One of Many Books in the Need to Know Series from BrainMass

A NEED TO KNOW TEMPLATE

End User Information SYSTEMS POLICY

By Rob Beachy

Ideal for Information Technology Professionals

BRAINMASS

www.brainmass.com

End User Information Security Policy Template

By Rob Beachy

© BrainMass Inc. 2012

What Is This Book?

Everything You Need to Know publications are the best way to get a quick but detailed overview of a specific topic. Within the pages of this book, you'll find exactly what you need in order to understand the key concepts of this topic. You'll find yourself completely prepared for the next stage of your learning as is relates to this topic. Within every book, we include a collection of the most important terms and their definitions so that whenever you're in need of a refresher, you can easily refer back and remind yourself of what you're dealing with.

This book is a policy template that can be modified and used within your company. Templates are meant to provide a basic structure for a policy and are not deemed to be a one size fits all policy for every situation. If any part of this policy template is in question, you may want to seek the advice of a corporate attorney.

An End User Information Technology Policy is needed to ensure that all employees understand their responsibilities in regards to conduct and safeguarding of information and corporate data.

This book is ideal for the Information Technology professional that has been tasked with creating an End User Information Technology policy.

Table of Contents

Introduction

Personal computers (PCs), mobile devices, and Internet resources have become a powerful yet complex tool for *[Company Name]*. When used effectively, technology can significantly increase the productivity of employees and business activities. The Corporate Strategic Plan and external regulation require PCs be properly managed. This policy contains rules and working guidelines to be applied to the uses of this technology at *[Company Name]*.

It is *[Company Name]*'s intention to provide each employee reasonable access to the technology required to fulfill the responsibility of their position.

It is also *[Company Name]*'s objective to adequately safeguard the computing environment to ensure appropriate confidentiality, integrity, and availability of the data generated and to reasonably protect the significant dollar investment *[Company Name]* has made in this technology.

It is the responsibility of each individual user of *[Company Name]*'s computing resources to adhere to the guidelines set forth in this policy. It shall be made clear to all employees that all personal computers and software are the sole property of *[Company Name]* and as such are subject to monitoring without employee consent. Employees who violate any of these guidelines will be subject to the same disciplinary actions that accompany infractions of other *[Company Name]* policies. These actions may include counseling statements, suspensions and/or termination.
This Policy is effective immediately.

Everything You Need To Know

This eBook is a policy template. A policy template, unlike an instructional eBook is not meant to teach a subject. A policy template is meant as a starting point for establishing your own company specific policy. Policy makers often are responsible for different functions within a company. Creating a policy from scratch can be a daunting and time consuming process. By utilizing a policy template, 90% of the work is already done for you. All that would have to be done is change some company specific information, such as Company name, titles, and other names and then review the policy for completeness and modify as needed. If in question about anything within this template or its legal standings within your business, please consult a corporate attorney.

A policy template is structured in a similar, but slightly different manner then a regular BrainMass eBook. An instructional eBook is structured using a whole number (1, 2, 3, etc) for main topics and subtopics are listed as the main topic and a new number separated by a "." (1.1, 1.2, 1.3, 2.1 etc).

This policy template uses the same number scheme, but introduces a new formatting option, a placeholder.

There will be points throughout the template where a term will be italicized and listed in square brackets "[ ]". This will be points where you can enter your own company specific information. For example: This policy is created so that *[Company Name]* employee's will understand the rules. The "*[Company Name]*" is a placeholder for you to enter your Company name.

This new option will allow for an easy copy and replace function. For example, in Microsoft Word you could hit Ctrl+H and choose to replace *[Company Name]* with ABC Inc.

1. Computer Hardware

The *[Title of IT Officer]* should be notified immediately of any problem occurring with PC Hardware. The *[Title of IT Officer]* or a designated representative will determine whether a vendor service call is required. They are the only employees allowed to place a hardware service call. On a case-by-case basis, it may be allowed by an end user to place hardware service calls.

1.1 Personal Hardware

No personally owned hardware may be used on the *[Company Name]*'s local area networks without approval of the *[Title of IT Officer]*. This is to include, but not limited to laptops, cameras, printers, USB drives, or scanners.

2. Computer Software

2.1 Approved Software

Any software used by *[Company Name]* will be obtained from a reputable dealer or agency. This will ensure a continued source of support and enhancements and give assurance that the software meets all legal guidelines.

Only legal software will be purchased and used by the *[Company Name]*. Legal software is that which is purchased and used according to the manufacturer's license agreement. This generally means that an original product package (CD and/or documentation or license certificate) is needed for each occurrence of the product on a PC or LAN.

2.2 Software Licensing

Each individual user is responsible for conforming to the terms and conditions associated with the license agreement for each software application package. Using or creating copies of *[Company Name]* owned software is strictly prohibited. Violators of this policy will be subject to immediate dismissal from *[Company Name]*.

2.3 Software Installation

Installation of all software, software upgrades or (use of) demonstration programs is to be done only under the direction of the *[Title of IT Officer]*.

2.4 Software Demo\Trials

Occasionally, vendors will supply demo or trials of programs that users may use to evaluate new programs or upgrades to existing programs.

If a demo requires installation onto one of the *[Company Name]*'s PCs, the installation must be done under the direction of the *[Title of IT Officer]*. The *[Title of IT Officer]* must also be notified if a demo program is to be run directly from a CD. This will ensure that the demo does not conflict with any software currently residing on the PC. It will also aid in keeping the *[Title of IT Officer]* informed as to the types of programs in which users are interested.

3. Computer Viruses/Spyware

A computer virus is the software equivalent of an infectious intruder. It is a small section of computer code (program) concealed within a "normal" program. A virus can secretly attach itself to a PC program or system file, and then reproduce itself by gaining control each time the infected program is executed. The purpose may be as benign as flashing a holiday greeting, or as malicious as reformatting hard disks.

Generally, viruses\spyware are designed to destroy or steal user data or programs as the result of a given action or at a predetermined time. Such processes might erase the contents of a disk either on a given date, or upon the use of an otherwise innocent command. In all occurrences, the action of the virus is unexpected and deliberate. In some circumstances, actions occur instantly; in others, slowly, as in the occasional destruction of data over a period of time. Additionally, most viruses can copy themselves to other disks, programs or computers without the user's knowledge, thereby spreading their destructive effect.

Viruses can destroy information on standalone PCs, local area networks and mainframes. Most often infection occurs through mass-distributed software, public domain programs (including email), pirated software, and programs obtained from computer clubs and computer bulletin boards.

Computer viruses pose a very real threat to *[Company Name]*'s computing environment.

[Company Name] will purchase and maintain antivirus software. This software is meant to protect *[Company Name]*'s computing assets. No employee shall attempt to uninstall, disable, or otherwise circumvent this software.

4. Internet Access

The Internet is a major method of acquiring and disseminating information, data, and programs within the personal computing community. Its use at *[Company Name]* must include prudent actions that will protect the *[Company Name]* from undue risk of infection by viruses, spyware, adware, or illegal copying of software and music.

For our purposes the "Internet" is to be defined as either public or private. Private Internet locations (or "pages"), as well as private bulletin boards are often "sponsored" by a legitimate and known corporation or government entity for a specific business purpose. Material available on these mediums is commonly screened and controlled by the owning organization, which oversees the contents of the service, but this is not always the case. While users of such private services generally are not allowed to upload executable code for access by other users, this can happen.

While *[Company Name]* respects the privacy of all users, from time to time *[Company Name]* may routinely inspect or monitor Internet-related electronic services and transmissions without the end-user's consent. *[Company Name]* provides access to internet-related services and therefore *[Company Name]* may deny access to said services and may inspect or monitor usage when:

- Required by and consistent with law
- There is substantiated reason to believe that violations of law or Company policies have taken place
- There are compelling circumstances
- As provided for by this policy and other Company policies and procedures, which may be applicable

Public services, such as the Internet, are defined as those electronic services allowing the unregulated exchange of material including programs, with no attempt of quality controls applied to the contents of the service.
Public services such as these have become a very convenient method for distributing freeware/shareware. Unfortunately freeware/shareware programs are likely virus carriers. These services can provide value in certain circumstances when properly used. The following guidelines apply to their use at *[Company Name]*:

- Use of public electronic service is prohibited, except as directly authorized and monitored by the Information Technology Department
- No freeware/shareware is to be downloaded, installed, or negotiated in any way without the express knowledge and permission of the *[Title of IT Officer]*
- Items must be downloaded legally. This means that if upgrades to products are downloaded, the *[Company Name]* must be legally licensed to do so.

4.1 Personal Use

[Company Name] provided Internet-related services may be used for incidental personal purposes provided that, in addition to the foregoing constraints and conditions, such use does not: (1) directly or indirectly interfere with *[Company Name]'s* operation of computing facilities or electronic services; (2) burden the Company with noticeable incremental cost; or (3) interfere with the user's employment or other obligations to *[Company Name]*. Internet services users should assess the implications of the presumption in their decision to use *[Company Name]* Internet services for personal purposes.

4.2 Cautions

Electronic transactions via Internet related services, whether or not created or stored on Company equipment, may constitute a record subject to disclosure under regulations or other laws, or as a result of litigation. However, the Company does not automatically comply with all requests for disclosure, but evaluates all such requests against the precise provisions of the laws concerning disclosure and privacy, or other applicable laws. Users should be aware that stipulations of regulations and other laws may jeopardize the ability of the Company to guarantee complete protection of personal transactions or messages communicated via the Internet that utilize Company owned PC's, file servers, or communications servers for

such transactions. In general the Company does not condone use of its electronic services for personal use.

- *[Company Name]*, in general, cannot and does not wish to be the arbiter of either transactions or messages related to Internet related services when used by employees for personal means. Neither can *[Company Name]*, in general, protect users from receiving messages from the Internet they may find offensive.
- There is no guarantee, unless "authenticated" systems are in use, that messages and transactions either received or transmitted via Internet related services are secure. Additionally, it is a violation of this policy for users to disguise their identity for use of Internet related services for any reason.
- Staff members that are granted access to Internet related services are advised that all usage may be monitored by *[Company Name]*'s management through the use of logs and reports generated by the Company's file servers and proxy/firewall software. These logs and reports identify the services accessed by end-users and the time spent doing so.
- *[Company Name]*, prior to any inspection or monitoring, is not required to seek the end user's consent. Records or logs generated and stored on an employee's personal computer that pertain to *[Company Name]* business related dealings will be considered *[Company Name]* owned intellectual property.
- *[Company Name]* permits the inspection, monitoring, or disclosure of logs or records pertaining to Internet services without the consent of the holder; (i) when required by and consistent with law; (ii) when there is substantiated reason to believe that violations of law or of *[Company Name]* policies have taken place; (iii) when there are compelling circumstances; or (iv) should *[Company Name]* desire to review such records on the basis to ensure compliance with all published *[Company Name]* policies and procedures. *[Company Name]* reserves the right to utilize automated electronic tools to "scan" data flows for inappropriate content or abuse of services at any time. When the content that employees have requested or published to the Internet must be inspected, monitored, or disclosed without the end user's consent, the following shall apply:

    1. **Authorization.** *[Company Name]* need not obtain authorization in advance from the end user, but may seek such authorization from the end user's supervisor or manager. Requests for such non-consensual access from

either supervisors or managers must be submitted in writing to the Vice President of Operations or ISTC.

2. **Notification.** This policy serves as notification that at any time *[Company Name]* may monitor the data flow and information that end users request from and transmit to the Internet and other Internet related services.

3. **Compliance with Law.** Actions taken under Paragraphs 1 and 2 shall be in full compliance with the law and other applicable *[Company Name]* policies.

- **Recourse.** As Company owned Internet access and Internet related systems and the rights for usage of said systems are the property of *[Company Name]*, *[Company Name]* believes that recourse issues related to usage, monitoring or disclosure are not applicable.
- **Misuse.** In general, both law and *[Company Name]* policy prohibit the theft or other abuse of computing resources. Such prohibitions apply to Internet related electronic services and include but, are not limited to, unauthorized entry, use, transfer, and tampering with the accounts and files of others, and interference with the work of others and with other computing facilities. Under certain circumstances, the law contains provisions for felony offenses. Users of Internet related services are encouraged to familiarize themselves with these laws and policies.
- **Offensive and Inappropriate Material.** *[Company Name]* employees are not to access or distribute any material that could be considered inappropriate, offensive, counter-productive, or disrespectful to others. While it is impossible to list every form of such material, some clear examples include but, are not limited to:
    1. Materials that contain sexually explicit images or descriptions
    2. Materials that advocate illegal activity
    3. Materials that advocate intolerance for others
    4. Any material considered to be "Joke" material, such as chain letters or joke software programs

- **Representation.** Internet services users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of *[Company Name]* or any unit of *[Company Name]* unless appropriately authorized to do so. Where appropriate, an explicit disclaimer shall be included unless it is clear from the context that the author is not

representing *[Company Name]*. An appropriate disclaimer is: "These statements are my own, not those of the *[Company Name]*."

- **Interference.** *[Company Name]* provided Internet related services shall not be used for purposes that could reasonably be expected to cause; directly or indirectly, excessive strain on any computing facilities, or unwarranted or unsolicited interference with others' use of *[Company Name]* systems or Internet accounts. Such uses include, but are not limited to, the use of Internet services to; (i) access illicit or immoral content; (ii) access of confidential or illegal resources that may be available on the Internet; (iii) publish, disseminate or share confidential or classified *[Company Name]* and/or customer related data; (iv) utilize Internet related services for personal gain or competition with *[Company Name]*; and (v) streaming audio or video.

- **Unacceptable Activities.** The following list, although not all-inclusive, provides some examples of unacceptable uses:
    1. Private or personal for-profit activities (e.g., consulting for pay, sale of goods such as Avon, Amway, or Excel products, etc.), without prior written consent of *[Company Name]* management
    2. Use for any illegal purpose, including communications which violate any laws or regulations
    3. Intentionally seeking information about, obtaining copies of, or modifying files, other data, or passwords belonging to other users, unless explicitly authorized to do so.
    4. Transmitting or forwarding threatening, obscene, or harassing messages
    5. Interfering with or disrupting network users, services, or equipment. Such disruptions could include, but are not limited to, (1) distribution of unsolicited advertising or messages (2) propagation of computer worms or viruses (3) using Internet access to gain unauthorized entry to another machine or network resource via the Internet
    6. Personal use such as, seeking, searching for information regarding employment opportunities, any chat room program (other than those run by *[Company Name]*), etc.

7. Illicit use, such as pornographic web-sites, militant organizations, or any other uses that may be construed as an act of moral turpitude.

5. Work from Home (Telecommuting)

Many employees at *[Company Name]* own their own personal computers and would like to use them to do work at home. To guard against the threat of viruses *[Company Name]* does not allow business work to be taken home, except upon management approval and no offsite connection is allowed except on prior approval from management.

6. Security

Any user of a *[Company Name]* PC is responsible for its physical safety as well as the safety of its software and the information it processes. Employees are responsible for immediately reporting any violations, abuses or other security weaknesses to their supervisors.

6.1 Hardware Security

All fileservers, gateways, routers, network communications equipment, and hubs will be located in a safe, secure place where access is limited to authorized personnel only. The environment should be consistent with vendor specifications for the equipment being installed.

It is the responsibility of the individual users to bring to their supervisor's immediate attention any suspected tampering with their PC hardware. Moving or transferring the location of any PC hardware can only be done with the knowledge and approval of the *[IT Officers Title]*.

No vendor will remove any PC hardware from *[Company Name]* premises without first giving a written receipt to the *[IT Officers Title]*.

6.2 Local Area Network (LAN) Security

Security over the *[Company Name]'s* local area networks will be evaluated by the *[IT Officers Title]*. The level of such security will be commensurate with the vulnerability and importance of the application being accessed and

the sensitivity of the data being processed. Wherever feasible, the physical security of the PC will be the first consideration. In some cases, it may be appropriate to remove a PC from the local area network environment and have it function as a standalone.

Passwords will be the security control over software access wherever appropriate. Password parameter policy such as rotation schedule, minimum length, and reusability will be determined and maintained by the *[IT Officers Title]*. In all cases, it is the responsibility of each employee to maintain secrecy regarding their individual passwords and under no circumstances shall a password be divulged or shared with another.

Passwords should not be stored on computers, monitors, under keyboards, or in any fashion that would jeopardize password security.

In keeping with the policy of password protection, it is not prudent or acceptable to record or document a password in a location or manner which is not absolutely secure and invulnerable to unauthorized access. Whenever possible, multiple layers of passwords will be used to minimize accessibility by unauthorized personnel. More detailed policy regarding password management and responsibility will be addressed in sections following. Senior management or the *[IT Officers Title]* should be immediately notified, and the compromised password(s) immediately changed, if a user suspects someone has gained unauthorized knowledge of their password. This is critical because each individual user is responsible for any access gained to the system using their password.

6.3 Information Security

Information contained in *[Company Name]*'s computing environment is considered a corporate asset. The wide use of PC generated information has created opportunities for abuse and unauthorized use of these assets. Each user should be aware that they come into contact with various information that should be properly safeguarded. Information should be discussed and shared on a need-to-know basis only. Sensitive printed material should be kept out of sight. Accidental disclosure of customer and/or Corporate information could have a significant detrimental impact on *[Company Name]*.

Discarding PC information containing sensitive or confidential information should be done with extreme care and follow other *[Company Name]* policies and procedures for this type of data.

6.3 Other Security

Users should sign-off the network if their PC will be unattended. The primary reason for this, as stated earlier, is that all individual users are accountable for all activity and access that occurs via their logon passwords. Users should exit any software application when not in use. *[Company Name]* purchases a limited number of licenses of certain software applications. When users access one of these programs one of the licenses is considered "used" even though the user may not actually be performing functions within the program when others may need it.

7. Email

This section clarifies *[Company Name]*'s policies regarding electronic mail. It also defines new policy and procedures where existing policies do not specifically address issues particular to the use of electronic mail. This section is detailed and it is important that it is thoroughly understood

[Company Name] recognizes that principles such as freedom of speech and privacy of information hold important implications for electronic mail and electronic mail services. *[Company Name]* affords electronic mail privacy protections comparable to that which it traditionally affords paper mail and telephone communications. This Policy reflects these firmly held principles within the context of the *[Company Name]*'s legal and other obligations.

[Company Name] encourages the use of electronic mail and respects the privacy of users. While *[Company Name]* respects the privacy of all users, from time to time *[Company Name]* may routinely inspect, monitor, or disclose electronic mail without the author's or holder's consent. Electronic mail systems and the contents contained therein are the property of *[Company Name]* and therefore *[Company Name]* may deny access to its electronic mail services and may inspect, monitor, or disclose electronic mail when:

- Required by and consistent with law
- There is substantiated reason to believe that violations of law or *[Company Name]* policies have taken place
- There are compelling circumstances
- Under time dependent, critical operational circumstances

7.1 Cautions

Users should be aware of the following:

- Both the nature of electronic mail and the private character of the *[Company Name]*'s business make electronic mail less private than users may anticipate. For example, electronic mail intended for one person sometimes may be widely distributed because of the ease with which recipients can forward it to others. A reply to an electronic mail message stored on a file server intended only for the originator of the message could be distributed to all subscribers to the file server. Furthermore, even after a user deletes an electronic mail record from a computer or electronic mail account it may persist on backup facilities. *[Company Name]* cannot routinely protect users against such eventualities.

- Electronic mail, whether or not created or stored on *[Company Name]* equipment, may constitute a record subject to disclosure under regulations or other laws, or as a result of litigation. However, *[Company Name]* does not automatically comply with all requests for disclosure, but evaluates all such requests against the precise provisions of the laws concerning financial institution disclosure and privacy, or other applicable law.

- Users of *[Company Name]* provided electronic mail services also should be aware of stipulations in regulations and other laws may jeopardize the ability of *[Company Name]* to guarantee complete protection of personal electronic mail resident on *[Company Name]* owned PC's, file servers, or mail servers. In general, *[Company Name]* does not condone use of its electronic mail services for personal use.

- *[Company Name]*, in general, cannot and does not wish to be the arbiter of the contents of electronic mail when used by employees for personal means. Neither can *[Company Name]*, in general, protect users from receiving electronic mail they may find offensive. Employees however, are strongly encouraged to use the same personal and professional courtesies and considerations in electronic mail as they would in other forms of communication.

- There is no guarantee, unless "authenticated" mail systems are in use, that electronic mail received was in fact sent by the

purported sender, since it is relatively straightforward, although a violation of this Policy, for senders to disguise their identity. Furthermore, electronic mail that is forwarded may also be modified. Authentication technology is not widely or systematically in use as of the date of this Policy. As with print documents, in case of doubt receivers of electronic mail messages should check with the purported sender to validate authorship or authenticity.

- *[Company Name]* provides an Internet interface for its mail system. Use of this interface in public places, such as coffee shops, malls, hotels, or any place providing Internet access poses a potential security risk. Although the use of web mail is a great tool while out of the office, extra care should be taken while reading *[Company Name]* email in a public place.

- Employees will at no time send any information containing customer's nonpublic information to anyone, including themselves. When it becomes necessary for nonpublic information to be sent via email, information will be given to the *[IT Officers Title]* to be encrypted. This information will be provided via any means, but the original documents to be encrypted will NOT be emailed.

7.2 General Provisions

As noted in the introduction, *[Company Name]* recognizes that principles of freedom of speech, and privacy of information hold important implications for electronic mail and electronic mail services. This Policy reflects these firmly held principles within the context of the *[Company Name]*'s legal and other obligations.

- Purpose. In support of its mission to provide the necessary tools to encourage the efficient sharing of information relative to transacting of financial services, *[Company Name]*encourages the use of electronic mail services to share information, to improve communication, and to exchange ideas.

- *[Company Name]* employees are expected to comply with *[Company Name]* requests for copies of email records in their possession that pertain to the administrative business of the *[Company Name]*, or whose disclosure is required to comply with applicable laws, regardless of whether such records reside on a computer housed or owned by the *[Company Name]*. Email

records generated and stored on an employee's personal computer that pertain to *[Company Name]* business related dealings will be considered *[Company Name]* owned intellectual property.

- *[Company Name]* electronic mail systems and services are *[Company Name]* facilities as that term is used in other policies and guidelines. Any electronic mail address or account associated with the *[Company Name]*, or any sub unit of *[Company Name]*, assigned by *[Company Name]* to individuals, sub units, or functions of the *[Company Name]*, is the property of *[Company Name]*. Contents of electronic mail messages produced or stored on *[Company Name]* owned electronic mail systems are also considered the property of *[Company Name]*.

- Those who use *[Company Name]* electronic mail services are expected to do so responsibly, that is, to comply with local, state and federal laws, with this and other policies and procedures of *[Company Name]*, and with normal standards of professional and personal courtesy and conduct. Access to *[Company Name]* electronic mail services, when provided, is a privilege that may be wholly or partially restricted by *[Company Name]* without prior notice and without the consent of the email user when required by and consistent with law, when there is substantiated reason to believe that violations of policy or law have taken place, or, in exceptional cases, when required to meet time dependent, critical operational needs. Such restriction is subject to established *[Company Name]* procedures or, in the absence of such procedures, to the approval of *[IT Officers Title]*.

- *[Company Name],* prior to any inspection or monitoring is not required to seek an email author’s or holder's consent or disclosure of *[Company Name]* email records in the holder's possession.

- *[Company Name]* permits the inspection, monitoring, or disclosure of electronic mail without the consent of the author or holder of such email (i) when required by and consistent with law; (ii) when there is substantiated reason to believe that violations of law or of *[Company Name]* policies have taken place; (iii) when there are compelling circumstances; (iv) under time dependent, critical operational circumstances, or (v) should *[Company Name]* desire to review such email on the basis to

ensure compliance with all published *[Company Name]* policies and procedures. *[Company Name]* reserves the right to utilize automated electronic tools to "scan" email records for inappropriate content at any time.

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

- *[Company Name]* need not obtain authorization in advance from the end user, but may seek such authorization from the end user's supervisor or manager. Requests for such non-consensual access from either supervisors or managers must be submitted in writing to the *[IT Officers Title]*. *[Company Name]'s* counsel's advice may be sought prior to authorization because of changing interpretations by the courts of laws affecting the privacy of electronic mail, and because of potential conflicts among different applicable laws. Where the inspection, monitoring, or disclosure of email held by employees is involved, the advice of the Human Resources Manager shall be sought in writing in advance, following procedures as set in *[Company Name]* policy. All such advice shall be given in a timely manner.

- In emergency circumstances the least perusal of contents and the least action necessary to resolve the emergency may be taken immediately without authorization, but appropriate authorization must then be sought without delay following the procedures described above. If the action taken is not subsequently authorized, the responsible authority shall seek to have the situation restored as closely as possible to that which existed before action was taken.

- In either case, the responsible authority or designee shall, at the earliest possible opportunity that is lawful and consistent with other *[Company Name]* policy, notify the affected individual of the action(s) taken and the reasons for the action(s) taken.

- Compliance with Law. Actions taken under Paragraphs 1 and 2 shall be in full compliance with the law and other applicable *[Company Name]* policy. This has particular significance for email residing on computers not owned or housed by the *[Company Name]*. Advice of counsel may be sought prior to any action taken under such circumstances. It also has particular significance for email whose content is protected under the

Financial Institutions Privacy Act, which applies equally to email as it does to print records.

7.3 Misuse

In general, both law and *[Company Name]* policy prohibit the theft or other abuse of computing resources. Such prohibitions apply to electronic mail services and include (but are not limited to) unauthorized entry, use, transfer, and tampering with the accounts and files of others, and interference with the work of others and with other computing facilities. Under certain circumstances, the law contains provisions for felony offenses. Users of electronic mail are encouraged to familiarize themselves with these laws and policies.

Chain letters and hoaxes come in many versions, for example offering a free trip or a large amount of money, warning about a computer virus, or relating to a sympathetic cause. These letters often request that you send them on to other people.

Using *[Company Name]*'s computer systems to send or reply to chain letters, hoaxes, or virus warnings is strictly prohibited. If you receive an e mail chain letter or virus warning, do not send it on, but send it to *[IT Officers Title]*.

[Company Name]'s employees are not to access or distribute any material that could be considered inappropriate, offensive or disrespectful to others. While it is impossible to list every form of such material, some clear examples include:

- Materials that contain sexually explicit images or descriptions
- Materials that advocate illegal activity
- Materials that advocate intolerance for others

Employees should discuss questions concerning inappropriate or offensive material with their managers.

7.4 Phishing\Pharming

Phishing is a tactic to trick people into giving out personal and financial information by pretending to be from a legitimate company.

The most common form of phishing is by e-mail. Pretending to be from a financial institution, or a legitimate retailer or government agency, the sender asks you to "confirm" your personal information for some made-up

reason. Typically, the e-mail contains a link to a phony Web site that looks just like the real thing – with sophisticated graphics and images. In fact, the fake Web sites are near-replicas of the real one, making it hard even for experts to distinguish between the real and fake Web sites. You enter your personal information onto the Web site – and into the hands of identity thieves.

Pharming is the exploitation of a vulnerability in the DNS server software that allows a hacker to acquire the Domain Name for a site, and to redirect traffic intended for that website to another web site. DNS servers are the machines responsible for resolving Internet names into their real addresses - the "signposts" of the Internet.

If the web site receiving the traffic is a fake web site, such as a copy of a *[Company Name]*'s website, it can be used to "phish" or steal a computer user's passwords, PIN number or account number. Note that this is only possible when the original site was not SSL protected, or when the user is ignoring warnings about invalid server certificates.

If customers contact *[Company Name]* asking about emails sent from a *[Company Name]* representative or a website requesting personal or financial information, instruct them to ignore the email and to not divulge any information. *[Company Name]* will never request this type of information through an email.

7.5 Allowable Use

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

- Electronic mail services are to be provided by *[Company Name]* in support of the organization's mission in providing financial services to the customer base, and the administrative functions that support this mission.

- Users of *[Company Name]* electronic mail services are to be limited primarily to *[Company Name]* officers and staff for purposes that conform to the requirements of this section. If employee job duties change, the removal of *[Company Name]* owned email addresses may occur to conform to the employee's new job duties.

- *[Company Name]*'s electronic mail services shall not be provided in competition with commercial services to individuals or companies outside *[Company Name]*.

- *[Company Name's]* electronic mail services may not be used for: unlawful activities; commercial purposes not under the auspices of *[Company Name]*; personal financial gain (see applicable *[Company Name]* policies and procedures); personal use that interferes with *[Company Name]* business or uses that violate other *[Company Name]* policies or guidelines. The latter include, but are not limited to, policies and guidelines regarding intellectual property, or regarding sexual or other forms of harassment.

- Electronic mail users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of *[Company Name]* or any unit of *[Company Name]*, unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer shall be included, unless it is clear from the context that the author is not representing *[Company Name]*. An appropriate disclaimer is: "These statements are my own, not those of *[Company Name]*."

- *[Company Name]* email users shall not employ a false identity. Email may, however, be sent anonymously provided this does not violate any law or this or any other *[Company Name]* policy, and does not unreasonably interfere with the administrative business of *[Company Name]*.

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

7.6 Archival and Retention

- *[Company Name]'s* record management policies do not distinguish among media with regard to the definition of *[Company Name]* records. As such, electronic mail records are subject to these policies. In particular, such records are subject to disposition schedules as maintained by *[Company Name]*.

- *[Company Name]* does not maintain central or distributed electronic mail archives of any mail sent or received.

- Email users should be aware that generally it is not possible to assure the longevity of electronic mail records for record-keeping purposes in part because of the difficulty of guaranteeing that electronic mail can continue to be read in the face of changing formats and technologies and in part because of the changing nature of electronic mail systems.

- Email users and those in possession of *[Company Name]* records in the form of electronic mail are cautioned, therefore, to be prudent in their reliance on electronic mail for purposes of maintaining a lasting record.

8. Instant Messaging

Instant Messaging programs that access the Internet (MSN Messenger, Yahoo Instant Messenger, etc.) are not authorized on any *[Company Name]* computer.

9. Policy Violations

Violations of *[Company Name]* policies governing the use of *[Company Name]* information technology services may result in disciplinary action, up to and including dismissal; as provided for under other *[Company Name]* policies and/or guidelines.

Employee Acknowledgment Form

Please sign and return this agreement. Signature confirms agreement and acceptance to be bound by this policy. Failure to return signed receipt may affect your ability to access Internet related services and PC systems.

I have read and fully understand my responsibilities and the policy of *[Company Name]* in regard to its End User Information Policy, which includes PC, Email, Internet, and Software usage.

_____

Printed Name

_____

Signature

_____

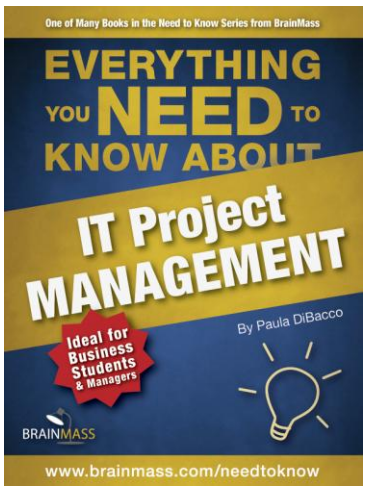
Date

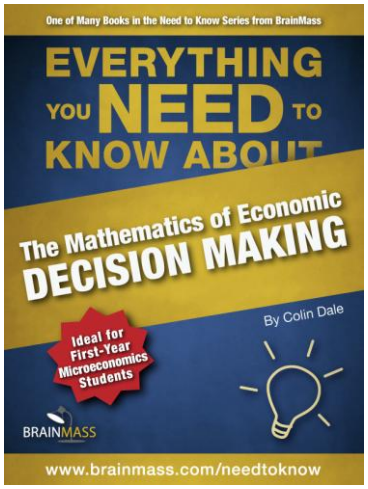
About the Author

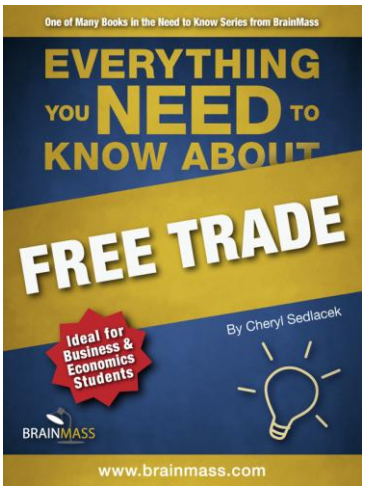
Rob Beachy is the current Vice President of Information Technology for a community bank located in Michigan. He received his Bachelor's degree in Information Systems from the University of Phoenix, graduating with a perfect 4.0 GPA. He went on to obtain a Master of Science in Information Assurance from Davenport University in Grand Rapids, Michigan with a GPA of 3.96. Mr. Beachy holds certification in Novell, Microsoft, and holds a CompTIA Security+ certification. He is an active BrainMass expert and enjoys sharing his knowledge with lifelong learners. Mr. Beachy has completed a National Security Systems Information Systems Security (INFOSEC) professional's course in 2010.

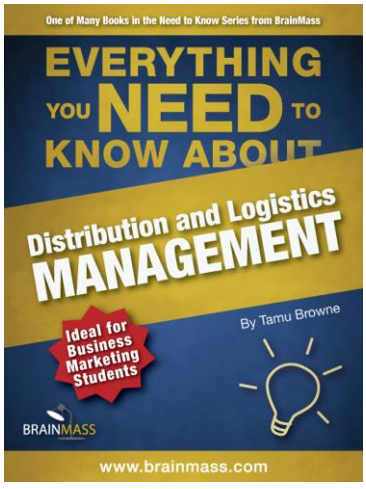
More eBooks from BrainMass

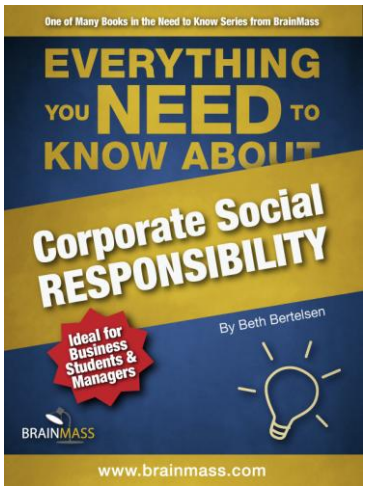
There are a number of other books in the BrainMass eBook Library. Here are a selection that you might be interested in:

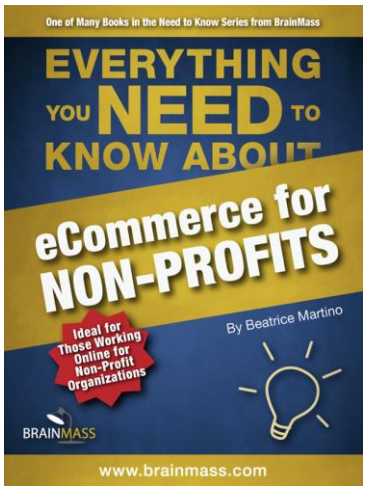












To read more about these books and more, click on the link below:

http://brainmass.com/ebooks