications Use Policy
By Tim O'Neil
July 2, 2001

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Table of Contents
Development of an Effective Communications Use Policy

Introduction	3
Statement of Purpose	4
Privately Owned Computers Used for Business	5
Personal Use Policy	6
Ownership of Information	6
Informed Consent	7
Prohibited Conduct	9
Disciplinary Action	11
Violations of Law and Policy	12
Use of Non-Limiting Language	12
Awareness is Key to a Successful Communications Use Policy	12
Publication of the Policy	12
List of References	15

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

INTRODUCTION

Development of a good Communications Use Policy (also called an Acceptable Use Policy) is the cornerstone of a strong information security program. As an Information Security Professional, the development and implementation of such a policy is one of the most effective tools that you have for insuring the proper use of your company's information systems.

Therefore, development of the policy should be a top priority and it should be continuously updated to insure that new technologies or threats are properly addressed. Consider the policy your contract with the end user to allow the use of the company's information technology assets in exchange for an agreement by the employee to act appropriately when utilizing them. You might even consider it to be a driver's license for the Information Superhighway.

I have just finished editing a proposed Communications Use Policy that is currently awaiting adoption by my company's leadership. The policy was in draft form when I received it, but I inherited the responsibility for getting the policy approved by the governing board of the company.

The proposed policy faced almost immediate re-editing due to an outbreak of a computer virus caused by a user accessing an Internet based email service through the company's Internet portal. While I was editing the policy, by drafting a restriction on accessing e-mail accounts of this type, I also researched existing policies on the Internet.
I thought that this topic might be a worthy candidate for discussion. Therefore, the goal of this dissertation is to:

1. Identify the most common elements of a communications use policy.
2. Discuss why these elements are necessary to having a successful policy.
3. Compare and contrast these identified elements among the different policies.
4. Offer guidance in the furtherance of having a successful policy.

I drew from the various policies I encountered in order to finish our use policy and also researched information for this article. Because most communications use policies belonging to private companies remain private internal documents; most of the published use policies I was able to locate on the Internet belonged to public universities.

All of the policies encountered during my research followed a fairly standard format, sharing relatively common provisions, requirements and prohibitions:

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The policies I encountered held the following provisions in common:

- Statement of purpose
- Ownership and expectation of privacy
- Personal use policy
- Prohibitions on unacceptable conduct
- Disciplinary action

STATEMENT OF PURPOSE:

The main reason for the policy needs to be enumerated because end users need to know the rules of the road, specifically what is permissible and what is prohibited use of the company's computing assets.

The reasoning for placing such parameters into a formal document should be self-evident in these days of vagarious legal liability: The employee cannot be expected to conform to unwritten rules pertaining to use of the company's IT assets. The company's leadership must insure each employee is provided information and will abide by a known and published code of acceptable computer usage.

Users need to understand the policy objectives. There is a two fold reason for this; you wish the reader to understand the policy was written with a worthy goal in mind and that hopefully, the employee will partner with the company by obeying the policy in furtherance of this goal. The scope of the policy defines what will be addressed and how it will be effected by the policy.

The Purpose Statement in the California State University San Bernardino Acceptable Use Policy for Electronic Communications:

> **The purposes of the University computing and communications resources are to provide a setting and opportunity for members of the academic community to express and explore ideas openly and freely subject to conditions and terms of this policy, to acquire and develop the skills of intellectual inquiry, and to examine critically the values of culture and society. This policy assumes as a condition of use the exercise of common sense, common courtesy, and a respect of the rights and property of the University and others.**
>
> **This policy sets forth users' rights and responsibilities and is designed to address related access, use, and privacy issues in a way that meets intellectual and creative needs of campus users. The University's legal responsibility assures the maintenance of the campus network systems and treats the campus community with respect.**[1]

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The purpose statement in the University's policy statement conveys a sense of academic freedom and intellectual inquiry. It also assumes a certain level of common understanding among the user base in the definition of sometimes ambiguous terms such as "common sense" and "common courtesy".

The University of California's Communications Use Policy defines the purpose of their communications policy as follows:

- **Establish policy on privacy, confidentiality, and security in electronic communications;**
- **Ensure that University electronic communications resources are used for purposes appropriate to the University's mission;**
- **Inform the University community about the applicability of laws and University policies to electronic communications;**
- **Ensure that electronic communications resources are used in compliance with those laws and University policies; and**
- **Prevent disruptions to and misuse of University electronic communications resources, services, and activities[2].**

This policy seems a little bit clearer in delineating or defining what the policy applies to and seems to shy away from the more esoteric concepts of the previous purpose statement.

My company's purpose statement is four paragraphs long and I consider it to be on point when it comes to delineating the objective of the policy. I will just share the last two paragraphs, which I developed in order to convey two points: (1) that the systems represent a substantial investment. And (2) that the end users have to agree to consent to the policy before they can use the systems:

> **This policy was developed to protect the company's communication system investment from loss due to exposure to computer viruses, end user misconduct, activities that waste system resources, or any other prohibited conduct that could result in damage to these systems.**
>
> **These systems represent a substantial financial investment in equipment, personnel and resources. Therefore, it is important that each user understand what is acceptable use of the company's communications systems, as well as what is prohibited use. It is required that the user agrees to abide by this policy before access to the company's communications systems will be granted[3]**

PRIVATELY OWNED COMPUTERS USED FOR BUSINESS

The scope of the policy should apply to all company owned or controlled computer systems and to every employee or contractor. <u>Be careful when applying the policy to computer systems owned by a third party.</u>

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The law generally favors the employer in issues involving discovery during litigation involving an employee's privately owned home computer, if it is used to do company related work. "Co-mingle at your own risk" is a fairly standard refrain from attorneys involved in discovery against such personally owned systems. This means that if you use the system for any company business, the company can and may subpoena such information in a civil action, should the need arise.

It would not be advisable to have a communications use policy apply to an employee's personal home computer, other than to perhaps bar its use for business purposes.
Contractor owned computers can and should only be addressed in the policy concerning connection to the network, review of material on the computer, and virus protection, but more properly, this issue could be better addressed in a separate policy.

PERSONAL USE POLICY:

Allow personal use of the computer, if in the view of the company's leadership, the use does not interfere with the main job functions of the employee. You may wish to limit this personal use to break and lunch times, but maintaining these restrictions may be difficult.

Some employers have tried to ban all personal use of the computers and have essentially painted themselves into a corner, as this is akin to barring personal use of the telephone at work. Sure, there may be certain jobs were no personal use of a computer could be allowed, such as on production lines, however, in normal office environments, employers should be realistic when evaluating what the limits should be on the personal use of computers.

At the end of the day, it should be a conscious managerial decision to allow some personal use of the computer and to set limits on that usage. Each workplace is different, so the amount of personal use should be a managerial decision made at each company or at different departments throughout the company.

The limits of this use should be established as a well thought out policy that will both ensure that workers do have some access to a wonderfully powerful tool, yet protect the employer from liability and ensure a reasonably productive environment.

THE OWNERSHIP OF INFORMATION AND INFORMATION SYSTEMS:

Current accepted legal doctrine, at least in the United States, is that information produced on company electronic data processing equipment is company property and end-users should have little expectation of privacy. A statement concerning the ownership of information and the user's expectation of privacy are important, as it is necessary that the user be informed of this condition and consent. We use the following stipulation, which serve as a fair warning of both the ownership of the information and the user's expectation of privacy:

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

INFORMATION TRANSMITTED ON COMPANY COMMUNICATION SYSTEMS IS COMPANY PROPERTY

> **All information or data created, transmitted, received or stored using any Company communication system remains Company property and may be monitored, reviewed, used, published or disseminated by the Company for any purpose it deems appropriate. Company employees do not have any right or expectation of privacy with respect to such information or data. Any decision to monitor, review or use personal communications, including stored or retained information or data, will be made by the Company consistent with legitimate business interests and will require the approval of the Human Resources Department.**
>
> **The company may access, at any time, a user's communication or computer systems to review, retrieve, delete or otherwise make use of such information or data. Additionally, the company may track, monitor and/log any and all aspects of an employee's use of such systems, including monitoring Internet sites visited, chat and newsgroups joined, file downloads and all communications, information or data transmitted, sent, received, viewed or stored by users.**[4]

The California State University San Bernardino Acceptable Use Policy for Electronic Communications addresses the ownership of information in the purpose statement as follows:

> **In keeping with its mission, the University provides computing and communications resources to members of its community. The computers, networks, and computing facilities made available by the University for student, faculty, and staff use are the property of California State University, San Bernardino, and are provided for the completion of academic requirements, scholarship, and administration of the University**[5]

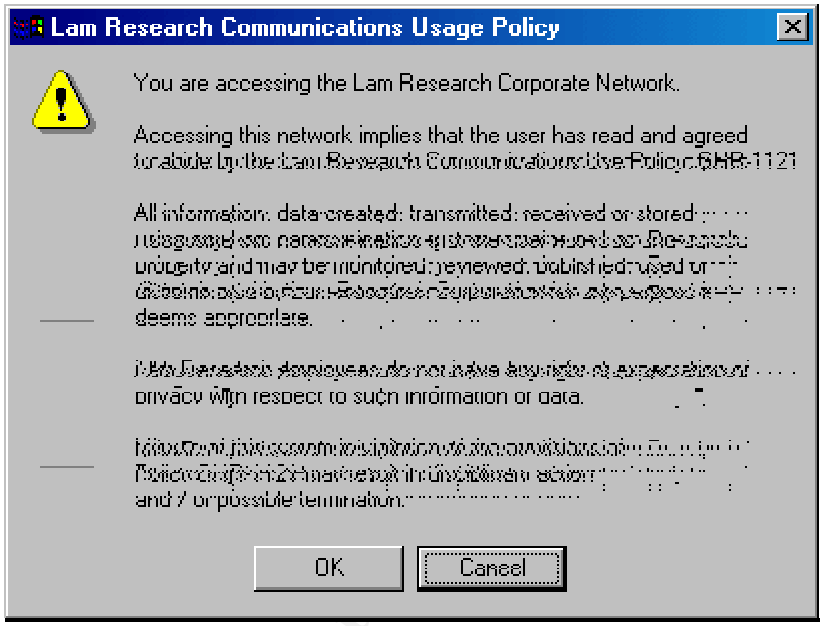
INFORMED CONSENT

There may be a desire to actually have the end user sign the policy document stating that he or she has read and will abide by all the provisions of the policy. While this activity will certainly not hurt the employer in court, the logistics of this undertaking in a large company are quite significant. It might be better to simply post the policy on the company's Intranet site and send out an email with a link to the site informing the users of their responsibility to read and abide by the policy.

Banner warnings are also in wide use in the military and government. When a user logs onto the computer a banner will appear with a written warning that normally paraphrases verbiage contained in the use policy specifically addressing the ownership of information, the user's expectation of privacy and the monitoring of the computer usage. The user must click "OK" to log on and acknowledge the warning. I have heard feedback from

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

government officials saying that a banner warning amount to little in terms of informed consent, but again its inclusion may serve as a counter argument to a user claiming total ignorance of a policy's existence. The configuration of a banner warning can be accessed directly through the Registry in Windows NT or W2K or through the Policy Editor (Poledit)



Companies that have less robust workstations such as Windows 95, 98 or ME, which do not have this capability may consider configuring the warning to run as a log-on scripts or may place the warning on filtering software, if they use this subscription service, or on the company 's firewall.

> **All information or data created, transmitted, received or stored using any company communication system remains company property and may be monitored, reviewed, used, published or disseminated by the company for any purpose it deems appropriate. Company employees do not have any right or expectation of privacy with respect to such information or data. Any decision to monitor, review or use personal communications, including stored or retained information or data will be made by the company consistent with legitimate business interests and will require the approval of the Human Resources Department**.
>
> **The company may access, at any time, a user's communication or computer systems to review, retrieve, delete or otherwise make use of such information or data. Additionally, the company may track, monitor and/log any and all aspects of an employee's use of such systems, including monitoring Internet sites visited, chat and newsgroups joined, file downloads and all communications, information or data transmitted, sent, received, viewed or stored by users**.[6]

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

PROHIBITED CONDUCT

Be specific in areas concerning prohibited conduct. We get some interesting feedback in reference to the steps we take to stem the flow of pornography on our network. Some feedback from the user base is that surfing for pornography is a harmless pastime and should be overlooked. The absurdity of this stance should be evident in this litigious society that we live in.

> **In the article Liability Cyberviolence Poses Legal Problems by Peyton Smith**
>
> **A February 1999 poll by Stamford, Connecticut-based NFO Interactive revealed that more than half of surveyed workers said they received inappropriate e-mails while at work, e-mails that were racially offensive, sexually explicit, or hostile towards a particular religion.**
> **Aside from a loss of worker productivity, should an employer care about violence perpetrated through cyberspace? The answer is a resounding "yes." As a June 1, 2000, case by the New Jersey Supreme Court makes very clear, an employer can be liable for violence committed with the aid of employer-sponsored computers and services.**
>
> **An employer can be liable for the actions an employee takes against a third party on several different theories, most of which are grounded in common law: (1) negligent hiring; (2) negligent retention and supervision; (3) voluntary assumption of a duty to protect another from harm from someone else; and (4) "respondeat superior," or vicarious liability.**
>
> **There are also statutory theories of liability when the victim is a co-worker. The Occupational Safety and Health Act of 1970 imposes a general duty on employers to provide a workplace free of recognized hazards. State law also usually provides for some sort of recourse against an employer; for example, a claim for retaliation of an employee under workers' compensation statute.**[7]

Therefore, it is best to prohibit conduct, which could make the employer liable. We address the issue in specific enough terms to clearly identify the conduct, while still leaving enough “wiggle room” or non-limiting language to allow for discretion in how the policy will be applied.

We break down prohibited categories of content accessed via a company workstation into several categories:

- **Is sexually explicit or can be considered vulgar or obscene;**
- **Can cause or contribute to a hostile work environment or one which is patently offensive to or disrespectful of fellow employees; or**

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- **Violates company policies or procedures relating to equal opportunity, sexual harassment, and protection of confidential information or workplace violence.**
- **Is considered a danger or risk to the security, or operability of the company's information technology infrastructure[8]**

The last criteria addresses such things as viruses and hacking or password guessing programs and provides the company with enough latitude to address evolving threats, such as newly developed malicious programs such as Back Orifice and Sub-Seven while not addressing the specific programs.

The Carnegie Mellon CERT defined their criteria for Acceptable Use Policy Issues for Users as follows:

- **prohibiting sharing of accounts**
- **requiring good passwords**
- **guidelines for accessing unprotected programs or files**
- **breaking into accounts**
- **breaking into systems**
- **cracking passwords**
- **disrupting service[8]**

Finally, we enumerate in detail the specific things that are prohibited, again using non-limiting language: Certain uses of the communication systems are specifically prohibited, <u>including, but not limited to, the following:</u>

- **Creating, transmitting, viewing, using or storing any communication, data or information that violates Company's policies or procedures relating to equal opportunity, sexual harassment, protection of confidential information, workplace violence, or the terms or conditions of employment.**
- **Creating, transmitting, viewing, using or storing any communication, data or information that is sexually explicit or that can be considered vulgar or obscene, or which can cause or contribute to a hostile work environment or one which is patently offensive to or disrespectful of fellow employees.**
- **Creating or transmitting to fellow employees, clients or customers chain letters.**
- **Creating or transmitting to fellow employees, clients or customers personal business ads, solicitations, promotions or commercial announcements.**
- **Creating or transmitting to fellow employees, clients or customers any communication, data or information for the purposes of religious recruitment or conversion.**
- **Creating, transmitting, viewing, using or storing "pirated" software or any communication, data or information which is in violation of another person's legal, proprietary or trade secret rights or Company's Legal Use of Software policy.**

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- **Creating, transmitting, viewing, using or storing destructive software code or programming (e.g., viruses, Trojan horse programs, etc.).**
- **Creating, transmitting, viewing, using or storing any unauthorized communication, data or information, or otherwise making public or disseminating any unauthorized message or transmission, relating to Company, its business, products, finances or competitors, or containing any Company confidential or trade secret information.**[9]

Other Prohibitions: Streaming stock tickers and media, Web radio, MP3 files and many other web based applications waste network bandwidth. The use of non-business related bandwidth intensive applications should be limited or prohibited in order to conserve bandwidth. The same goes with email chain letters and other mass mailings of emails; they tie up systems resources for no good reason.

You cannot prohibit every computer- related practice simply because it is not work related, but an otherwise benign activity. Current computer technology evolves so quickly, there is a constant stream of innovative programs being introduced, some of which may prove detrimental to the health of your network. Visual Basic constructed viruses, such as the Melissa Virus, have taken innovative programming language and put it to a malicious use. These viruses have multiplied, yet few within the mainstream IT industry had foreseen their arrival. Some companies have taken extraordinary steps to protect their systems by not allowing VBS attachments to cross their email gateway

Our company recently had a .vbs based virus infiltrate our network through a users private Internet email account, which was accessed through the company network. While most of these services do have very proactive virus screening programs the service; the one our user connected to did not, our network became infected and a stipulation barring the access of such services was the result.

Concerning repercussions for knowingly violating our Communications Use Policy, we have added the following stipulation:

DISCIPLINARY action

> **Each employee is responsible for controlling and monitoring his or her use of company communication systems both during and outside regular business hours. Any improper use of company communication systems or violation of company policies or procedures with respect to such systems, core values harassment or discrimination may result in severe disciplinary action, up to and including termination of employment.**
>
> **Violations of this policy that result in the transmittal of a computer virus into Company's data network may result in the termination of the employee responsible for the violation.**
>
> **Questions regarding the interpretation, application or enforcement of the company's policies and procedures should be directed to and will be resolved**

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

by the Human Resources Department.[10]

The University of California's policy regarding

VIOLATIONS OF LAW AND POLICY

> **Sanctions of Law. Both federal and state law prohibits the theft or abuse of computers and other electronic resources such as electronic communications resources, systems, and services. Abuses include (but are not limited to) unauthorized entry, use, transfer, tampering with the communications of others, and interference with the work of others and with the operation of electronic communications resources, systems, and services. The law classifies certain types of offenses as felonies (see Appendix B, References).**
>
> **University Disciplinary Actions. University policy prohibits the use of University property for illegal purposes and for purposes not in support of the mission of the University. In addition to any possible legal sanctions, violators of this Policy may be subject to disciplinary action up to and including dismissal or expulsion, as relevant, pursuant to University policies and collective bargaining agreements. Further information on permitted and prohibited uses is given in Section III, Allowable Use**.[11]

Non-Limiting Language

Every policy needs to incorporate a standard statement enumerating the penalty for the violation of the policy. This section needs to reinforce the company is serious about protecting its investment in information technology and provide "fair warning" to employees their misuse of the systems could result in serious repercussions. While it is necessary to do this, it is helpful to use statements that give the management of the company a great degree of latitude or discretion in punishing offenders. The use of non-limiting language is recommended; i.e., use the word 'may" instead of 'will", and "up to and including" when discussing termination of employees.

Awareness is Key to a Successful Communications Use Policy

The best communications use policy is not worth the paper it's written on if the end users don't know about it. The level of awareness among the user base must be cultivated until not only do the users know there is a policy, but they remember the key provisions of the policy and support its goals. Publication, distribution and reinforcement are key, as well as developing a mechanism for feedback, as you will surely need to know if the policy is overly burdensome or if key policy provisions simply don't work

Publication of the policy:

Make the document a living one that serves as your contract with the end user and the basis for the development of implementation of procedures by:

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- Notifying the end user's of its existence and their responsibility to read, understand, and agree to abide by the policy.
- Introducing the policy during new hire orientation.
- Publishing the document on the company's Intranet site.
- Distributing pamphlets or handouts.
- Consider hosting events to highlight the new policy.
- Using give-away items like key chains or mouse pads inscribed with slogans.
- Using Logon Banner ads that notify the user that logging on to the network implies consent.
- Reinforcing the policy at every opportunity, notify the users on a regular basis of its existence.
- **Using other innovative techniques to get your message out to the end users such as the following example concerning an information security program developed by Aetna Insurance:**

  The biggest security risk to any organization comes from within. The Computer Crime and Security Survey conducted by the Computer Security Institute has found that an average of 70 percent of respondents over six years has cited disgruntled and dishonest employees as a likely source of security problems. But a report from the SANS Institute says that many insider security problems also result from employees' lack of knowledge.

  The keystone of the Aetna InfoSec Awareness program is a Web-based exam that resides on Aetna's security portal. The exam must be completed by employees within 30 days of hire and annually thereafter. Before beginning the exam, employees must sign off on Aetna's security policy.
  The exam is divided into six modules. Each module presents information and a series of questions for reinforcement. Each module takes 3 to 7 minutes to finish, and employees can complete them at their convenience within a one-year period.
  The exam covers things that are generally part of Aetna's "...Code of Conduct, which addresses the use of technology and information resources, and the handling of confidential information. For example, you don't want to open up attachments if they have an extension of .vbs or .exe," Richmond said. "Or you don't want to fax something sensitive if you don't have someone ready on the other end to pick it up."
  The exam isn't technically a test because employees can't fail, but the testing paradigm engages the user and provides employees with an interactive experience. It's up to managers to enforce Aetna's security awareness training policy and address employees who don't comply.
  Compliance with the program has been high—85 percent the first year and 100 percent last year. Aetna's security team is also increasing awareness through some savvy internal marketing. "We've tried to brand information security internally," said Richmond. "We conducted a Web-based contest to come up with a logo, a lighthouse called Beacon--a guiding light for good security practices.[12]

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

In summary, the value of the information and information systems on which they reside should be the key determinate in the development and implementation of a strong communications use policy. Currently there are several legislative initiatives under way that will legalize mandates for the security and privacy of information systems. A company would be remise if it were not more proactive than to wait for legal mandates to be placed into law. Information Security professionals must do everything within its power to ensure the end user is aware of and will abide by policies made to address the legitimate legal concerns of their employer concerning the security of the network and the legal responsibility to provide a safe work environment

© SANS Institute 2001, Author retains full rights.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

List of References:

[1] California State University Cam San Bernardino Acceptable Use Policy for Electronic Communications

[2] The University of California's Communications Use Policy found at http://www.ucop.edu/ucophome/policies/

[3] Lam Research Corporation Communications Use Policy, unpublished

[4] Lam Research Corporation Communications Use Policy, unpublished

[5] California State University Cam San Bernardino Acceptable Use Policy for Electronic Communications.

[6] Lam Research Corporation Communications Use Policy, unpublished

[7] Cyberviolence: Liability Poses legal Problems by Peyton Smith, Workplace violence Prevention Reporter.

The Carnegie Mellon CERT defined their criteria for Acceptable Use Policy Issues for Users at http://www.cert.org/present/cert-overview-trends/tsld217.htm

[8] The Carnegie Mellon CERT defined their criteria for Acceptable Use Policy Issues for Users at http://www.cert.org/present/cert-overview-trends/tsld217.htm

[9] Lam Research Corporation Communications Use Policy, unpublished

[10] Ibid.

[11] The University of California's Communications Use Policy found at http://www.ucop.edu/ucophome/policies/

[12] A Healthy Security Attitude; Aetna's InfoSec Awareness Training Program Keeps Employees on Course by Debra Donston, eWeek, June 11, 2001 12:00 a.m.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: August 31st, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced